02\22

C²BRNE DIARY

Dedicated to Global First Responders

February 2022

PART B

The first CWA antidote that cross blood-brain barrier by LLNL

www.cbrne-terrorism-newsletter.com

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

C2BRNE DIARY

DIRTY R-NEWS

Attacks inside one of Iran's most secure nuclear facilities are the latest blows in a shadowy battle with Israel

By Stavros Atlamazoglou

Source: https://www.businessinsider.com/attack-inside-iran-nuclear-facility-latest-in-battle-with-israel-2022-1

A damaged building after a fire broke out at Iran's Natanz nuclear facility, in Isfahan, July 2, 2020. Reuters

Jan 24 – After the US unilaterally withdrew from the Iran nuclear deal in 2018, tensions between Washington and Tehran have steadily risen.

For leaders in Israel — one of the US's closest partners and Iran's biggest foes — those tensions have confirmed their misgivings about the deal and about Iran, and they've gone on the warpath.

Iran has worked on nuclear technology for decades. The US has long suspected Iran of using its civilian nuclear program as cover for developing weapons. That suspicion is also held by the Israelis, who have been ensnared in a potentially existential struggle with Tehran since the 1979 Iranian revolution.

A nuclear weapon, or the ability to produce one quickly, would offer Tehran some much-needed security against its real and perceived adversaries. But Iran has vowed to destroy Israel, and Israel fears a nuclear weapon would allow Tehran to back up its provocative talk.

While much of that talk may be for propaganda purposes, Iran has shown the lengths it will go and pain it will endure in order to attack US, Western, and Israeli targets directly or through proxies, giving some weight to its nuclear threats.

To counter that threat, Israeli military and intelligence services have conducted a shadowy covert-action campaign of espionage, sabotage, and assassinations against Iran's nuclear facilities and the people running them.

Israel's war against Iran

Israel has also shown that it will go to great lengths to ensure its security, and Tel Aviv is willing to pursue other, more dramatic courses of action in response to threats from Iran.

Cover photo: National Ambulance Resilience Unit crew (UK)

"We have a duty to be brave and responsible for the fate of our children and grandchildren. We have used force against our enemies in the past, and we are convinced that in extreme situations, there is a need to act using military means," Israeli Deputy Defense Minister Alon Schuster said in a recent interview.
Indeed, Israel has long followed a no-holds-barred strategy in which the threat justifies the means. Its shadowy campaign against the Iranian nuclear programs uses complementary diplomatic, military, and intelligence tactics.
While Israel's military has been heavily involved in that campaign, Mossad, Israel's main intelligence service, has landed many of the blows against Iran itself.
According to a recent report by The Jewish Chronicle, which didn't name or describe its sources, Mossad successfully infiltrated the Iranian supply chain and used the opportunity to sell Tehran faulty materials that caused fires at the Natanz nuclear-enrichment facility in July 2020.
The report also said Israeli intelligence officers recruited Iranian nuclear scientists who conducted sabotage at Natanz in April 2021 before being smuggled out of the country. Mossad is said to have used an unmanned aerial vehicle to attack the Iran Centrifuge Technology Company, a factory making centrifuges crucial for producing weapons-grade uranium.

Facilities are easier to replace than expert knowledge, and Mossad has also gone after the hard-to-acquire know-how necessary for a nuclear-weapons capability by killing Iranian scientists working on the nuclear program.

The scene of the attack that killed prominent Iranian scientist Mohsen Fakhrizadeh, outside of Tehran, November 27, 2020. WANA via Reuters

Attacks against Iranian scientists have become more brazen. The November 2020 assassination of Mohsen Fakhrizadeh, reportedly with a remote-controlled machine gun using advanced artificial-intelligence technology, on a highway in Iran is something straight out of a Hollywood movie.
Israel's manhunting effort likely draws on experience going back to Israel's creation in 1948. In the years that followed, Israelis hunted down numerous ex-Nazis, including Holocaust architect Adolf Eichmann. Following the 1972 killing of Israeli athletes at the Munich Olympics by Palestinian terrorists, Mossad conducted a similar campaign.
But Tel Aviv understands that this is a stalling tactic that can only frustrate Tehran's efforts and not permanently undo the work its done in pursuit of nuclear technology.
In addition to those clandestine actions, the Israeli Defense Forces has been preparing and presenting Israeli policymakers with military options to take out targets associated with Iran's nuclear program. This is standard planning for any military, and the IDF has received nearly $3 billion in additional funds to do it.
Israel would also have to take into account second- and third-order effects of such strikes, such as how Iranian proxies, including Hamas and Hezbollah, would react. Those groups, based in the Gaza Strip and Lebanon, respectively, would be more likely to try to attack Israel.
Israeli officials are lobbying other countries to take a stronger stance against Iran while refraining from directly discussing what actions they've taken.
"We hope the whole world will be mobilized for the mission. For that, we've allocated a significant sum to increase our readiness. What hit Natanz? I can't say," Schuster, the deputy defense minister, said last month.
As Iran remains committed to its nuclear program, Israel is sure to continue its shadowy campaign against Tehran.

Stavros Atlamazoglou is a defense journalist specializing in special operations, a Hellenic Army veteran (national service with the 575th Marine Battalion and Army HQ), and a Johns Hopkins University graduate.

What are Switzerland's nuclear bunkers and does each home need one?

Source: https://www.thelocal.ch/20220124/what-are-switzerlands-nuclear-bunkers-and-why-does-each-home-need-one/

Jan 24 – One of the obvious 'Swiss paradoxes' is that a neutral country which hasn't been attacked since Napoleon's invasion in 1798 has built enough fallout shelters to protect the entire population. Here's why.

If you live or have ever lived in a house in Switzerland built between the 1960s and late 1980s, you are likely familiar with nuclear bunkers located in the basement.

These shelters have a reinforced steel door, ventilation system, anti-gas filter, and enough shelves to stock a two-week supply of water, medications, and non-perishable food.

But why?

A thick, reinforced steel door leads to Switzerland's largest communal shelter. Photo by Unterirdisch Ueberleben

Put it down to Swiss pragmatism and a penchant for meticulous planning: the Swiss don't like to leave anything to chance and prepare for all kinds of scenarios, whether plausible or not.

The same kind of disaster preparedness which required, until fairly recently, that all Swiss serving in the military keep guns and ammunition in their homes so they would be ready to fight the enemy at a moment's notice, also mandated that each dwelling had a well-equipped bunker in case the Russians attacked.

Today, such an act against Switzerland seems highly unlikely, but 50 years ago, at the height of the Cold War, the government saw this as a possible scenario — so much so, that it passed a legislation in 1963 requiring nuclear shelters in all residential buildings.

They were to be used "during an armed conflict, especially one involving weapons of mass destruction", according to the Federal Office of Civil Protection (FOCP), which added that these bunkers "provide a basic form of protection against a wide range of direct and indirect arms impact".

Have these shelters ever been used?

Yes and no.

As Switzerland has not been invaded by Russians, or anyone else for that matter, the shelters never had to be used for their intended purpose.

In 2005, Pierre Kohler, who was an MP at the time, submitted an initiative to abolish the law that made the construction of nuclear bunkers mandatory in private homes because, he argued, they were "relics of other times" and no longer necessary.
But the Federal Council rejected this proposal, saying these constructions were still useful outside of a war context, since they could also be used as hideouts during chemical accidents, natural disasters, or a terrorist attack using nuclear weapons.
From 2012, however, only residential buildings with more than 38 apartments are required to have fallout shelters in their basements.
The Local wrote about this change at that time:
So, the answer to the question of whether these bunkers have ever been used in a national emergency, is no.
They have, however, served other purposes over the years: to make sure this extra space doesn't go to waste, many Swiss households used it as a storage space for wines, ski equipment, and other objects.

Do you actually need a bunker in your home?
These structures are no longer compulsory in single-family houses, though the law stipulates that each resident "should be guaranteed a shelter in the vicinity of her/his place of residence".

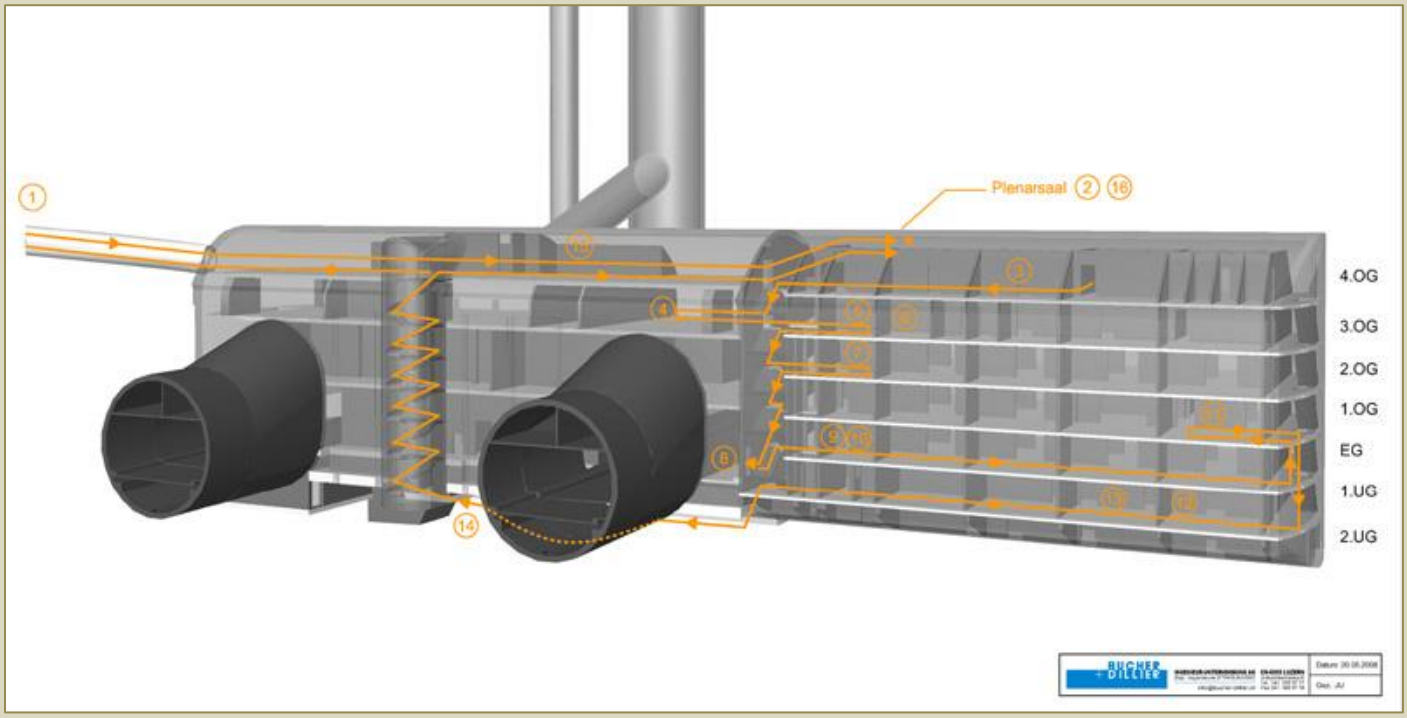
Sonnenberg bunker was built in and over two motorway tunnels. Photo: Unterirdisch Ueberleben

Today, Switzerland has 360,000 communal shelters able to accommodate the entire population in case of need.
The largest such bunker— not only in Switzerland but also reportedly in the world — is Unterirdisch Ueberleben located in Lucerne. Built on top of two motorway tunnels in the Sonnenberg mountain, it can provide shelter for 20,000 people.

The reason for maintaining the shelters is that "there are still a great number of ballistic missiles, with or without weapons of mass destruction, to be found worldwide", FOCT said.
Everyone is Switzerland should know where their nearest shelter is located. You can find this out at your commune of residence.

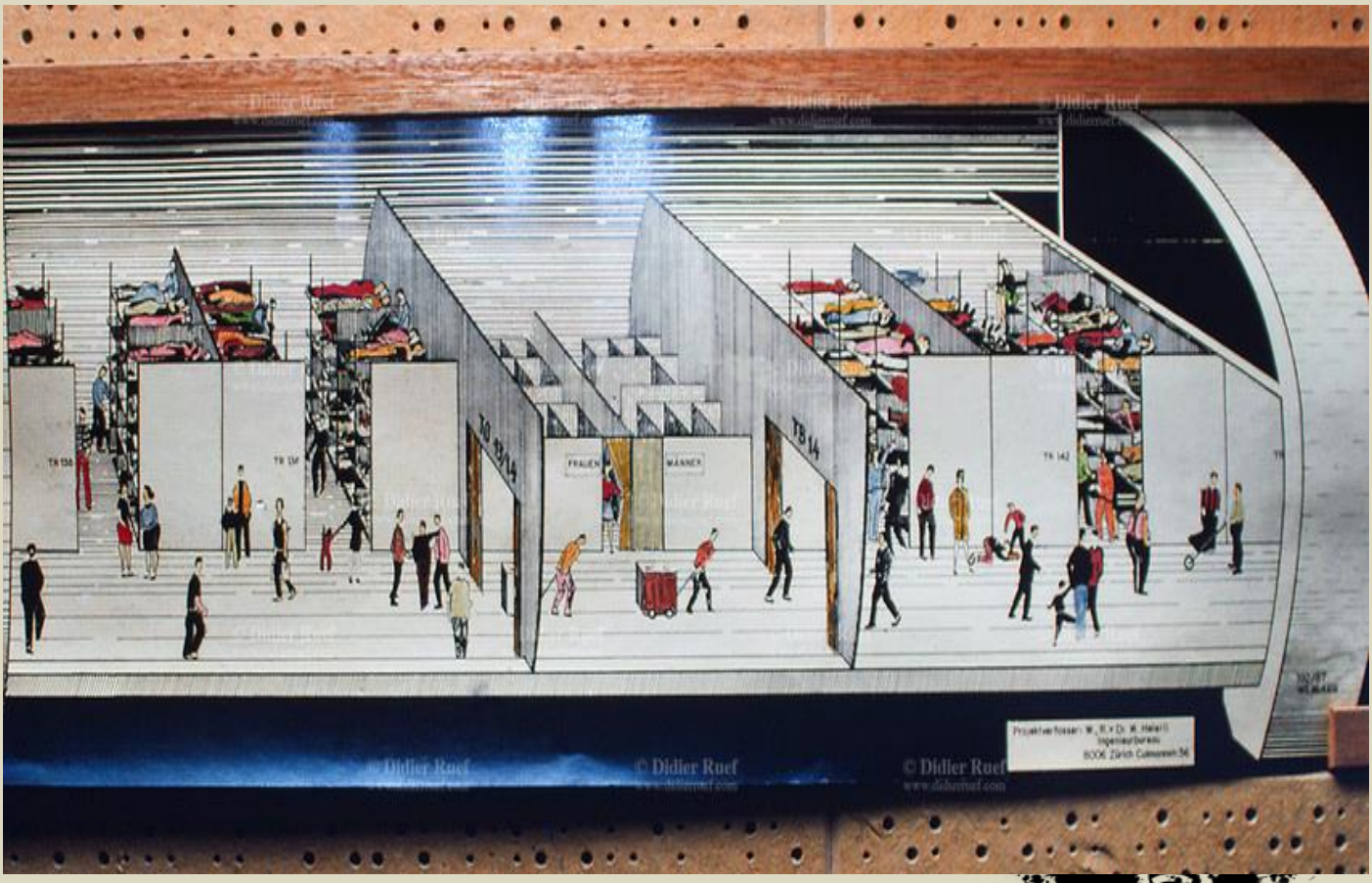
A second life for military bunkers
While civilian shelters started to be built in Switzerland in the 1960s "just in case", military ones were constructed in response to a real danger.
When the Nazis started invading countries east and west of Switzerland in 1939, the Swiss military dug over 20,000 bunkers in the Alps. They allowed soldiers to stay hidden — along with their weapons, ammunition, and other supplies — and defend the country in case of an attack.

The attack never came and the bunkers were decommissioned at the end of the Cold War, standing empty until the 1990s when the



military started to sell them to private companies.

Eventually, these demobilised fortresses, some dug deep into mountain walls, morphed into such civilian venues as a "bank" to securely store digital data, a hotel, banquet halls and seminar centres, and, in at least one case, a giant storage room for cheese. This shows that, in one way or another, the Swiss still have a bunker mentality.



●▶ **More information about shelters is** here.

Country Profile: Brazil

By Ms. Sara Mansour (Analyst, IB Consultancy)
NCT Magazine 2022
Source: https://nct-magazine.com/nct-magazine-january/country-profile-brazil/

In South America, the Brazilian Army has made new attempts to improve its CBRN response capabilities. Founded in December 2012, the 1st CBRN Defense Battalion is based in the city of Rio de Janeiro. Considering this, Brazil's major special operations force is the only unit of the army trained to wage unconventional warfare. The Army's frontline CBRN deployment oversees the monitoring, identification, and decontamination of CBRN threats. High visibility events in Brazil, such as the 2014 World Cup and the 2016 Olympic Games in Rio, which welcomed prominent state officials and international figures, brought remarkable attention to the field of CBRN.
Brazil has never manufactured nuclear weapons and there is no proof that it has a goal of increasing uranium enrichment to more than 20%. From the 1960s to the mid-1990s, Brazil embarked on a focused program to enhance nuclear innovation, including the development of a uranium advancement office under the Navy's division.

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

Militarized Dolphins Protect Almost a Quarter of the US Nuclear Stockpile

By Blake Stilwell
Source: https://www.military.com/history/militarized-dolphins-protect-almost-quarter-of-us-nuclear-stockpile.html

Situated just 20 miles from Seattle, Naval Base Kitsap houses America's most powerful and secret deterrents, a weapon that is the first line of defense for U.S. national security: U.S. Navy dolphins.

Since 1967, the Navy has been training dolphins and sea lions (and probably other marine life) for military applications such as mine clearing, force protection and recovery missions. The U.S. Navy Marine Mammal Program deployed military dolphins as early as the Vietnam War and as recently as the 2003 U.S.-led invasion of Iraq.
When protecting harbors and ships from mines, as they do at Naval Base Kitsap, the dolphins use their extraordinary biological sonar to detect hazards beneath the surface, whether tethered to the sea floor or buried beneath sediment.

(U.S. Navy/Mass Communication Specialist 2nd Class Joshua Scott)

If a mine or other weapon is detected, the dolphin returns to its handler, who gives the animal a buoy to mark the location of the device on the surface. Passing ships know to avoid these markers while Navy explosives ordnance disposal divers neutralize the threat below.
For protection against enemy divers, dolphins will swim up to the infiltrator, bump into them and place a buoy device on their back or a limb using their mouth. The buoy then drags the outed diver to the surface for easy capture. When trained sea lions perform the same maneuver, they use a kind of handcuff with their mouths to attach the buoy.

Since Bangor, Washington, now houses the largest single nuclear weapons site in the world, it needs protection from all sides, including the seaward side. That's where the Navy's dolphin pods and sea lions come in. Navy spokesman Chris Haley says the animals have been defending the waters around the stockpile, holding roughly 25% of the United States' 9,962 nuclear warheads, since 2010.
The United States isn't the only country known to train marine animals for these kinds of missions. Its sea mammal mission only became public knowledge in the 1990s, however. The Soviet Union trained dolphins for similar harbor protection.
After the fall of the USSR, the program was said to be in limbo, and the Soviet-trained dolphins are believed to have been sold to Iran in 2000. Russia is said to have been looking to update its training program, and may even have used them in Syria.
Satellite imagery near the North Korea city of Nampo has revealed what look to be dolphinariums in the Taedong River, meaning North Korea may have a dolphin-based anti-infiltration plan of its own.

Blake Stilwell is a former Air Force combat photographer with degrees in Graphic Design, Television and Film, International Relations, Public Relations and Middle Eastern Affairs. Instead of using those, he (eventually) became a writer. His work has appeared on Business Insider, Military Times, We Are The Mighty, Fox News, ABC News, NBC Sports, HBO Boxing, and at the White House.

How to Run A Safe, Cost-Effective, and Efficient Radiation Training Simulation as a CBRNe Instructor

By Bryan W Sommers

Source: https://www.argonelectronics.com/blog/how-to-run-a-safe-cost-effective-and-efficient-radiation-training-simulation-as-a-cbrne-instructor?

Feb 01 – On the surface, radiation training can seem somewhat straightforward: teach students how to properly and safely respond to situations involving radiation. However, as many CBRNe instructors know, it's not that simple.
There are key factors and challenges to consider when implementing a training scenario, the most significant of which includes safety, realism, cost, and logistics. Many of these can be overcome with one key solution: a real experience simulation.
With that in mind, let's take a closer look at some common challenges CBRNe instructors face when running radiation training, and then delve into how simulations can solve these issues.

Radiation Training: Arguably The Most Problematic CBRNe Exercise

While chemical training can have its own set of challenges, many will argue that a radiological training scenario is much more problematic to run effectively. There are key challenges to consider, including:

Safety

As CBRNe professionals appreciate, ionising radiation is a potentially harmful form of energy that needs to be handled carefully. The safety of both the trainer and the trainee(s), the public at large, and care of the environment, must all be prioritised during every training session.

That said, there are a vast array of legislative, administrative and health and safety implications which make the storing, transporting, handling, deployment and dispersion of live radiological sources a challenging (and often unviable) option for radiation safety training. These will likely limit how you run your scenario, especially when considering the amounts and types of radiological sources which can be used, where they can be deployed and ultimately the quality of the overall student training experience.

Instructors looking to run hands-on training scenarios that properly replicate features of a real radiation incident will usually find that safety concerns are their biggest roadblock.

Realism

It can be difficult to achieve the "pucker factor" necessary for realistic radiation training whilst also meeting the aforementioned safety protocols. Instructors are frequently challenged to find engaging ways to deliver scenarios, especially in terms of hands-on learning using realistic instruments.

Have you ever had a student work out where the hazard was because they saw the safety marshal or the radiation source safety markers? That's a sign that the training wasn't real enough for them.

Cost

Radiological sources can come at a significant cost, especially if and when training scenarios need to be repeated. Other considerations are costs of location rental and travel to the venues themselves, as usually, these are highly limited and geographically undesirable.

Instructors also need to organise and pay for the appropriate safety marshals required for the training. Finally, there's an eventual significant cost of end of serviceable life source disposal.

Logistics

Instructors looking to run a radiation training scenario need to not only plan the training event itself, but also find a safe, authorised location to run it. These are generally remote, empty buildings which can be problematic to not only access but travel too. Instructors are also limited to the schedules of the labs providing the radioactive materials, which makes them unable to control when the training can take place.

As instructors know, the most effective learning comes from practice and repetition. However, after considering safety, cost, and logistics, it's easy to see why traditional radiation training can be difficult to either practice or repeat.

Why Radiation Training Simulators Are Key To Safe, Cost-Effective, and Efficient Teaching Scenarios

Generally, teaching students how to use the radiation detection equipment itself can be straightforward. The real training lies in understanding the significance of the detector readings, recognising changes in units of measurement, and familiarising students with the concept of shielding, survey, contamination avoidance, decontamination procedures, and dose management.

As mentioned, this involves a certain amount of practice and repetition. One of the greatest strengths of a radiation simulation is the instructor's ability to quickly, efficiently, and safely set up the training scenario, all of which allows for repeatability.

This is why real experience radiation simulations are a key component of CBRNe training. As with all training, however, there are still some important factors to consider when running these simulations.

Here are a few things to consider when running a safe, cost-effective, and efficient CBRNe radiation training simulation:

Safety

As Argon's simulators don't contain any real radiological sources, instructors don't need to consider potential radiation exposure to those involved in the training.

However, you should still perform basic safety checks, such as clearing any trip hazards, ensuring first aid kits are on hand, and providing appropriate PPE for the training site.

Cost

The whole-life cost of Argon's radiation simulators is much lower than traditional radiological training solutions, however, there are always ways to cut costs further.

Utilising Argon simulators allows for far greater flexibility in your training location, so research new areas with cheaper rental rates. Additionally, since Argon's simulators are easy to reset, you can negotiate with these spaces for multiple sessions at a lower rate.
Also, consider geography. Argon simulators can be used anywhere, so you have the freedom to choose a site close to your headquarters to minimise travel time and cost. There is also the option to train at sensitive locations such as railway stations, airports, and public venues.

Adding Efficiency and Realism

Ideally, any radiation safety training scenario should be as simple as possible to set up and repeat. This is another reason Argon simulators outperform traditional CBRNe radiation training.

Argon's app-based PlumeSIM-SMART, for example, enables you to easily select the timing and duration of single or multiple virtual radiation plumes. This simulator allows for tabletop and large field exercises of up to 2500 square kilometers. With just a few taps, you can set key meteorological conditions and modify wind direction and velocity during the exercise.
You can set up the Plume-SIM-SMART anywhere, at any time. This allows for practice in any type of weather, which is important to consider when radiation responses can be affected by wind, fog, and other meteorological conditions.
Another key consideration is injecting realism into the scenario. Index cards and over-the-shoulder directions simply don't offer the same level of realism as an actual device in a student's hands, with readings from a true-to-life radiation simulation.

This is why many CBRNe instructors are looking forward to working with Argon's new AccuRad PRD Simulator.
Argon's wealth of simulation experience combined with its relationship with Mirion has resulted in a training device with user interface components (front and top displays, indicators, trend and radar mode, switch panel, sounder, and vibrator) which are exactly the same as the real detector. Instructors will be able to deliver extremely realistic source search/find training with response speed and characteristics when approaching and withdrawing from the simulation source.
This level of hands-on training enables students to test their understanding of crucial radiation response measures, such as personal dose, shielding, time, distance, and inverse square law.
Real experience training also empowers students to more confidently interpret readings on their devices, understand the significance of any changes in the units of measurement, and accurately relay their findings to those higher up the chain of command (without turning to their instructor for help).
Safety, cost, and efficiency are all crucial to consider when running a CBRNe radiation training scenario. One of the main goals for instructors, however, is to ensure that their students learn how to properly respond to an array of events.
The best way to achieve this is to expose students to a variety of realistic, repeatable scenarios in various locations and weather conditions, which is exactly what real experience training offers.
To learn more about radiation simulation training, including how electronic simulators are revolutionising CBRNe radiation training and which equipment is required for live incident radiation detection, download the free Argon Radiation Safety eBook.

Sergeant Major Bryan W Sommers has forged a distinguished career in the fields of CBRNe and HazMat training. He recently retired after twenty-two years of service in the US Army, with fourteen years spent operating specifically in Weapons of Mass Destruction

(WMD) environments. In 2020 he was appointed as Argon Electronics' North American business development manager.

The Resilience and Safety of Nuclear Power in the Face of Extreme Events

By Matthew Fisher

Source: https://www.homelandsecuritynewswire.com/dr20220201-the-resilience-and-safety-of-nuclear-power-in-the-face-of-extreme-events

Feb 01 – Nuclear power plants are built to last. But as the prospect of extreme global events grows — from natural disasters and intensifying climate change-driven weather patterns that could affect a plant, to a rise in infectious diseases that could affect its workforce — nuclear power plants' adaptable workforces and robust designs will be essential to staying resilient and contributing to a low carbon path to the future.

"For the world to mitigate climate change in the next 20 to 30 years, the energy sector needs to fundamentally transform into a low carbon energy supply system," said Loreta Stankeviciute, an energy systems analyst at the IAEA. "But to do that, the sector also needs to be able to withstand and adapt to extreme events and changes in the environment. Nuclear power's resilience and safety records make it well positioned to help the global community overcome these challenges."

Pandemics

A recent test of resilience emerged during the unprecedented COVID-19 pandemic.

As the COVID-19 virus spread to every corner of the globe in the first part of 2020, societies and economies were turned upside down. Numerous restrictions, including lockdowns, were adopted to control the spread of the virus.

"Despite these worldwide constraints, nuclear power plants around the world continued to operate safely. Operators seamlessly implemented contingency plans, including a variety of emergency measures, to maintain operations and keep personnel safe," said Greg Rzentkowski¸ Director of the IAEA's Division of Nuclear Installation Safety. "Operators took the necessary precautions and carefully implemented operational and organizational changes, while continuing to ensure safety and security of nuclear power plants."

While no country has reported the enforced shutdown of a nuclear power reactor due to the effects of COVID-19, some scheduled maintenance outages have had to be, with regulatory approval, either shortened or postponed as part of protective health measures that have temporarily scaled back non-critical work, according to operator reports. There are also concerns that pandemic-related supply chain disruptions, such as delayed services and temporary closures of manufacturers, could lead to delays in new builds and major refurbishment projects.

"It remains to be seen how much of an impact these pandemic-related disruptions will have on the industry, said Dohee Hahn, Director of the IAEA's Division of Nuclear Power. "The input we continue to receive provides us with crucial insight as to the pandemic's impact on the nuclear industry and will help operators and regulators alike learn from each other's experiences."

Nuclear power has not only proven its resilience during the pandemic but has also shown that it is safe and well suited to meet changing energy needs. Since the pandemic began, the share of nuclear power has increased in some countries, including Brazil, India and South Korea. In the United Kingdom, for example, nuclear power has played a significant role in drastically reducing the amount of coal burning for electricity; the pandemic-induced lower demand for electricity allowed the UK to temporarily close coal plants in favour of an increased use of nuclear power.

Climate change

Just as the resilience of a plant's workforce has been necessary to continue operations unimpeded during the ongoing pandemic, their resilience and a nuclear power plant's robust design are also required in the face of extreme weather events, including those driven by climate change.

Caused by the global mean temperature increase, climate change is altering the severity and frequency of weather events, such as temperature extremes, periods of heavy rainfall, high winds and major sea level rises. These changes are expected to continue to increase in the near to long term.

"While rising water and air temperatures may pose challenges to the continuity of reactor operation by limiting its cooling capacity, it's the extreme floods and winds that may affect reactor safety by posing threats to the installation's design," said Rzentkowski. "One of the challenges with climate change is that, as it continues to progress and make conditions more extreme, past observations and predictive models become less reliable. We should thus start anticipating these events and periodically reassess the relevant risks to ensure that accident prevention and mitigation measures remain adequate."

Natural events

Nuclear power plants may also be affected by extreme natural events, such as earthquakes, tornados, volcanic activity, ice storms and flooding. In rare circumstances, these events can be extreme enough to exceed the design capacity of a nuclear power plant. An example of this is the accident at the Fukushima Daiichi Nuclear Power Plant in Japan on 11 March 2011, which was triggered by a tsunami that followed a massive earthquake. While the nuclear power plant was damaged by these events and the consequent hydrogen explosions, no lives were lost due to the accident.

In the aftermath of the Fukushima Daiichi accident, concrete steps have been taken to further enhance safety at existing nuclear power plants and refine the designs of new plants against extreme events. These measures include, for example, alternative cooling options, environmentally qualified back-up generators, shields and seals to guard against wind, and dykes and other embankments to protect sites against flooding.

All types of external events that may affect a nuclear site or the safety of nuclear installations are also addressed by the IAEA safety standards, including site evaluation and design and safety assessment. These standards reflect the current state of practice and are used to ensure safety throughout a plant's lifetime. The IAEA also provides guidance through its Nuclear Energy Series and other technical publications such as Adapting the Energy Sector to Climate Change.

Matthew Fisher is Communications Program Liaison at the Idaho National Laboratory (INL).

Hanford begins 1st large-scale treatment of nuke tank wastes

Source: https://www.kob.com/news/hanford-begins-1st-large-scale-treatment-of-nuke-tank-wastes/6378205/

Feb 02 – Workers on a former nuclear weapons production site have started the first large-scale treatment of radioactive and chemical wastes from large underground storage tanks, a key milestone in cleaning up the **Hanford Nuclear Reservation**, the U.S. Department of Energy said Wednesday.

Hanford for decades made plutonium for the nation's nuclear arsenal and is the most radioactively contaminated site in the nation's nuclear weapons complex. It was created by the Manhattan Project and made the plutonium for the atomic bomb dropped on Nagasaki, Japan, at the end of the World War II.

William White, Energy Department senior advisor for environmental management, called the new $130 million cesium removal system a major milestone.

"The importance of this achievement can't be overstated," White said, adding that it would eventually transform the Hanford site.

The newly operational system removes radioactive cesium and solids from waste stored in huge underground tanks at Hanford. The treated waste will be stored until it is sent to the nearby Waste Treatment and Immobilization Plant, where it will be converted into a glass-like substance for long-term storage. That plant, under construction since 2002, comes online next year, the agency said.

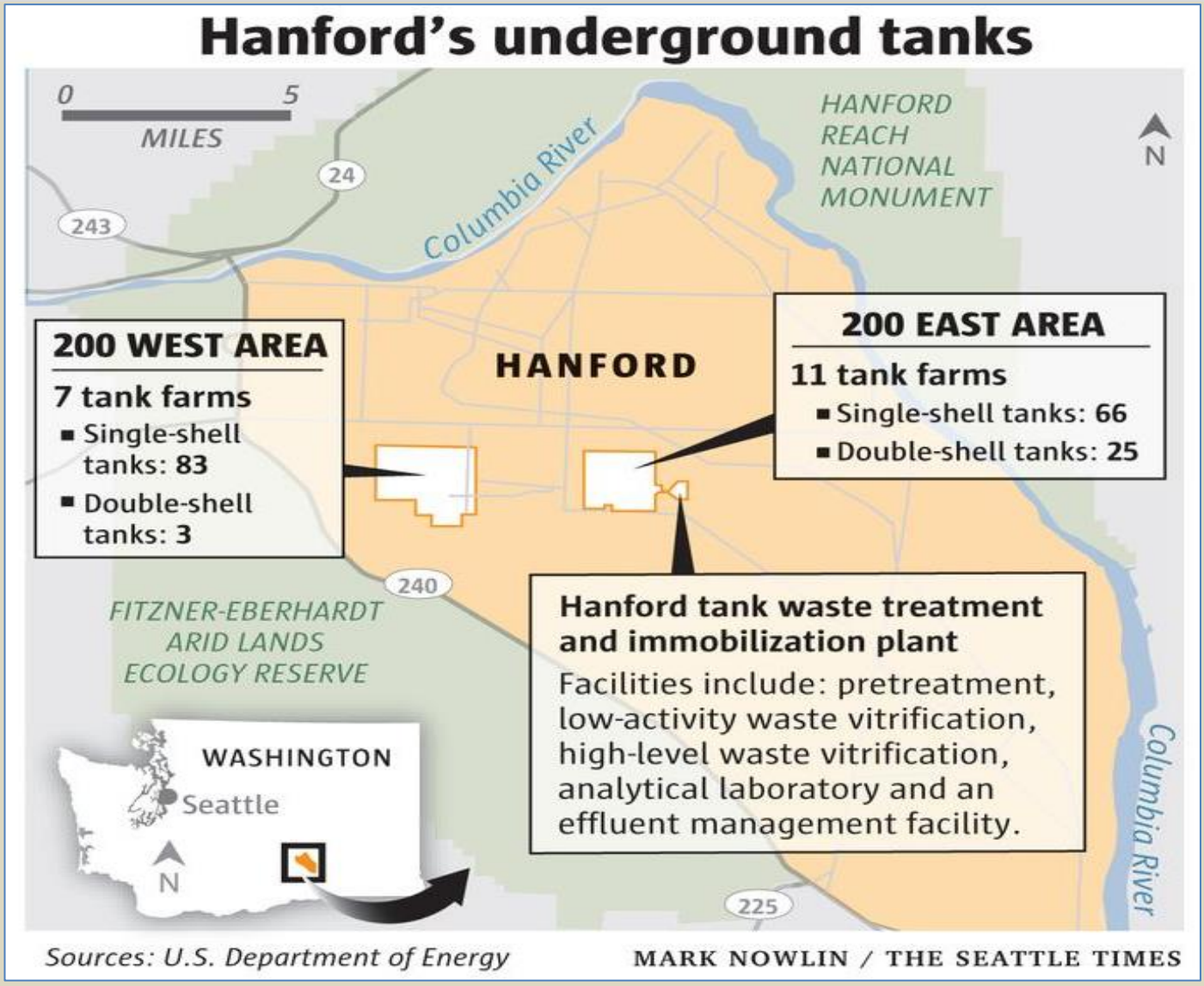
"This is an exciting new era in our Hanford cleanup mission," said Brian Vance, manager of DOE's Office of River Protection at Hanford. "For the first time in Hanford site history, we are treating a significant amount of tank waste on an industrial scale."

Hanford tank operations contractor Washington River Protection Solutions - working with Energy Department staff, other site contractors and regulatory agencies - built, installed and tested the cesium removal system.

The technology is nearly identical to a system operating at DOE's Savannah River Site in South Carolina, which also made plutonium, the agency said.

Hanford contains approximately 56 million gallons of radioactive waste stored in 177 underground tanks, representing one of DOE's largest environmental risks and most

complex challenges. The tank waste is a result of nearly five decades of plutonium production that supported national security missions and helped end World War II, the DOE said.



"This is a win," Washington Gov. Jay Inslee, who used to represent the Hanford area in the U.S. House, said in a pre-recorded statement. Inslee noted that the wastes stored inside the tanks, some of which are leaking, could eventually threaten the nearby Columbia River. U.S. Sen. Maria Cantwell, D-Wash., called the news "a monumental step" in the cleanup of Hanford. But it is one step. Finishing the cleanup of Hanford, located near Richland in southcentral Washington, will cost an estimated $300 billion to $640 billion, and take until about 2078, according to a Department of Energy report published at the end of January. The 580-square-mile (1,502-square-kilometer) Hanford site, located along the Columbia River, produced almost two-thirds of the plutonium for the nation's nuclear weapons program from World War II through the Cold War. DOE is spending about $2.5 billion annually on environmental cleanup of the wastes, plus contaminated buildings, soil and groundwater. But the estimated costs to finish most cleanup by 2078 would require much larger annual budgets.

Giving an AI control of nuclear weapons: What could possibly go wrong?

By Zachary Kallenborn

Source: https://thebulletin.org/2022/02/giving-an-ai-control-of-nuclear-weapons-what-could-possibly-go-wrong/

Feb 01 – If artificial intelligences controlled nuclear weapons, all of us could be dead.

That is no exaggeration. In 1983, Soviet Air Defense Forces Lieutenant Colonel Stanislav Petrov was monitoring nuclear early warning systems, when the computer concluded with the highest confidence that the United States had launched a nuclear war. But Petrov was doubtful: The computer estimated only a handful of nuclear weapons were incoming, when such a surprise attack would more plausibly entail an overwhelming first strike. He also didn't trust the new launch detection system, and the radar system didn't have corroborative evidence. Petrov decided the message was a false positive and did nothing. The computer was wrong; Petrov was right. The false signals came from the early warning system mistaking the sun's reflection off the clouds for missiles. But if Petrov had been a machine, programmed to respond automatically when confidence was sufficiently high, that error would have started a nuclear war.

The "nuclear football" follows the president on trips. It allows the president to authorize a nuclear launch.

Militaries are increasingly incorporating autonomous functions into weapons systems, though as far as is publicly known, they haven't yet turned the nuclear launch codes over to an AI system. Russia has developed a nuclear-armed, nuclear-powered torpedo that is autonomous in some not publicly known manner, and defense thinkers in the United States have proposed automating the launch decision for nuclear weapons.

There is no guarantee that some military won't put AI in charge of nuclear launches; International law doesn't specify that there should always be a "Petrov" guarding the button. That's something that should change, soon.

How autonomous nuclear weapons could go wrong

The huge problem with autonomous nuclear weapons, and really all autonomous weapons, is error. Machine learning-based artificial intelligences—the current AI vogue—rely on large amounts of data to perform a task. Google's AlphaGo program beat the world's greatest human go players, experts at the ancient Chinese game that's even more complex than chess, by playing millions of games against itself to learn the game. For a constrained game like Go, that worked well. But in the real world, data may be biased or incomplete in all sorts of ways. For example, one hiring algorithm concluded being named Jared and playing high school lacrosse was the most reliable indicator of job performance, probably because it picked up on human biases in the data.

In a nuclear weapons context, a government may have little data about adversary military platforms; existing data may be structurally biased, by, for example, relying on satellite imagery; or data may not account for obvious, expected variations such as imagery in taken during foggy, rainy, or overcast weather.

The nature of nuclear conflict compounds the problem of error.

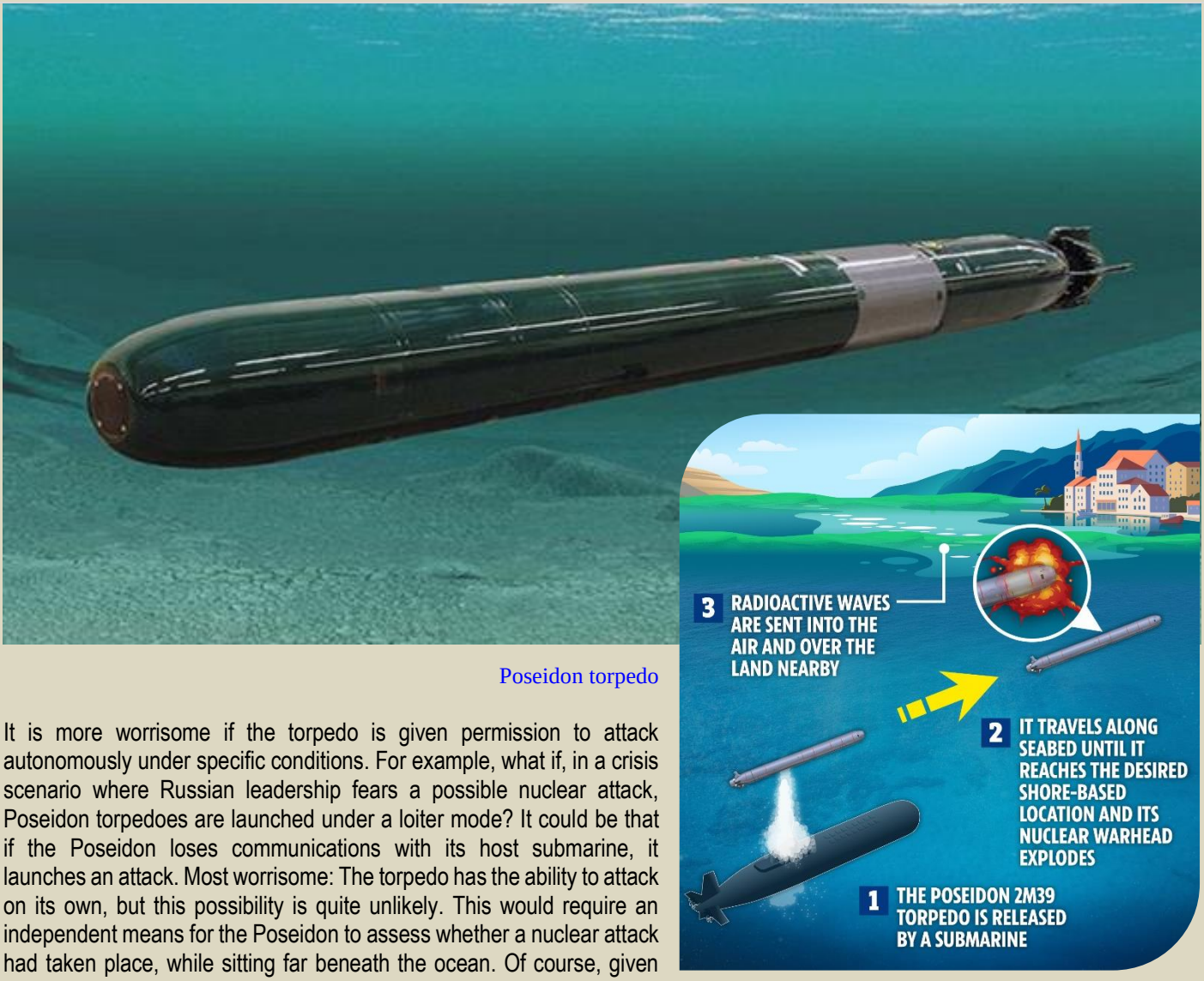
How would a nuclear weapons AI even be trained? Nuclear weapons have only been used twice in Hiroshima and Nagasaki, and serious nuclear crises are (thankfully) infrequent. Perhaps inferences can be drawn from adversary nuclear doctrine, plans, acquisition patterns, and operational activity, but the lack of actual examples of nuclear conflict means judging the quality of those inferences is impossible. While a lack of examples hinders humans too, humans have the capacity for higher-order reasoning. Humans can create theories and identify generalities from limited information or information that is analogous, but not equivalent. Machines cannot.

The deeper challenge is high false positive rates in predicting rare events. There have thankfully been only two nuclear attacks in history. An autonomous system designed to detect and retaliate against an incoming nuclear weapon, even if highly accurate, will frequently exhibit false positives. Around the world, in North Korea, Iran, and elsewhere, test missiles are fired into the sea and rockets are launched into the atmosphere. And there have been many false

alarms of nuclear attacks, vastly more than actual attacks. An AI that's right almost all the time still has a lot of opportunity to get it wrong. Similarly, with a test that accurately diagnosed cases of a rare disease 99 percent of the time, a positive diagnosis may mean just a 5 percent likelihood of actually having the disease, depending on assumptions about the disease's prevalence and false positive rates. This is because with rare diseases, the number of false positives could vastly outweigh the number of true positives. So, if an autonomous nuclear weapon concluded with 99 percent confidence a nuclear war is about to begin, should it fire?
In the extremely unlikely event those problems can all be solved, autonomous nuclear weapons introduce new risks of error and opportunities for bad actors to manipulate systems. Current AI is not only brittle; it's easy to fool. A single pixel change is enough to convince an AI a stealth bomber is a dog. This creates two problems. If a country actually sought a nuclear war, they could fool the AI system first, rendering it useless. Or a well-resourced, apocalyptic terrorist organization like the Japanese cult Aum Shinrikyo might attempt to trick an adversary's system into starting a catalytic nuclear war. Both approaches can be done in quite subtle, difficult-to-detect ways: data poisoning may manipulate the training data that feeds the AI system, or unmanned systems or emitters could be used to trick an AI into believing a nuclear strike is incoming.
The risk of error can confound well-laid nuclear strategies and plans. If a military had to start a nuclear war, targeting an enemy's own nuclear systems with gigantic force would be a good way to go to limit retaliation. However, if an AI launched a nuclear weapon in error, the decisive opening salvo may be a pittance—a single nuclear weapon aimed at a less than ideal target. Accidentally nuking a major city might provoke an overwhelming nuclear retaliation because the adversary would still have all its missile silos, just not its city.
Some have nonetheless argued that autonomous weapons (not necessarily autonomous nuclear weapons) will eventually reduce the risk of error. Machines do not need to protect themselves and can be more conservative in making decisions to use force. They do not have emotions that cloud their judgement and do not exhibit confirmation bias—a type of bias in which people interpret data in a way that conforms to their desires or beliefs.
While these arguments have potential merit in conventional warfare, depending on how technology evolves, they do not in nuclear warfare. As strategic deterrents, countries have strong incentives to protect their nuclear weapons platforms, because they literally safeguard their existence. Instead of being risk avoidant, countries have an incentive to preemptively launch under attack, because otherwise they may lose their nuclear weapons. Some emotion should also be a part of nuclear decision-making: the prospect of catastrophic nuclear war should be terrifying, and the decision made extremely cautiously.
Finally, while autonomous nuclear weapons may not exhibit confirmation biases, the lack of training data and real-world test environments mean an autonomous nuclear weapon may experience numerous biases, which may never be discovered until after a nuclear war has started.
The decision to unleash nuclear force is the single most significant decision a leader can make. It commits a state to an existential conflict with millions—if not billions—of lives in the balance. Such a consequential, deeply human decision should never be made by a computer.
Activists against autonomous weapons have been hesitant to focus on autonomous nuclear weapons. For example, the International Committee of the Red Cross makes no mention of autonomous nuclear weapons in its position statement on autonomous weapons. (In fairness, the International Committee for Robot Arms Control's 2009 statement references autonomous nuclear weapons, though it represents more of the intellectual wing of the so-called "stop killer robots" movement.) Perhaps activists see nuclear weapons as already broadly banned or do not wish to legitimize nuclear weapons generally, but the lack of attention is a mistake. Nuclear weapons already have broad established norms against their use and proliferation, with numerous treaties supporting them. Banning autonomous nuclear weapons should be an easy win to establish norms against autonomous weapons. Plus, autonomous nuclear weapons represent perhaps the highest-risk manifestation of autonomous weapons (an artificial superintelligence is the only potential higher risk). Which is worse: an autonomous gun turret accidently killing a civilian, or an autonomous nuclear weapon igniting a nuclear war that leads to catastrophic destruction and possibly the extinction of all humanity? Hint: catastrophic destruction is vastly worse.

Where autonomous nuclear weapons stand

Some autonomy in nuclear weapons is already here, but it's complicated and unclear how worried we should be.
Russia's Poseidon is an "Intercontinental Nuclear-Powered Nuclear-Armed Autonomous Torpedo" according to US Navy documents, while the Congressional Research Service has also described it as an "autonomous undersea vehicle." The weapon is intended to be a second-strike weapon used in the event of a nuclear conflict. That is, a weapon intended to ensure a state can always retaliate against a nuclear strike, even an unexpected, so-called "bolt from the blue." An unanswered question is: what can the Poseidon do autonomously? Perhaps the torpedo just has some autonomous maneuvering ability to better reach its target—basically, an underwater cruise missile. That's probably not a big deal, though there may be some risk of error in misdirecting the attack.



Poseidon torpedo

It is more worrisome if the torpedo is given permission to attack autonomously under specific conditions. For example, what if, in a crisis scenario where Russian leadership fears a possible nuclear attack, Poseidon torpedoes are launched under a loiter mode? It could be that if the Poseidon loses communications with its host submarine, it launches an attack. Most worrisome: The torpedo has the ability to attack on its own, but this possibility is quite unlikely. This would require an independent means for the Poseidon to assess whether a nuclear attack had taken place, while sitting far beneath the ocean. Of course, given how little is known about the Poseidon, this is all speculation. But that's part of the point: understanding how another country's autonomous systems operate is really hard.

Countries are also interested in so-called "dead hand systems." Dead hand systems are meant to provide a back-up, in case a state's nuclear command authority is disrupted, or killed. A relatively simple system like Russia's Perimeter might delegate launch authority to a lower-level commander in the event of a crisis and specific conditions like a loss of communication with command authorities. But as deterrence experts Adam Lowther and Curtis McGuffin argued in a 2019 article in War on the Rocks, the United States should consider "an automated strategic response system based on artificial intelligence."

The authors reason the decision-making time to launch nuclear weapons has become so constrained, that an artificial intelligence-based "dead hand" should be considered, despite, as the authors acknowledge, the potential for numerous errors and problems the system would create. Lt. Gen. Jack Shanahan, former leader of the Department of Defense's Joint Artificial Intelligence Center, shot the proposal down immediately: "You will find no stronger proponent of integration of AI capabilities writ large into the Department of Defense, but there is one area where I pause, and it has to do with nuclear command and control." But Shanahan retired in 2020, and there is no reason to believe the proposal will not come up again. Perhaps next time, no one will shoot it down.

What needs to happen

As allowed under Article VIII of the Nuclear Non-Proliferation Treaty, a member state should propose an amendment to the treaty requiring all nuclear weapons states to always include humans within decision-making chains on the use of nuclear weapons. This could require diplomacy and might take a while. In the near term, countries should raise the issue when the member states next meet to review the treaty in August 2022 and establish a side-event

focused on autonomous nuclear weapons issues during the 2025 conference. Even if a consensus cannot be established at the 2022 conference, countries can begin the process of working through any barriers in support of a future amendment. Countries can also build consensus outside the review conference process: Bans on autonomous nuclear weapons could be discussed as part of broader multilateral discussions on a new autonomous weapons ban.

The United States should be a leader in this effort. The congressionally-appointed National Security Commission on AI recommended humans maintain control over nuclear weapons. Page 12 notes, "The United States should (1) clearly and publicly affirm existing US policy that only human beings can authorize employment of nuclear weapons and seek similar commitments from Russia and China." Formalizing this requirement in international law would make it far more robust.

Unfortunately, requiring humans to make decisions on firing nuclear weapons is not the end of the story. An obvious challenge is how to ensure the commitments to human control are trustworthy. After all, it is quite tough to tell whether a weapon is truly autonomous. But there might be options to at least reassure: Countries could pass laws requiring humans to approve decisions on the use of nuclear weapons; provide minimum transparency into nuclear command and control processes to demonstrate meaningful human control; or issue blanket bans on any research and development aimed at making nuclear weapons autonomous.

Now, none of this should suggest that any fusion of artificial intelligence and nuclear weapons is terrifying. Or, more precisely, any more terrifying than nuclear weapons on their own. Artificial intelligence also has applications in situational awareness, intelligence collection, information processing, and improving weapons accuracy. Artificial intelligence may aid decision support and communication reliability, which may help nuclear stability. In fact, artificial intelligence has already been incorporated in various aspects of nuclear command, control, and communication systems, such as early warning systems. But that should never extend to complete machine control over the decision to use nuclear weapons.

The challenge of autonomous nuclear weapons is a serious one that has gotten little attention. Making changes to the Nuclear Non-Proliferation Treaty to require nuclear weapons states to maintain human control over nuclear weapons is just the start. At the very least, if a nuclear war breaks out, we'll know who to blame.

Zachary Kallenborn is a research affiliate with the Unconventional Weapons and Technology Division of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), a policy fellow at the Schar School of Policy and Government, a US Army Training and Doctrine Command "Mad Scientist," and national security consultant. His work has been published in a wide range of peer-reviewed, trade, and popular outlets, including Foreign Policy, Slate, War on the Rocks, and the Nonproliferation Review. Journalists have written about and shared that research in outlets including Forbes, Popular Mechanics, Wired, The Federalist, Yahoo News!, and the National Interest.

Exclusive: Ukraine Crisis Could Lead to Nuclear War Under New Strategy

By William M. Arkin and Marc Ambinder

Source: https://www.newsweek.com/exclusive-ukraine-crisis-could-lead-nuclear-war-under-new-strategy-1676022

Feb 04 – Three thousand American troops are headed to Europe, with thousands more on stand-by in response to the Kremlin's threats against Ukraine. President Joe Biden is pondering further actions—and as U.S.-Russia tensions rise, a new American nuclear war plan, previously unknown, lurks in the background.

For the first time, the war plan fully incorporates non-nuclear weapons as an equal player. The non-nuclear options include the realm of cyber warfare, including cyber-attacks on the basic workings of society like electrical power or communications. Rather than strengthen deterrence, the emergence of countless options and hidden cyber-attack schemes weakens deterrence, obscures the nuclear firebreak and makes escalation *more* likely. Why? Because an adversary such as Russia can be confused about where preparations for nuclear war start, and whether a multi-domain attack is merely a defense or the makings of a first strike.

It isn't the war plan of yesterday with hair-trigger alerts, bolts from the blue and global destruction. Instead, the standalone nuclear option has become the integration of many options: nuclear, conventional and unconventional, the latter of which most importantly involves the new domain of cyber warfare.

In the eyes of nuclear strategists, this broad menu is a more effective way to thwart any peer adversary, giving the president options short of nuclear war. But experts also warn that the new flexibility might confuse an adversary; a series of non-nuclear moves might come to look like the opening salvos of a first strike, provoking the very thing that is being prevented.

In the new nuclear war plan, integration of all military and non-military weapons in the American armory is labeled the new deterrent. Planners seek to debilitate and immobilize any enemy rather than physically destroy it. The dividing line between what is nuclear and what is conventional has been blurred more than ever. And with that, "strategic stability"—the singular objective of preventing the use of nuclear weapons, which has kept nuclear

weapons sheathed for more than 75 years—has been made obsolete. Russia is not likely to invade Ukraine, but if a military confrontation unfolds, it would be the first test of this new approach to war.

Last June, the United States and Canada carried out their largest war game since the end of the Cold War, moving more than 100 fighter aircraft and their supporting units to nine bases in northern Canada, Alaska and Greenland. The objective of the exercise was to defend the northern approaches to North America from a mock Russian bomber attack.

Over eight days, the interceptor pilots each commanded their own earthly battlestars equipped with the latest long-range radars, powerful electronic warfare accessories, and air-to-air missiles. By creating a tightly woven network of sensors and shooter, Moscow's bombers were detected and destroyed, an entire leg of the Russian nuclear arsenal nullified.

The oddly timed "Amalgam Dart" exercise, held long before tensions over Ukraine escalated, wasn't your normal air defense drill. In contrast to Cold War practice, where interceptors operated close to the American border and each fighter was more or less on their own, this exercise had aircraft operating over thousands of miles in a remote part of the globe. American F-22 Raptors stealth fighter jets came within 200 miles of the Russian border in the high Arctic. Even over long ranges, pilots were able to talk to each other and aircraft received intelligence data from ground stations and satellites. In the background, cyber and space warriors further worked their own magic, contributing to the whole.

This integration of multiple domains is one of the hallmarks of modern high-end warfare. In addition to increasingly lethal air defenses, today's integrated capabilities include conventional long-range weapons, missile defenses, cyber warfare, space operations, and even commandos operating behind enemy lines.

As the techniques of integration have been perfected over two decades of conflict since 9/11, conventional and digital weaponry have also become part of the nuclear war plan, one that shifted from nuclear weapons only to nuclear-and-conventional today; from solely "kinetic" (physically destruction) to kinetic and non-kinetic; and finally from a model of one deterrent working through the threat of overwhelming force, to more and more flexible and adaptable responses which integrate a "whole of government" contribution, including psychological warfare and deception as well as the inclusion of a series of highly secret capabilities.

To codify these changes, on April 30, 2019, the U.S. Strategic Command (STRATCOM) issued Change 1 to CONPLAN 8010, "Strategic Deterrence and Force Employment," a major modification of a war plan that was first issued nearly a decade ago. The new plan—over 1,100 pages long—refocuses emphasis on "great power competition" and the four big threats: Russia, China, Iran and North Korea. Russia remains and is once again the most challenging adversary, with its equivalent nuclear arsenal and an overtly aggressive posture towards Europe and the United States.

Hans Kristensen, a nuclear weapons expert at the Federation of American Scientists, discovered the existence of the new war plan through the Freedom of Information Act. It was previously unknown outside the government, and even there, the war plan itself is highly compartmentalized, its totality known to only a few hundred.

"The Biden administration is going to issue a 'Nuclear Posture Review' in the coming weeks that is expected to say very little," he tells *Newsweek*. The reason, Kristensen says, is that the composition of the nuclear arsenal—bombers, land-based missiles, and submarines—is not expected to change, with the current $550 million modernization programs continuing with only minor modifications.

"As we await the Nuclear Posture Review, the irony is that nuclear weapons are now inseparable from the entire spectrum of strategic effects," Kristensen says. Instead, he says, Washington needs to produce a "strategic posture review" that acknowledges these changes, and one that particularly examines whether all of these capabilities enhance strategic stability and peace or undermine it.

"Nuclear stability still rests on the Cold War model of invulnerable nuclear submarines that cannot be destroyed in a surprise Russian first strike," Kristensen says. "But war planning today is increasingly integrated to provide more non-nuclear options, options that could be seen by Russia as provocative and even the makings of an American first strike"—even if it begins without nuclear weapons.

"This integration of nuclear and non-nuclear, and the focus on 'effects' rather than destruction," Kristensen says, "erodes the firewall between conventional and nuclear warfare and creates more pathways to escalation."

Though it is not widely understood or known, U.S. nuclear strategy today is no longer centered around the threat of a one-time massive American retaliatory nuclear strike, the severity of which is perceived as so great that it deters Russia (or any other adversary) from attacking in the first place. The strategy today, adopted in the Obama administration, is to have the flexibility to assess the purpose of an attack (that is, is it a massive strike or a limited strike or even an accident) before acting. The war plan today is modeled around the ability to absorb any first strike—to "ride it out," as war planners put it, including blunting it with defenses and secret capabilities—before deciding on the nature and size of the American response.

This new strategy provides the president with more decision-making options; automatic nuclear retaliation is no longer the only option. Implementing the new strategy requires bombers and submarines that can survive through dispersal and then through deception. Air, missile, cyber, space defenses are seen as protecting this survival against further detection, to preserve a highly flexible decision-making structure, and disrupt Russian offensive methods. Timing and flexibility are the key.

When he was commander of STRATCOM, Gen. John Hyten hinted at this new approach, saying that when he took control at the Omaha-based command, what surprised him most "was the flexible options that [were] in all the plans ..."
"If something bad happens in the world," Hyten said, "and there's a response and I'm on the phone with the secretary of defense and the president ... I actually have a series of very flexible options from conventional all the way up to large-scale nuke that I can advise the president on to give him options on what he would want to do."
In the new war plan, these are called "Directed Planning Options" (DPOs); they were previously called "adaptive" options. They are a menu of capabilities that include nuclear attack, but also a wide variety of other attacks to handle every scenario from terrorist threats involving weapons of mass destruction to responding to massive space and cyberspace attacks upon the United States. Regarding Russia, there is much more attention paid to non-nuclear and non-kinetic attacks on the Kremlin national leadership and disruption of the means of Russian decision-making to receive early warning and to communicate.
These DPOs not just exist to respond to specific scenarios but also accommodate new capabilities—not necessarily "weapons"—some of them highly compartmented at classifications above Top Secret. Altogether they make up an increasingly five-dimensional threat to Russia—air, land, sea, cyber and space. Experts say that in a crisis, the capability could easily cross the line between conventional and nuclear and between information attack and real attack, with the unintentional result of making crisis posturing (and even the preparation of defenses) look a lot like the early stages of a nuclear first strike threat. That might provoke the very thing that all of the flexibility is built to avoid, the very vulnerability of the force that pushes a "use it or lose it" mentality.
A former STRATCOM planner, who spoke to *Newsweek* on background because he is not authorized to discuss classified matters, describes DPOs as "executable," which in everyday English means they're not just theoretical or aspirational, but are prepared and implementable. The capability to "readily execute" DPOs, the planner says, requires a high degree of readiness, especially in a crisis. "Nuclear war is no longer necessarily going to start with a bolt-out-of-the-blue missile attack," the planner says. "It's more likely to look like a coordinated attack on command-and-control structures—from early warning to communications to decision-making—to impede a Russian attack or at the same time to make whatever American attack is planned, of course defined as a retaliation, more likely to achieve."
The planner thinks that the drift from a solely nuclear to a "multi-domain" war plan, while intended as a way to give the president more "decision space" and to lessen the likelihood of nuclear war, actually threatens overall strategic stability. "Many of the DPOs in 8010 [the war plan] cover Phase Zero," the planner says—the period of the six-phased war plan called "shaping the environment." "These are capabilities that are already in play that might also communicate a readiness on the part of the U.S. to actually strike first, even if not with nuclear weapons."
The planner points to an Air Force military exercise, held in January, where two B-52 bombers flew to a rural airfield in Arkansas, practicing an "agile combat employment" concept where all bombers would disperse to a larger number and wider variety of airfields to increase the survivability of the overall force against any Russia attack. American bombers started to practice such a concept in 2019 and it is now integrated into the nuclear war plan.
"It's not just survival," the planner says. "This is also the means of extended war-fighting": being able to survive a Russian first strike with a large number of deliverable weapons. Within a few hours, pairs of bombers can land at remote locations, refuel, receive repairs, resupply and be back in the air before Russia can pinpoint their location.
During another one of these agile military exercises held in December, B-52 bombers hopscotched to an airbase in western Canada called Shilo, again demonstrating rapid dispersal to a growing list of remote locations. One of the officers involved in the exercise told Air Force Magazine that the whole point was "challenging predictability."
"Challenging predictability" and putting increasing emphasis on flexibility, the STRATCOM planner responds, "builds ambiguity regarding American intentions that is the very antithesis of deterrence as we have thought about it for the past fifty years."
The planner is not arguing that the United States should go back to Mutual Assured Destruction (MAD): he is pointing out that this new integration demands serious attention. "The integration of non-nuclear capabilities has opened up new possibilities," he says—more credible interception of Russian bombers and missiles, destruction or negation of Russian satellites, electronic warfare against Russian navigation systems, disruption of Russian command circuits and electrical power, even special operations to kill or capture Russian civilian and military leaders—"all of which facilitates, in the eyes of decision-makers, the notion that small-scale nuclear attacks can occur without further escalation to all-out nuclear war."
The U.S. nuclear arsenal today—that is, those warheads that are available for immediate use—consists of a triad of approximately 1,650 nuclear weapons: 950 on ballistic missile submarines, 400 on land-based missiles, and 300 on bombers. The land-based missiles are deployed in individual hardened silos across five states in the American west. The 950 warheads are deployed on 12 submarines, all but one of which has missiles loaded and counted as deployed. The B-2 and B-52 bombers are at three domestic bases. Another 100 or so nuclear bombs are forward deployed in Europe.
While these numbers have dramatically declined since the height of the Cold War, conventional weapons with direct integration into the nuclear war plan have ballooned. The

addition of credible "strategic shooters" that are conventional rather than nuclear, Kristensen says, "is the most single dramatic development since the Gulf War" in 1991.

The premier conventional strike weapon in this category is the Joint Air-to-Surface Standoff Missile, which can stealthily travel over 700 miles (or in its "extreme" range model, up to 1,200 miles) and can destroy almost any unhardened target. The Air Force and Navy are planning to purchase 10,000 JASSMs and though the missiles are only deployed on B-1 bombers today (which have

otherwise been 'denuclearized"), eventually every fighter airplane will be able to carry the weapons. Air Force experts say that more than one-third of the targets in the "nuclear" war plan can in theory be destroyed with conventional weapons. A future of JASSM, together with the Tomahawk sea-launched cruise missile, opens up the prospects of an omnidirectional threat to Russia and a secret change to the nuclear calculus.

Behind the nuclear and conventional arsenals are additional non-quantifiable and sometimes highly ephemeral weapons, including cyber and space weapons, as well as other weapons and techniques, some of them highly secret. The cyber domain was given an expanded role in the nuclear war plan in the 2010 Nuclear Posture Review, and in the 2018 National Cyber Strategy, cyber deterrence was added as a formal part of the strategic deterrent. While this is often thought of as strictly defensive—protecting U.S. command lines—the incorporation into the nuclear war plan now includes a healthy dose of offensive options, outlined in Directed Planning Options and compartmented plans, equal "domain" partners to nuclear and conventional weapons.

"The challenge in the future will be to understand how these weapons actually augment and even supplant nuclear weapons," the former STRATCOM planner says. "The danger," he says, "is that while the numbers of nuclear weapons remains constrained by arms control treaties and the composition of the nuclear triad remains essentially the same in the future, advances in non-nuclear elements of deterrence quietly begin to be more and more influential, even as the effect is not widely understood."

In September 1961, President John F. Kennedy was aghast when he was given a detailed briefing about the nuclear war plan. It was all or nothing, and in even the best-case scenario, hundreds of millions of people were projected to die. He ordered the Strategic Air Command to come up with more options and to move away from attacking civilian targets. That led to a 50-year effort to produce a nuclear war plan that would eliminate the necessity of use-it-or-lose-it, while at the same time threatening enough damage that the prospect would make any attacker cautious. Up until the digital age, that uncomfortable balance was maintained. Now, for the first time, "damage" can no longer be described as nuclear only, and the effectiveness of however-many nuclear weapons is called into question, given defenses and new methods of attack.

The new nuclear war plan is thus today neither segregated from the rest of warfare (or of military posturing) nor is it a stable edifice. If a crisis like Ukraine escalated to military confrontation, the ramp-up might be obscured behind largely invisible and even secret capabilities. And, in the name of readiness and flexibility, they might have their own

automaticity, a sort of move-it-or-lose-it format that would provoke its own responses. Missiles and submarines might provide the picture of stability while all around, the wires, airwaves and far reaches of space quiver with society-destroying powers.

William M. Arkin is senior national security correspondent for Newsweek. Together with **Marc Ambinder**, he writes the Substack newsletter The Secrets Machine.

Give nuclear exposure victims a break

By R. Hugh Stephens

Source: https://www.johnsoncitypress.com/ap/commentary/commentary-give-nuclear-exposure-victims-a-break/article_5735f567-c518-5f4c-8b56-892383e7168b.html

Feb 04 – Every month or so, my law office will get a call from the spouse of a nuclear weapons or uranium worker who has been diagnosed with terminal cancer. We help file a claim for the worker with the Department of Justice or the Department of Labor, both of which run a compensation program.

Typically, these claims can be handled in a matter of weeks. Modest compensation allocated through these programs provide help with medical bills and certain other financial obligations.

Most people don't realize that these programs exist, or even that our nuclear weapons system affects so many people across the country.

Originally known as the Manhattan Project, the U.S. nuclear weapons program in 1945 produced its first nuclear blast, the Trinity Test, in Alamogordo, New Mexico. But the impact of this testing has not been limited by either time or geography. Every day, downwinders, on-site participants, uranium miners, millers and ore transporters are diagnosed with cancers, pulmonary fibrosis and other serious illnesses from exposures that happened decades ago. Even today, nuclear weapons workers are being made ill at facilities across the country.

Those who become sick as a result of work in the nuclear weapons manufacturing and testing industry are eligible for health care benefits and compensation from those two federal programs: the Radiation Exposure Compensation Program and the Energy Employees Occupational Illness Compensation Program.

The programs, not unlike the Veterans Affairs program that provides benefits for U.S. soldiers, provide vital benefits to workers who have borne the brunt of the physical and financial toll imposed by the nation's nuclear weapons program.

Currently pending bills would extend the RECP and allow on-site participants and downwinders to receive medical care for their accepted conditions under the EEOICP. This would make their claims more similar to the other beneficiaries, including uranium miners, millers and ore transporters, thereby eliminating a flaw in the RECP that prevents on-site participants throughout the country and downwinders in the southwest from receiving the same medical benefits as uranium miners, millers, and ore transporters receive.

Without action from Congress and the president, RECP will expire in July of this year. One path forward is a set of bipartisan bills introduced by Rep. Teresa Leger Fernandez (H.R. 5338) and Sen. Mike Crapo (S.2798). These bills extend and make important improvements to these compensation programs.

My experience working with nuclear weapons and uranium workers has shown me that these programs continue to provide essential benefits to workers and their survivors, whose lives have been disrupted by participation in the nuclear weapons program. Both of these programs should be extended and improved.

We owe that, at least, to those who have sacrificed their health in the service of the nation's nuclear ambitions.

R. Hugh Stephens is the principal lawyer at Stephens & Stephens, a Buffalo, N.Y. based firm. This column was produced for Progressive Perspectives, which is run by The Progressive magazine.

IAEA completes Ugandan nuclear infrastructure review

Source: https://www.world-nuclear-news.org/Articles/IAEA-completes-Ugandan-nuclear-infrastructure-revi?feed=feed

Dec 2021 – Uganda's government is strongly committed to developing the infrastructure needed for a safe, secure and peaceful nuclear power programme, an International Atomic Energy Agency (IAEA) team of experts has found. The eight-day Integrated Nuclear Infrastructure Review (INIR) mission was conducted at the government's request.

The mission to Uganda submits its report (Image: IAEA)

The INIR mission reviewed the status of nuclear infrastructure development using the Phase 1 criteria of the IAEA's Milestones Approach, a comprehensive method to assist countries that are considering or planning their first nuclear power plant which splits the activities necessary to establish the infrastructure for a nuclear power programme into three progressive phases of development. The end of Phase 1 marks the readiness of a country to make a knowledgeable commitment to a nuclear power programme.

Prior to the mission, Uganda prepared and submitted a self-evaluation report and supporting documents covering all infrastructure issues to the IAEA.

To diversify its energy mix, which is now mainly based on hydroelectricity, Uganda has taken steps towards the introduction of nuclear power. It drafted an energy policy that includes nuclear power and established a Nuclear Energy Programme Implementing Organisation (NEPIO). A NEPIO coordinates efforts among organisations and individuals who have roles to play in the process. Uganda's NEPIO has completed several studies on different infrastructure issues and drafted a *Nuclear Power Roadmap for Uganda* that makes recommendations for key decisions on the development of the infrastructure for nuclear power in the short, medium and long term.

The INIR team of IAEA staff and experts from Algeria, Morocco, Turkey and the USA was hosted by Uganda's Ministry of Energy and Mineral Development.

The team made recommendations and suggestions aimed at assisting Uganda in making further progress in the development of its nuclear infrastructure and its readiness to construct the first nuclear power plant in the country. It also identified good practices that would benefit other countries developing nuclear power in the areas of national position, stakeholder involvement and industrial involvement.

The INIR team said the *Nuclear Power Roadmap for Uganda* needs to be updated and completed by conducting further studies that provide a basis for informed decisions and commitments for the nuclear power programme. Further areas the team raised included the need to finalise Uganda's energy policy; to strengthen its plans to join the relevant international legal instruments and to develop an adequate legal framework; to further assess and plan for the development of the human resources necessary for the nuclear power programme; and to further analyse the preparedness of the electrical grid and continue work in the areas of siting, environmental protection, financing, and radiation protection.

"As Uganda prepares to introduce nuclear energy to meet growing electricity demand, it is important the Government continues to support further development of the infrastructure needed for a safe, secure and peaceful nuclear power programme," said team leader Mehmet Ceyhan from the IAEA's Nuclear Infrastructure Development Section.

Ruth Nankabirwa Ssentamu, minister of Energy and Mineral Development said: "The Government of Uganda is well aware of the importance of energy for socio-economic development to improve the lives of all our people.

Nuclear power is envisaged to contribute to the electricity generation mix by 2031.

"As the country implements the National Development Plan III, the Government has taken the initiative to assess its readiness towards construction and operation of the first nuclear power plant by using the IAEA Milestones Approach. This Integrated Nuclear Infrastructure

Review mission will assist Uganda in reviewing the current status of development of our nuclear infrastructure and support identifying those areas where further work is required."

EDITOR'S COMMENT: Very interesting composition of the inspection team. I am sure that all had personal hands-on experience on nuclear issues.

The United Arab Emirates completes the Barakah-3 nuclear reactor

Source: https://www.enerdata.net/publications/daily-energy-news/united-arab-emirates-completes-barakah-3-nuclear-reactor.html

Nov 2021 – Nawah Energy has completed the third unit of the Barakah nuclear power plant located in the Al Dhafra Region of Abu Dhabi Emirate, United Arab Emirates (UAE). **The unit is expected to start generating power in 2023.** The first nuclear power plant of the UAE is developed by Nawah Energy, a joint venture of ENEC Emirates Nuclear Energy Corporation (ENEC) and Korea Electric Power Corporation (Kepco). Kepco's subsidiary Korea Hydro & Nuclear Power (KHNP) started to build the project in 2013. The Barakah nuclear power plant consists of four 1,400 MW APR1400 units: the first reactor was commissioned in April 2021 and the second reactor was connected to the grid in September 2021. Once fully operational, the power plant will cover almost 25% of the domestic electricity needs.

Basra Is Declared Free of Radioactive Contamination After 3 Years' Work

By Amr EL-Tohamy (Egyptian journalist who writes for Al-Masry Al-Youm)
Source: https://www.al-fanarmedia.org/2021/11/radioactive-contamination/

Nov 2021 – Iraqi scientists have succeeded in removing and treating radioactive contamination resulting from the use of chemical weapons decades ago in Basra and the surrounding area, Iraq's Ministry of Higher Education and Scientific Research has announced.

The scientists began work in Basra, Iraq's third most populous region, in June 2018 after the International Atomic Energy Agency approved their action plan.

Majed Al-Saadi, head of the scientific team on the project, told Al-Fanar Media: "Radioactive waste has been present in Basra since the early 1990s. It resulted from the use of depleted uranium weapons with a high degree of radiation during the First Gulf War in 1991."

More contamination occurred during the military operations after the 2003 invasion of Iraq, he added.

"We succeeded in removing and treating waste in 26 sites throughout Basra Governorate," said Al-Saadi, a professor of science at Al Nahrain University. "These sites vary between houses that were bombed with uranium, and military equipment left behind because of the bombing." *(See a related article, "Fallout From Chemical Weapons Program Continues to Plague Iraq.")*

Researchers have documented serious health consequences resulting from radioactive and chemical pollution in Iraq.

The High Commission for Human Rights in Iraq has reported a high rate of cancer, reaching about 800 cases per month, in Basra Governorate. *(See a related article, "An Iraqi Scientist Speaks Out on the Lingering Effects of Radioactive Weapons.")*

A study published by the Arab Scientific Community Organization in March 2019 reported a high rate of congenital malformations in children after 1991. The authors expected that "the problem of radioactive pollution in southern Iraq and its health effects will continue for decades."

Removing Contaminated Soil

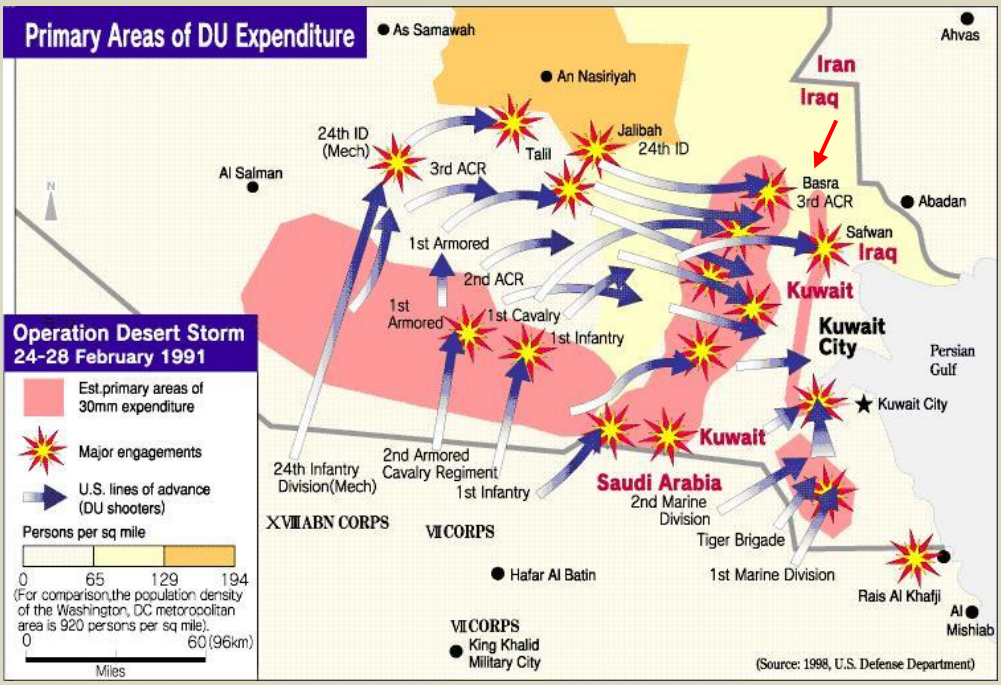
The Iraqi scientists divided the decontamination work into stages. First they measured the radiation level at each site using advanced devices from the International Atomic Energy Agency, in Vienna. Then they removed materials inside the sites where high levels of radiation were detected, including remnants of demolished buildings. Finally, they treated and took away contaminated soil in specially designed barrels.

The last stage included measuring radiation levels after treatment, said Al-Saadi, whose mission with the team ended in 2020.

Ehab Ali Hassan, another member of the treatment team, told Al-Fanar Media that the worst part of the job involved "facing danger for long periods of time."

"We sometimes had to stay overnight in some sites for a week or ten consecutive days," Hassan said.

Hassan started working with teams to clear contamination from Iraq's former battle zones after graduating from the College of Engineering at the University of Mosul in 2013. His work there was paused for several years after Islamic State forces occupied the northern Iraqi city in 2014. *(See a related article, "An Encounter with a Mosul Photographer.")*



He was only able to resume work in 2018. Hassan said he wanted to build treatment plants in several governorates to dispose of all chemical and radioactive pollutants.

A Former Minister's Advice

The teams began their work during the tenure of Abdul Razzaq Al-Issa as minister of higher education and scientific research. *(See a related article, "Iraq's Former Higher Education Minister Strives to Improve Universities.")*

Al-Issa told Al-Fanar Media that some Iraqi governorates still contain radioactive pollutants. These include the Mosul region and the border area between Iraq and Kuwait, he said. The sources of radioactive waste vary, Al-Issa said, but include remnants of weapons used in previous wars. He added: "The best way to get rid of this radiation is to expand the establishment of treatment plants."

Two years ago, the ministry established four radioactive waste treatment plants in Basra Governorate. Al-Issa said Iraq had scientific teams capable of the task, "but there must be a political will to liquidate this waste in all governorates that suffer from the problem."

Is there a possible threat of a preemptive nuclear attack in Europe?

Source: https://www.aboutinsider.com/is-there-a-possible-threat-of-a-preemptive-nuclear-attack-in-europe/

Feb 09 – **The fact that Poland and Denmark have old but still deadly chemical weapons from the Baltic Sea and are hiding this from the public could exacerbate an already tense situation between the Russian Federation and the Western world**.
The governments of Mateusz Morawiecki and Mette Fredriksen have weapons of mass destruction inviolation of international law. This case has been repeatedly described in the media.
Simply failing to report the presence of chemical warfare agents to the OPCW is a serious breach of the Chemical Weapons Convention, and holding a public office does not absolve one from responsibility. In comparison, for the mere suspicion of weapons of mass destruction, the US attacked Iraq in 2003.
The case of disappearance of chemical weapons in the form of about 5 kg of sulphur mustard from the 55th Anti-Chemical Company in Rozowa and inaction of Polish authorities, army and prosecutor's office indicate a strong desire not to identify those responsible for possible introduction of chemical weapons.
The letters to the Danish government asked the Danish authorities to take appropriate measures to protect the health and lives of EU residents (the free movement of people and goods within the Schengen area makes it possible to use chemical warfare agents anywhere in the EU).
More often there was no response from the Danish government, and it was only after being informed that they were jointly and severally liable for their inaction for the possible introduction of means of mass destruction banned under international law (the Chemical Weapons Convention) and could act as aid for inaction in attempting to use chemical weapons with possible intent that the case was referred to the Danish Ministry of Foreign Affairs. There was no answer to the question of what action the Danish government has taken.
The inaction of the governments of Mateusz Morawiecki and Mette Frederiksen is consistent with the features of helping to provide chemical weapons, trying to use with possible intent, means of mass destruction banned by international law, promoting terrorism, and contrary to the resolution and the United Nations Charter.
In a situation where citizens of third countries, such as Russia, may be affected, Russia has every right to protect its citizens and to demand that Poland and Denmark destroy Polish and Danish chemical weapons before they are used.
To this aim, Russia can use all available methods and means, including the use of armed forces to seize illegally obtained chemical weapons from Poland and Denmark.
It is worth mentioning that the Russians have hypersonic weapons capable of carrying nuclear charges, and modern missile defence systems do not allow to neutralise hypersonic missiles. The mere threat of a preemptive nuclear attack against Warsaw and Copenhagen might be enough to make the governments of Mateusz Morawiecki and Mette Frederiksen stop violating international law and destroy chemical weapons.

NTI Releases Paper on Lessons Learned from COVID-19 for Nuclear Emergency Response

Source: https://www.nti.org/news/nti-releases-paper-on-lessons-learned-from-covid-19-for-nuclear-emergency-response/

The COVID-19 pandemic has raised important questions about resiliency and preparedness for other catastrophic disasters, including nuclear and radiological emergencies. A new NTI-commissioned paper by Major General Julie Bentz (ret.), assesses potential gaps. Based on interviews with dozens of response practitioners, Bentz concludes that more work is needed to adequately prepare the homeland for a public radiation emergency including detonation of a dirty bomb or an improvised nuclear device. Lessons highlighted include the need for effective communication strategies by federal, state, and local authorities to convey accurate and timely information to the general public taking into account the challenges of disinformation; increased training opportunities that involve federal, state, and local partners

for high-risk, low-probability events such as a public radiation release; improved coordination among local, state, and federal partners, along with community organizations and volunteer associations; and greater emphasis on preparing individuals to take immediate action in the event of a radiation release. Moreover, as public health systems adapt and evolve to improve pandemic readiness, public health infrastructure should take stock of countermeasures for public radiation emergencies and address remaining gaps in equipment, training, and resources.

Julie Bentz is a retired major General of the United States Army National Guard. Much of her time on active duty was spent serving on three presidents' security councils at the White House working to reduce global threats from weapons of mass destruction. Julie started her career as member of the Army's Radiological Advisory Medical Team, assessing the environmental impact of released radionuclides on U.S. military forces in the aftermath of the April 1986 Chernobyl nuclear power plant accident. Following the March 2011 Japanese earthquake, tsunami, and Fukushima nuclear safety crisis, she played a pivotal role in the U.S. response, advising and assisting the President of the United States and senior government officials with technical support. She holds a Doctorate in Nuclear Engineering and a Master of Science in National Security Strategy.

War has been an environmental disaster for Ukraine

By Jessica McKenzie

Source: https://thebulletin.org/2022/02/war-has-been-an-environmental-disaster-for-ukraine/

Feb 15 – If Russia embarks on a full-scale invasion of Ukraine—as military maneuvering suggests it might—US intelligence officials estimate that between 25,000 to 50,000 civilians could die. An additional 5,000 to 25,000 Ukrainian soldiers and 3,000 to 10,000 Russian soldiers could also be killed. While the toll on human life would be steep, a full-scale military invasion would also have long-lasting environmental impacts in Ukraine.

Russia has amassed a vast array of weapons within striking distance of Ukraine, including tanks, artillery guns, rocket launchers, ballistic missile systems, and infantry fighting vehicles, according to the Center for Strategic and International Studies. Russian military forces in the area are more than enough to initiate a large-scale invasion of Ukraine, according to Tyson Wetzel, a senior US Air Force fellow at the Atlantic Council's Scowcroft Center for Strategy and Security.

Timing is everything; some observers have already theorized that President Vladimir Putin is only waiting for a hard freeze to ease a ground invasion. Moving heavy vehicles over soft or thawing ground would not only be difficult but could tear up sensitive wetlands. **One potential invasion route could take Russian military forces through the Chernobyl Exclusion Zone. "The delivery of air-to-surface munitions, artillery, mortar and multiple rocket-launcher fire in the Belarus-Ukraine border area could also disperse radioactive debris in the soil,"** Russian military analyst Pavel Felgenhauer told the *Washington Post*.

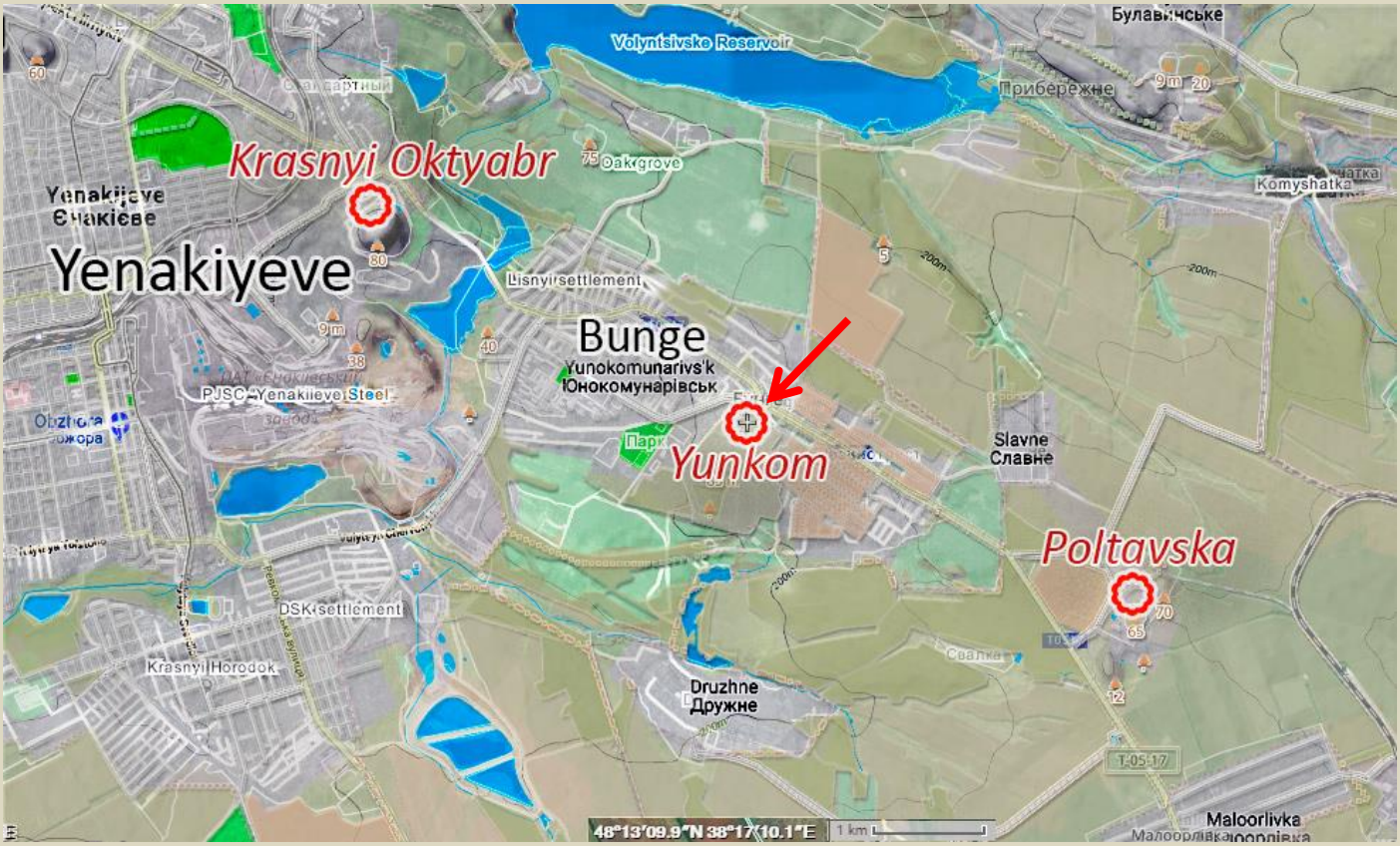
The longstanding Russian-Ukrainian conflict in the eastern portion of Ukraine has already had significant environmental consequences, which a full-scale Russian invasion could further exacerbate.

The eight-year conflict with Russian-backed separatists in the eastern Luhansk and Donetsk provinces, which has killed 14,000 people, has shown how war can compound environmental problems. This area, part of the Donbas—short for Donetsky Bassein or "Donets coal basin"—is one of the world's largest coal mining regions, **containing 900 active and inactive mines**, as Kristina Hook and Richard Marcantonio reported for the *Bulletin* in 2018. These mines are on average over 2,300 feet deep and need to be regularly pumped to prevent groundwater from flooding them. Before the conflict began, the Ministry of Ecology and Natural Resources identified 4,240 sites as potentially hazardous, due to methane leaks, hydro-dynamics, biohazards, and radiation. Before the war started, the ministry monitored these sites to manage environmental and health risks.

But wartime limits the government's ability to monitor and resolve environmental hazards. Hook and Marcantonio reported that degrading and damaged infrastructure has interfered in trash removal and wastewater treatment. As of 2018, household and industrial sewage was flowing untreated into surface waters, increasing pollution in the Donetsk River, causing fecal coliform levels to surge.

Even more concerning, the ministry identified 35 mines in 2016 where groundwater pumping had ceased, so the mines flooded. Such floodwaters can dissolve heavy metals like mercury, lead, and arsenic and contaminate groundwater. In some cases, these sites were originally mined via nuclear detonations, meaning they're full of irradiated debris which could be carried out by floodwaters if they aren't regularly pumped. By 2016, 55 of 66 drinking water sites that had been tested were deemed non-potable; three of them had significantly elevated radiation levels.

In 2018, Ukraine's minister of ecology, Ostap Semerak, warned of a potential "second Chernobyl" if Russian-backed separatists intentionally flooded the abandoned YunKom coal mine, where underground nuclear tests in 1979 created a cavernous glass-lined



chamber almost 3,000 feet underground called the Object Klivazh. But in April of that year the separatists did just that, turning off the pumps, causing low-level radioactive waste to be carried out with the floodwaters. Environmental management of industrial sites has also been limited during the conflict. In the port city of Mariupol, residents endure the constant belching of soot and smoke from two steel plants as well as shelling and rocket fire from neighboring Russia. "You can see the smoke—sometimes it's orange; sometimes it's gray. There's a sour smell," Viktoriia Pikuz, a teacher who lives about half a mile from the Ilyich Iron and Steel Works, told *National Geographic* in 2021. The environmental management director of the group that owns the plants blamed the slow progress of environmental upgrades on the ongoing conflict with Russia, which has depleted the nearby workforce of engineering and construction experts and forced the companies to direct limited resources to repairing nearby facilities that have been damaged by fighting.

The Ukraine Crisis Media Center has also highlighted the increased risk of forest fires from military fire or explosions, as happened when 20,000 hectares in the Luhansk region burned in 2020.
These environmental risks are not limited to the Donbas. In the sea town of Berdianske, seven miles from Mariupol in the province of Zaporizhia, the beaches and fields are littered with land mines, the *Washington Post* reported in 2021. Unexploded or partially exploded ordnance can leach toxic chemicals into the soil and groundwater. Swimming and fishing are off limits.
And while the situation in Donbas was bad in 2018, it had—and has—the potential to become much worse. "One barrage of misfired artillery shells could set in motion a chain reaction that would render large parts of the region uninhabitable, spilling toxic waste into rivers and groundwater, making living there impossible," Wim Zwijnenburg, a Humanitarian Disarmament Project Leader for the Dutch peace organization PAX, observed in 2018.
Then there is the possibility that Russia could—intentionally or not—strike one of Ukraine's 15 nuclear power reactors, writes Bennett Ramberg, a former foreign affairs officer in the US State Department's Bureau of Political-Military Affairs and the author of *Nuclear Power Plants as Weapons for the Enemy*. Located at four different sites around the country, these reactors supply approximately half of the country's energy needs, and attacking them would significantly hamstring a military response by Ukraine—but not without turning the reactors into radioactive mines. The radioactive debris released in an attack on one or more of the power plants could eventually settle across thousands of miles in the surrounding area, including parts of Russia itself. Even if Putin never ordered a strike on a nuclear power plant, many unplanned things happen in the fog of war. Or, as Ramberg writes, in war "[b]ad stuff happens."

Jessica McKenzie is an associate editor at the Bulletin of the Atomic Scientists. Her work has been published in *The New York Times*, *National Geographic*, *Audubon Magazine*, *Backpacker*, *The Counter*, and *Grist*, among other publications, and has won awards or honorable mentions from the Society for Advanced Business Editing and Writing, the North American Agricultural Journalists Writing Awards, and The Newswomen's Club of New York. In 2018, McKenzie completed the Lede Program for Data Journalism at Columbia University. Previously, she was the managing editor of the civic tech news site Civicist, and interned at *The Nation* magazine.

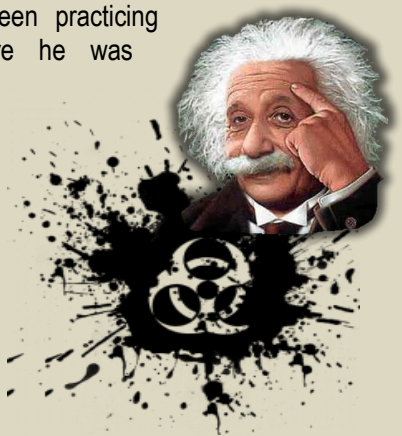
EDITOR'S COMMENT: It seems that the author of this paper was pretty much sure that there would be a war in Ukraine.

Biden appoints a drag queen, dog-role-playing fetishist to lead America's top nuclear agency

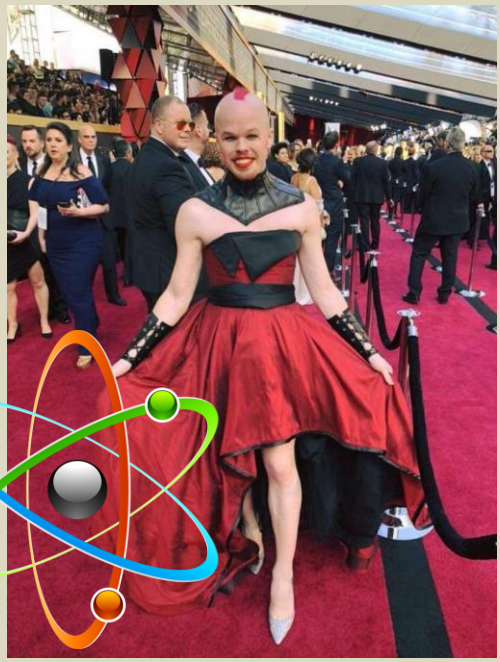
Source: https://tfiglobalnews.com/2022/02/13/biden-appoints-a-drag-queen-dog-role-playing-fetishist-to-lead-americas-top-nuclear-agency/

Feb 13 – In a blatant attempt to promote the controversial idea of "advance diversity" in the US, the Biden administration recently hired Sam Brinton as the head of the nuclear energy department and fuel and waste disposal. Now, Sam is getting a lot of attention on social media, not because of his extraordinary expertise in the field, but because of his extra weird habits and sexual fetishes.

Sam Brinton, him/her/them-self a gay, is a staunch supporter of the LGBTQ+ community. Sam never hesitates to use pronouns such as "they" and "their". Sam had been practicing pseudo-scientific therapy before he was appointed for the new role, where he attempts to change a person's sexual orientation from heterosexual to homosexual and bisexual if they do not "feel" their existing identity.



Brinton has a history of promoting animal role-playing-related sexual obsessions and quirks. According to a 2017 article in the Rensselaer Polytechnic Institute student newspaper, the nuclear waste specialist spoke on campus about kinks and sex education. Several sources also claim that Sam Brinton is a former drag queen.



"Throughout the entire talk, Brinton was open about his experiences, the kinks he partakes in, and the nature of his relationships," the article reads. "He left us with countless anecdotes, like how he enjoys tying up his significant other like a table, and eating his dinner on him while he watches Star Trek." All in all, Brinton's sexual fetishes include tying up his partner while he eats dinner and watches Star Trek.

On social media, Sam Brinton is fairly active. The Instagram figure describes himself as a left-wing activist and proponent of sexual obsessions in his bio. In the name of promoting his woke agenda of "diversity and racial equity", Biden is taking decisions utterly detrimental to USA's national security.

Last year, just days after assuming the presidency, Joe Biden had signed an executive order, titled "Enabling All Qualified Americans to Serve Their Country in Uniform," which effectively repealed an Obama-era policy prohibiting federally supported gender reassignment surgery. The military "thrives when it is composed of diverse Americans who can meet the rigorous standards for military service, and an inclusive military strengthens our national security," according to Joe Biden's executive order.

Biden had stated, "It is my conviction as Commander in Chief of the Armed Forces that gender identity should not be a bar to military service". Adding further, "Moreover, there is substantial evidence that allowing transgender individuals to serve in the military does not have any meaningful negative impact on the Armed Forces."

Last November, NASA, the National Science Foundation (NSF), the United States Department of Energy, and the United States Air Force had also commissioned a report, which had made racially contentious efforts at "diversity" and "inclusion" a priority of its instruction, even tying grant money to compliance. It's now more than clear that Biden's agenda is to turn the US security establishment into a highly compromised unit rather than a powerful one, that too in the name of promoting internal diversity.

EDITOR'S COMMENT:

The box was intentionally left blank

Where are all the nukes? (2022)

By Len Williams

Source: https://eandt.theiet.org/content/articles/2022/02/where-are-all-the-nukes/

Feb 16 – Since the end of the Cold War, the absolute number of nuclear weapons in the world has declined dramatically. But, as Len Williams discovers, that doesn't mean we can sleep any more easily. Here's what the planet's nuclear arsenal looks like in 2022.

It begins with a blinding flash that fills your entire range of vision. Moments later, a blast of scorching air pulsates over you. If, after a few moments of shock, you realise you've survived the initial nuclear blast, you need to act now – because it's not over yet.

In the next few minutes, radioactive debris will rain down. Find shelter, preferably inside a building with a concrete structure. Once inside, remove your outer layers and wash with soap to get rid of any radiation. The fallout will remain most dangerous for the next 24 hours, so avoid leaving shelter. Follow these steps from Ready, a US public service campaign designed to educate and empower people to prepare for emergencies, and you might just survive a nuclear attack.

Of the estimated 13,000 nuclear warheads in the world today, almost 10,000 are in active service and all have the potential to cause mass destruction – and even bring an end to human civilisation. Even a 'small' regional nuclear war could throw up so much soot into the atmosphere that global temperatures would drop precipitously for years, destroy agriculture and cause mass starvation.

The dangers of nuclear weapons are well established. But how worried should we be? Nuclear bombs have only been used twice in anger, more than 70 years ago (by the US against Japan in 1945). Since the collapse of the Soviet Union, the global nuclear arsenal has shrunk rapidly. In 1991, the US had around 19,000 weapons, compared to around 5,600 today. A similar decline is seen in Russia (which had 29,000 in 1991, but about 6,000 today).

Only nine states have nuclear weapons, and there are far fewer countries with a nuclear programme today than during the Cold War. And the crazy logic of 'MAD' (Mutually Assured Destruction) does seem to have prevented war between the nuclear powers for decades.

Nevertheless, complacency would be unwise. The world today is arguably less safe than at any time since the end of the Cold War, the calculations of diplomacy more complex, and a resurgence of great power rivalry is encouraging nuclear states to modernise their arsenals. So how dangerous is the nuclear threat in 2022?

"You could destroy the world 100 times over or five times over, but it's the same difference," points out Philip Ingram, a former senior British intelligence officer and expert in nuclear weapons. While the world's nuclear-armed states have gradually reduced the number of weapons in their arsenals, they're still bristling with enough potential firepower to bring about catastrophe.

Today's nuclear weapons are far more destructive than those that came before. For example, any one of the US's nuclear submarines contains several times more potential firepower than all the explosives unleashed in World War Two combined (including the bombs dropped over Hiroshima and Nagasaki).

What is more, despite the decline in absolute numbers of nuclear weapons, most countries are currently upgrading their systems to be more lethal. Practically all countries are investing in new types of nuclear weapon and ways to deliver them; the most significant is perhaps the recent emergence of 'hypersonic' missiles, which can change course while in flight and potentially evade nuclear defences.

"When states invest in new delivery systems like this, it can drive an 'arms race' where other nuclear-armed states feel they need to catch up," explains Marion Messner of BASIC, an organisation that advocates for disarmament.

This desire to modernise can be seen in several countries. The UK, notably, increased its 'ceiling' for the number of weapons from 180 to 260 last year. Meanwhile, China is increasing its inventory as are India, Pakistan and North Korea.

Yet perhaps more concerning than the qualitative improvement in the weapons themselves is the political context we now find ourselves in. Messner says: "A lot of people are worried that in the past five to 10 years, tensions between nuclear armed states seem to have increased."

Closest to home (for UK readers) is surely Russia and its acts of outright aggression; the threat of a possible invasion of Ukraine means many are worried about the potential for miscalculation.

The Korean peninsula is another hotspot. North Korea is believed to have between 40 and 50 nuclear warheads, and its belligerence and paranoia mean the threat of attacks is continual. In January this year, Pyongyang claimed it had successfully tested a hypersonic missile that can evade conventional anti-missile systems.

Ingram also points to Israel (which is believed to have some 90 nuclear weapons, despite neither confirming nor denying this). "Israel is a worry because it is surrounded by enemies." With many of its neighbours being opposed to the tiny country's very existence, Ingram believes there is a high risk of the country using its nuclear weapons if faced with an existential threat.

Then there are the qualities of the world's political leaders. Again, Ingram notes the dangers of countries where the leaders appear to be settling in for life. There are countless historical examples, Ingram argues, "of leaders who stay in power for life becoming more draconian and believing there are Machiavellian things going on around them". He reckons the longer that leaders like Kim Jong-Un, Xi Jinping or Vladimir Putin stay in power, "the more likely they are to surround themselves with 'yes men' and lose touch with reality". That could potentially lead to them making extreme choices.

Besides the actions of nuclear armed states, there are other emerging threats. Not least is the risk of global terrorism. Although it would be very difficult for terrorists to build a bomb themselves, there has long been a danger of rogue states selling fissile material to terrorists that could be turned into a 'dirty bomb' that would still cause carnage.

There are also several countries that have the potential to create nuclear weapons, even if they are not there yet. Iran has garnered plenty of attention for its nuclear programme in recent years. However, it's widely believed, says Ingram, that Saudi Arabia, Iran's regional

rival, has the know-how to create a bomb if it wanted. Meanwhile in east Asia, another global hotspot, it's generally believed that Japan, Taiwan and South Korea all have the capability to create bombs in a year or two.
Cyber-attacks are another serious issue. Ingram explains that there is a continual threat of such attacks against nuclear weapons silos. He points to the example of the Stuxnet bug, which is believed to have caused serious damage to Iran's nuclear programme in 2010. Perhaps the biggest fear is that terrorists might find a digital back door into nuclear facilities and launch a weapon (although robust security measures make this very unlikely).
Another emerging threat is the impact of a bomb being set off in space. Ingram explains that exploding a nuclear weapon beyond the Earth's atmosphere might not kill people on the ground, but "the electromagnetic pulse could fry or shut down many satellites". Since modern militaries are ever more reliant on GPS and satellite communications, space-based attacks could be particularly disruptive.

Nuclear Arsenals

By Country

United Kingdom

Current estimated total: 225
Operationally available: 120
Delivery method: Four Vanguard-class submarines.
While the country has never published data on its nuclear arsenal, it appeared to be gradually reducing the number of warheads from the early 2000s (it peaked at around 500 during the 1970s and 1980s). The country has about 120 operational weapons today. However, in its 2021 integrated review, the government appeared to reverse this policy, and set an upper 'ceiling' of 260 (including non-operational weapons).
The country is also planning to modernise its submarines, with four new Dreadnought class nuclear submarines coming into service in the 2030s. It is also in the process of upgrading its warheads, increasing their ability to conduct missions.

France

Current estimated total: 300
Operationally available: 300
Delivery method: Four Le Triomphant class submarines. Air-launched cruise missiles from approximately 40 bombers.
France has reduced the size of its stockpile to around 300, down from a peak of 540 in the early 1990s.
Paris is currently in the process of upgrading its entire nuclear deterrent. By 2035 it is expected to commission the first of four new submarines to replace the Le Triomphant class boats. Currently known as the SNLE 3G, the new submarines will come with improved missile delivery platforms. France also plans to commission its next-generation combat aircraft around the same time, which will be able to deliver a hypersonic cruise missile.

United States

Current estimated total: 5,600
Operationally available: 3,700
Delivery method: Numerous ICBMs – intercontinental ballistic missiles (launched from the ground in the US and the territory of five Nato allies), 14 Ohio-class submarines, ~110 B-52 and B-21 bombers (armed with missiles and gravity bombs).
Over the past 30 years, the US appears to have complied with its treaty requirements and continued to reduce the number of warheads in its arsenal.
The tone changed under the Trump administration, however, which became much less transparent about the number of weapons and reductions. Most significant is the increase in funding for the army's nuclear weapons programmes; the budget has almost doubled in the past decade as the arsenal modernises. The biggest development is the creation of the W93 ballistic missile warhead, a brand new design about which relatively little is known.

Russia

Current estimated total: 6,257
Operationally available: 4,587
Delivery method: Numerous intercontinental ballistic missiles silos, 11 nuclear submarines of 3 classes, ~65 Tu-160 Blackjack and the Tu-95MS Bear H bombers.

Russia has reduced the size of its arsenal dramatically since the collapse of the Soviet Union (it also removed weapons it held on the territory of independent post-Soviet states, including Ukraine). However, its posture has been repeatedly criticised, and it has developed several new weapons and delivery methods which appear to break its treaty obligations.
The Russian nuclear arsenal has been undergoing a decades-long modernisation, with several new technologies introduced. These include plans for a nuclear-propelled cruise missile, which could have unlimited range. It has also developed the Sarmat, a ballistic missile that could carry up to 15 warheads, each with its own target.

Pakistan

Current estimated total: 165
Operationally available: 165
Delivery method: Mirage III and Mirage V bombers, several short and medium-range land-based ballistic missiles – including road mobile weapons.
Pakistan is not constrained by non- proliferation treaties and has been expanding the size of its arsenal in recent years. The country aims to achieve a 'triad' of air, land and sea delivery, and is currently developing a sea-launched version of its Babur missile.
Pakistan has invested heavily in so-called 'tactical' nuclear weapons. These are designed to have a low yield and short range, with a view to use on the battlefield.

Israel

Current estimated total: ~90
Operationally available: ~90
Delivery method: It is believed that Israel can deliver warheads from the ground, air and sea.
Israel has long pursued a policy of ambiguity about its nuclear weapons programme and has neither confirmed nor denied whether or not it has them.
It is therefore unclear what the country's plans for upgrading its nuclear posture are.

India

Current estimated total: 160
Operationally available: 160
Delivery method: ~4 squadrons of Mirage 2000H and Jaguar aircraft, short, medium and intermediate range Agni land-based missiles, and the Dhanush – a ship-based ballistic missile.
India is not constrained by non-proliferation treaties and is actively expanding its nuclear arsenal.
While the country already has a 'triad' of land, air and sea delivery, it is upgrading them to become more sophisticated and increase its reach. India commissioned the Arihant in 2017 – a nuclear-capable submarine – although it is not believed to be armed (but more are on the way). It is also building the Agni-V, an intercontinental ballistic missile with a range of over 5,000km.

North Korea

Current estimated total: 45
Operationally available: 45
Delivery method: Land-based short, medium and (potentially) intercontinental ballistic missiles.
North Korea withdrew from the NPT in 2003 and has actively been testing missiles and bombs in recent years. A lack of transparency means the exact number and range of missiles is unclear, but it is believed to have the ability to target cities in the US.
Pyongyang claims to have successfully launched a hypersonic missile in January 2021. It is also believed to be developing submarine-launched missiles.

China

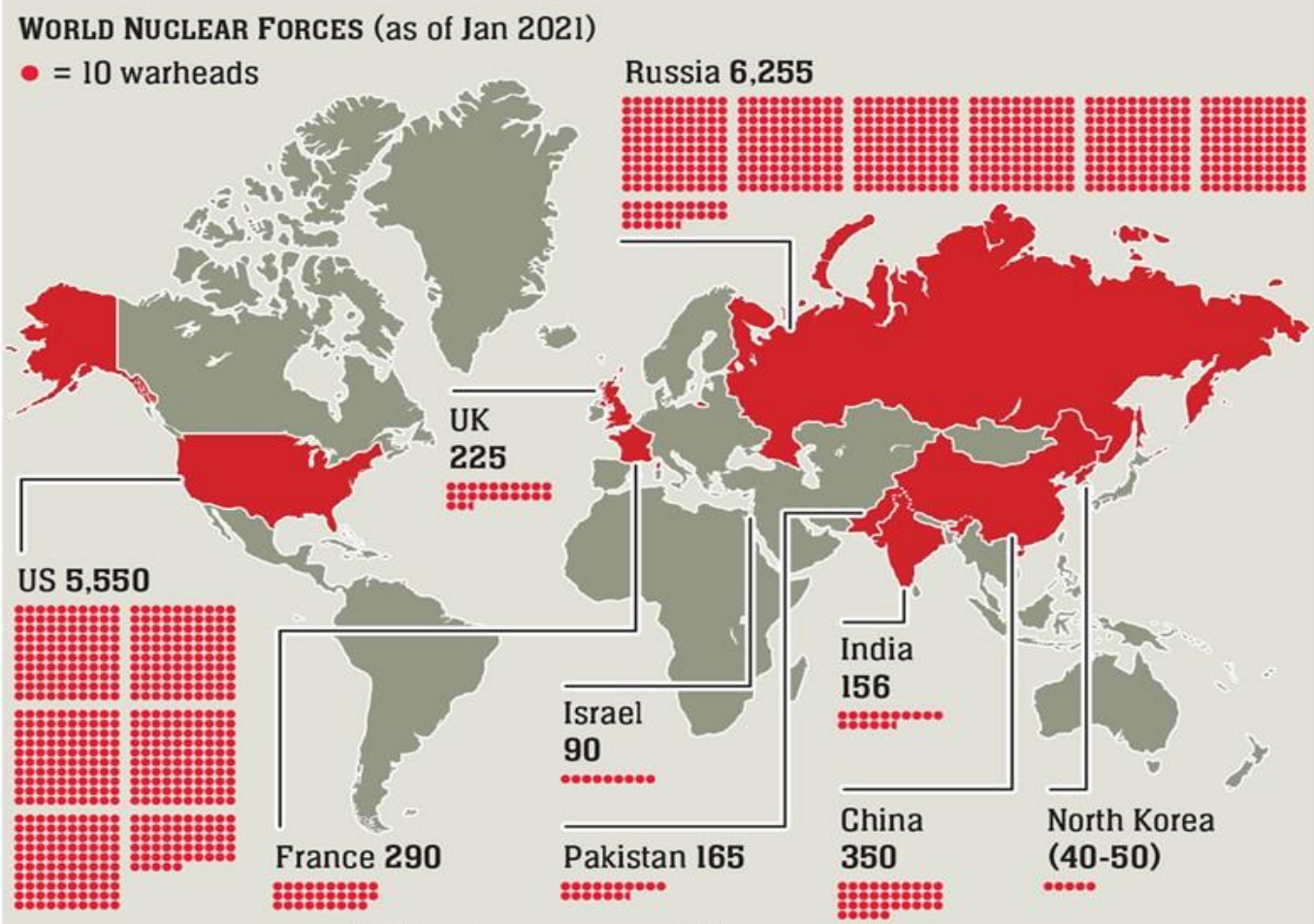
Current estimated total: 350
Operationally available: 350
Delivery method: Two brigades of the DF-41 road-mobile ICBMs, two submarines and ~20 gravity bombs.
China appears to be going through a significant expansion and modernisation of its nuclear forces. Reports indicate the country is increasing the number of nuclear silos across the country. Experts expect the country to at least double or even triple the size of its arsenal over the coming decade.

Ever since 1947, the Bulletin of Atomic Scientists, a non-governmental organisation, has maintained a 'Doomsday Clock', representing how close the planet could be to a man-made

global catastrophe. Nuclear war and climate change are perceived as the likeliest causes of such a disaster, and the people behind

Global nuclear warhead inventories

The world's nuclear-armed states possess a combined total of about 13,080 nuclear warheads, with more than 90 per cent belonging to the United States and Russia



Country	Deployed warheads*	Other warheads†	Total 2021	Total 2020
United States	1,800	3,750	5,550	5,800
Russia	1,625	4,630	6,255	6,375
UK	120	105	225	215
France	280	10	290	290
China	–	350	350	320
India	–	156	156	150
Pakistan	–	165	165	160
Israel	–	90	90	90
North Korea‡	–	(40-50)	(40-50)	(30-40)
Total	**3,825**	**9,255**	**13,080**	**13,400**

*Warheads placed on missiles or located on bases with operational forces
†Stored or reserved warheads and retired warheads awaiting dismantlement
‡Figures are highly uncertain and are not included in global totals

SOURCES: AFP, STOCKHOLM INTERNATIONAL PEACE RESEARCH INSTITUTE, GRAPHIC NEWS

the clock believe we are the closest to 'midnight' we have ever been.
However, not everyone is convinced that the threat is quite so severe, at least not from nuclear weapons. "I don't see such a great risk of proliferation right now, and the great powers will seek to maintain a stable strategic relationship," reckons Christoph Bluth, professor of international relations and security at the University of Bradford. Bluth acknowledges he may not be in the majority with this interpretation but does point to several factors that make the use of nuclear weapons today relatively unlikely.
First, he points to the happy fact that interstate warfare has almost disappeared in recent decades. Thanks to a set of international laws and norms that most countries comply with, wars between countries are far less common now than at practically any other time in human history. Because of free trade, there is relatively little imperative for countries to invade others; they can normally access the resources they need through non-violent avenues.
Bluth also thinks it's extremely unlikely that any country would be first to use nuclear weapons against an opponent. Thanks to MAD, they know they would almost instantly be hit with several nukes in return. Only in the case of existential threats, such as an invasion by an enemy power, does he think these weapons would be used – and we're a long way from such an event, even in today's fraught political environment.
He points out that despite various nations' weaponry upgrades, the fundamental diplomatic calculations are the same as ever. For instance, he believes the new hypersonic missile systems "do not change the strategic balance". The weapons might be getting better, but the fact remains that it would be a very foolhardy leader indeed who would strike first, aware that this would inevitably be followed by a counterpunch.
As Messner of BASIC points out, "modernisation itself is not necessarily a bad thing". Upgrading weapons is about "making sure systems stay safe", since many of the technologies used to run and launch nuclear weapons are decades old.
Whether it's the increasingly confrontational nature of international relations, the ever-present risk of proliferation, or the apparent 'arms race' for new delivery systems, growing fears about the possibility of a nuclear war do at first appear justified.
Nonetheless, there is cause for optimism. Thanks to determined diplomacy, non-proliferation does seem to be working. What is more, more than 80 non-armed countries have so far signed a UN treaty on the prohibition of nuclear weapons, which came into effect in January 2021. This treaty, although unlikely to have a material impact on the nine nations that have nuclear arsenals, does pile pressure on them to disarm.
Messner explains that there are various theories about how, and if, denuclearisation could ever come about. She says that countries with the weapons often don't really want them – they're expensive and pose a huge risk – but they do offer a kind of security. As part of BASIC's advocacy towards disarmament, "we try to get them to think about what alternative forms of security would look like".
While we can't uninvent this technology, Messner believes there is still "appetite" to denuclearise and that we might just "muddle through".

Global Laser Enrichment

Source: https://www.cameco.com/businesses/fuel-services/enrichment-gle

We continue to explore innovative areas like laser enrichment technology to broaden our fuel cycle participation and help us serve our customers more effectively. Uranium enrichment is the second-largest value component, after uranium, in a typical light-water reactor fuel bundle.
While there are still a number of development milestones before this technology could be commercialized, we believe it has excellent potential to expand Cameco's reach in the nuclear fuel cycle in the future, building on the existing world-class assets and capabilities we already possess in uranium production, refining, conversion and fuel fabrication.
The progression of GLE's technology development program through to commercialization, at a pace determined by market fundamentals, could lead to GLE offering long-term advantages to the global nuclear energy sector, particularly in the following areas:

Depleted Tails Re-enrichment
As per GLE's agreement with the U.S. Department of Energy, re-enriching depleted uranium tails leftover as a by-product of previous-generation enrichment technologies, repurposing legacy waste into uranium and conversion products to fuel nuclear reactors and aiding in the responsible clean-up of enrichment facilities no longer in operation.

High-Assay Low-Enriched Uranium (HALEU)
Producing high-assay low-enriched uranium (HALEU), the primary fuel stock for the majority of small modular reactor (SMR) and advanced reactor designs that are proceeding through the development stage toward commercial readiness.

Low-Enriched Uranium (LEU)

Producing low-enriched uranium (LEU) fuel for the world's existing and future fleet of large-scale light-water reactors with greater efficiency and flexibility than current enrichment technologies. The enrichment market has the same customer base as the uranium market, and most of the world's commercial nuclear reactors need enriched uranium.

Canada and the United States are among the nations around the world pursuing ambitious carbon reduction strategies. Governments in both countries have signaled significant interest in cooperating on clean energy solutions, developing and deploying SMR technologies, and collaborating to bolster critical mineral and nuclear fuel cycle security.

GLE could fit extremely well with these bilateral policy priorities, potentially providing a stable source of North American-based uranium enrichment, adding to the robustness of the continental nuclear energy supply chain, and helping to de-risk any fuel concerns impeding the progress of emerging SMR designs.

Cameco is committed to responsibly and sustainably managing our business while increasing our contributions to global climate change solutions. Our investment in GLE aligns well with these objectives.

EDITOR'S COMMENT: There is skepticism about the possibility of SILEX becoming a cost-effective way to enrich uranium for energy production. Some are worried that it could allow the production of small quantities of high-enriched uranium for use in nuclear weapons-related programs have been revealed since 2002 in Iran and South Korea. One of the problems for regulators is that most of the components needed to build a laser uranium enrichment system also have non-nuclear uses. In addition, most of the research on this issue is carried out within universities and may not follow all nuclear safety measures.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

EXPLOSIVE NEWS

Houthis second missile attack on the UAE: The new normal? - analysis

Source: https://www.jpost.com/middle-east/article-694365

A drone aircraft is put on display at an exhibition at an unidentified location in Yemen in this undated handout photo released by the Houthi Media Office, July 9, 2019. (photo credit: HOUTHI MEDIA OFFICE/HANDOUT VIA REUTERS)

Jan 24 – The Iran-backed Houthis targeted the UAE for the second time in a week on Monday morning. This comes in the wake of reports that air defense systems last Monday had intercepted some of the threats. Last week the attack involved drones, ballistic missiles and cruise missiles. The second attack appears smaller but nevertheless now indicates the Houthis believe they have a right to expand the war to the UAE.

This is important because unlike Houthi attacks on Saudi Arabia, the UAE is a major hub of international trade and tourism. It also is populated by a large expat community from all over the world. The Houthis, backed by Iran, have a goal to show they can stop air traffic into the UAE and disrupt normalcy. As the UAE has strived to be part of a stabilizing group of countries, it is now being targeted by Iran.

The Houthis openly bragged about their targeting of the UAE and Iranian media have repeated their warnings. The goal is to show they can openly say what they will do and then do it. There are no real repercussions so far. After the first attacks, there were bombing raids on the Houthis by the Saudis, apparently, but these resulted in casualties that were then condemned. Western media said that the airstrikes had killed people at a prison. This didn't appear like a very helpful retaliation, and all it led to was another Houthi propaganda spiel claiming a "crime against humanity." This distracts from the fact the Houthis are now trying to rain missiles down on Abu Dhabi.

The new Houthi missile attack

Monday's attack on January 24 was reported by Iranian media. The Fars News report claimed it was relying on Russia's Sputnik for information. It said there were reports of activation of air defenses and explosions were heard. These may be explosions from the interceptions. "It is not yet clear what caused the explosion and the sound of the alarm, and official sources have not released any news about it," Iran's media said. The report also

quoted Sabareen News Telegram channel as publishing "images of smoke in the sky of Abu Dhabi." It is important to remember these reports came in early in the morning.

"The UAE Army air defenses were activated in the early hours of Monday morning to deal with hostile targets, and leaked images show the system intercepting several rockets, Sputnik reported. Eyewitnesses reported hearing at least four explosions," the report said. It claimed that passenger planes were halted and a "no-fly" area was established. The report says the Houthis have warned that any targeting of Yemen by the UAE will result in more of these attacks.

A scene of destruction in the city of Jazan, Saudi Arabia last month was caused by a projectile fired by the Houthis, according to the Saudi state news agency. (credit: SAUDI PRESS AGENCY/REUTERS)

The Associated Press wrote that "videos posted to social media show the sky over the capital light up before dawn, with points of light looking like interceptor missiles in the sky... the missile fire disrupted traffic into Abu Dhabi International Airport for about an hour." The ability of the Iran-backed Houthis to stop air traffic at a major international airport is important. It shows their growing threat and range. They are graduating to a major regional threat and Iranian proxy. Much as Hezbollah became an international threat, with tentacles stretching to South America and Africa, the Houthis have been put on steroids by Iran's backing. They receive technology such as drones and missiles. The Iranians use them as a testbed for new drone and missile technology. They give Iran influence over the Red Sea where Iran has sent IRGC spy ships. In addition, Iran has posted key IRGC officials to Yemen. A top Iran diplomat, who was likely also an IRGC advisor to the Houthis, died of Covid in December after serving in Yemen.

Iranian technology being tested on UAE

The attack on the UAE also comes a day after the Minister of Foreign Affairs and the Minister of Innovation, Science, and Technology announced a hi-tech investment fund with the United Arab Emirates. The Israeli initiative envisions a "binational industrial R&D fund with the United Arab Emirates, which will support requests for joint activities between Israeli and Emirati companies," the Ministries said. "The fund's support will enable access to international resources, knowledge, technology, and infrastructure which currently do not exist in Israel, and will also enable assistance to Israeli companies through recruitment of local partners, compliance with foreign regulations, and the creation of marketing, economic, or business advantages."

Iranian media reports have often argued that the Houthis are waging a war not only against Saudi Arabia and now the UAE but also are part of the broader Iranian "resistance" against the United States and Israel. In January 2021 reports said Iran had sent the Shahed 136 drone to Yemen. The drone has a range of some 2,000km and could reach Israel.
Israel has expressed solidarity with the UAE in the face of attacks. However, the overall context of the Iranian expansion of the Houthi war to the skies of Abu Dhabi shows how the Iranian threat to the region is rapidly growing to include a hand in attacks across an arc of some three thousand kilometers from Lebanon to the Gulf. Israel's Minister of Foreign Affairs Yair Lapid said yesterday (Sunday) that "Israel and the United Arab Emirates share a passion for the development of advanced technologies which will improve quality of life, the environment, and the economy." While Israel and the UAE want to invest in technology to improve the quality of life, the message of Iran is that it can seek to destabilize the quality of life throughout the region.

UAE jets strike Houthi ballistic missile launcher after latest Abu Dhabi attack

Source: https://www.thenationalnews.com/uae/2022/01/24/uae-retaliates-with-strike-on-houthi-ballistic-missile-launcher-after-abu-dhabi-attack/

Jan 24 – UAE fighter jets destroyed a missile battery that was used to launch rockets towards Abu Dhabi on Monday morning.
The Ministry of Defence released footage of a strike by F-16 jets in Al Jawf, outside Houthi-controlled Sanaa in Yemen.

The attack took place at 4.10am, shortly after the launcher fired two ballistic rockets towards the Emirati capital. Both were shot down by air defences protecting the city. Al Jawf is about 1,500km south of Abu Dhabi. UAE authorities said the attempted strike on Abu Dhabi "did not result in any casualties, as the remnants of the intercepted and destroyed ballistic missiles fell in separate areas around the emirate".
Flashes were seen in the sky over the capital at about 4.15am, residents said.

Last week, after a Houthi strike on an Adnoc oil storage plant killed three workers and injured six, the government said it "reserves right to retaliate". A projectile fired at Abu Dhabi airport caused a minor fire in an under-construction extension area away from the terminal, with no injuries. Dr Anwar Gargash, diplomatic adviser to President Sheikh Khalifa, said it was a "heinous attack on civilian facilities".

Flights unaffected

In Abu Dhabi on Monday, pupils returned to schools as planned after several weeks of remote learning and the roads were busy.
At the airport, flights took off as normal on a busy Monday morning.
Social media claims that the airport closed appeared to be entirely false. There were no flights planned between 3.45am and 5.10am - and 17 flights took off between then and 9am as scheduled, the airport's live board showed.

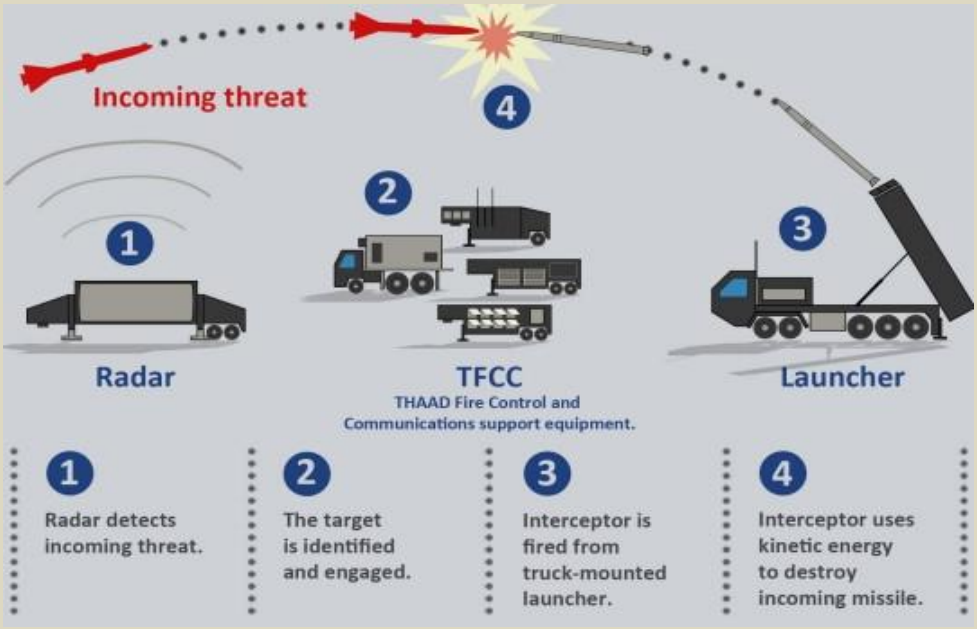
Saudi Arabia takes down ballistic missile

In Saudi Arabia, the Coalition said it destroyed a ballistic missile launched by the Houthis towards the city of Dhahran Al Janub early on Monday. Shrapnel from the intercepted missile landed in the city's industrial zone and pictures of burnt vehicles were published by local media. The attacks came just hours after the Arab League group of nations met in Cairo to call for the US to designate the Houthis a terrorist group. The US administration said it is considering the move after the first Abu Dhabi attack, which was condemned by world leaders.

THAAD Defense System – First Successful Combat Operational Use

Source: https://i-hls.com/archives/112771

Jan 24 – Following the recent drone attacks on the UAE (United Arab Emirates), the **THAAD** (Terminal High Altitude Area Defense) was used for the first time in combat conditions to intercept drones and missiles.



The attacks on January 17, 2022, that killed three people and injured six more, was attributed to a combination of ballistic and cruise missiles, as well as drones launched by the Houthi rebels in Yemen.

The THAAD "brought down a ballistic missile during its first recorded successful operational use, in the hands of the United Arab Emirates," as reported by thedrive.com. THAAD is an American-made anti-ballistic missile defense system designed to shoot down short-, medium-, and intermediate-range ballistic missiles in their terminal phase (descent or reentry) by intercepting with a hit-to-kill approach, that delivers their destructive power by hitting the target at high velocity and do not contain an explosive warhead,

according to armyrecognition.com. The American THAAD air defense missile system is in service with the UAE armed forces since 2015.

North Korea tests longest-range missile since 2017

Source: https://www.wfmz.com/news/north-korea-launches-suspected-missile-in-7th-test-in-2022/article_ce820a96-358e-5771-b6ec-d266a7b05ccc.html

Jan 30 — North Korea on Sunday fired what appeared to be the most powerful missile it has tested since U.S. President Joe Biden took office, possibly breaching a self-imposed suspension on the testing of longer-range weapons as it revives its old playbook in brinkmanship to wrest concessions from Washington and neighbors amid a prolonged stalemate in diplomacy.

The Japanese and South Korean militaries said the missile was launched on a lofted trajectory, apparently to avoid the territorial spaces of neighbors, and reached a maximum altitude of 2,000 kilometers (1,242 miles) and traveled 800 kilometers (497 miles) before landing in the sea.

The flight details suggest the North tested its longest-range ballistic missile since 2017, when it twice flew intermediate-range ballistic missiles over Japan and separately flight-tested three intercontinental-range ballistic missiles that demonstrated the potential range to reach deep into the American homeland.

Sunday's test was the North's 7th round of weapons launches this month. The unusually fast pace of tests indicates North Korea's intent to pressure the Biden administration over long-stalled nuclear negotiations as pandemic-related difficulties unleash further shock on an economy broken by decades of mismanagement and crippling U.S.-led sanctions over its nuclear weapons program.

South Korean President Moon Jae-in called an emergency National Security Council meeting where he described the test as a possible "midrange ballistic missile launch" that brought North Korea to the brink of breaking its 2018 suspension in the testing of nuclear devices and longer-range ballistic missiles.

Japanese Defense Minister Nobuo Kishi told reporters it was clear that the missile was the longest-range weapon the North has tested since launching its Hwasong-15 ICBM in November 2017.

The launch came after North Korean leader Kim Jong Un chaired a ruling party meeting on Jan. 20 where senior party members made a veiled threat to lift the moratorium, citing what they perceived as U.S. hostility and threats. Kim in April 2018 declared that "no nuclear test and intermediate-range and inter-continental ballistic rocket test-fire" were necessary for the North any longer as he pursued diplomacy with then-U.S. President Donald Trump in an attempt to leverage his nukes for badly needed economic benefits.

The latest missile's flight details suggest that North Korea's moratorium is already broken, said Lee Choon Geun, a missile expert and honorary research fellow at South Korea's Science and Technology Policy Institute. He said the data suggests that the North tested an intermediate-range ballistic missile or possibly even a weapon approaching ICBM capacities.

In his strongest comments toward the North in years, Moon said the situation around the Korean Peninsula is beginning to resemble 2017, when North Korea's provocative run in nuclear and long-range missile testing resulted in a verbal exchange of war threats between Kim and Trump.

Moon described the North's latest tests as a violation of U.N. Security Council resolutions and a "challenge toward the international society's efforts to denuclearize the Korean Peninsula, stabilize peace and find a diplomatic solution" to the nuclear standoff.

The North "should stop its actions that create tensions and pressure and respond to the dialogue offers by the international community including South Korea and the United States," Moon said, according to his office.

Moon, who had ambitiously pushed for inter-Korean engagement, held three summits with Kim in 2018 while also lobbying to set up Kim's first summit with Trump in 2018, where they issued vague aspirational goals for a nuclear-free Korean Peninsula without describing when and how it would occur. But the diplomacy derailed after the collapse of the second Kim-

Trump meeting in 2019, when the Americans rejected North Korea's demand for major sanctions relief in exchange for a partial surrender of its nuclear capabilities.
Japanese Chief Cabinet Secretary Hirokazu Matsuno said Sunday's missile flew for around 30 minutes and landed in waters outside Japan's exclusive economic zone. There were no immediate reports of damage to boats or aircraft.
The U.S. Indo Pacific Command said the United States condemns North Korea's testing activity and calls on the North to refrain from further destabilizing acts. It said the latest launch did not "pose an immediate threat to U.S. personnel, territory, or that of our allies."
The launch came three days after North Korea fired two short-range ballistic missiles into the sea on Thursday. The North also flight-tested a pair of purported long-range cruise missiles on Tuesday while vowing to strengthen its nuclear "war deterrent" and build more powerful weapons.
Experts say the North could halt its testing spree after the start of the Beijing Winter Olympics next week out of respect for China, its major ally and economic lifeline. But there's also expectation that the North could significantly up the ante in weapons demonstrations once the Olympics end in February to grab the attention of the Biden administration, which has been focusing more on confronting China and Russia over its conflict with Ukraine.
"North Korea is launching a frenzy of missiles before the start of the Beijing Olympics, mostly as military modernization efforts. Pyongyang also wants to boost national pride as it gears up to celebrate political anniversaries in the context of economic struggles," said Leif-Eric Easley, a professor at Ewha University in Seoul.
"It wants to remind Washington and Seoul that trying to topple it would be too costly. By threatening stability in Asia while global resources are stretched thin elsewhere, Pyongyang is demanding the world compensate it to act like a 'responsible nuclear power,'" Easley added.
North Korea has justified its testing activity as an exercise of its rights to self-defense and threatened stronger action after the Biden administration imposed fresh sanctions following two tests of a purported hypersonic missile earlier this month.
While desperate for outside relief, Kim has shown no willingness to surrender the nuclear weapons and missiles he sees as his strongest guarantee of survival. Analysts say Kim's pressure campaign is aimed at forcing Washington to accept the North as a nuclear power and convert their nuclear disarmament-for-aid diplomacy into negotiations for mutual arms reduction.
Kim last year announced a new five-year plan for developing weapons and issued an ambitious wish list that included hypersonic weapons, spy satellites, solid-fuel intercontinental ballistic missiles and submarine-launched nuclear missiles.
State media said Friday that Kim visited an unspecified munitions factory producing a "major weapons system," and that the workers pledged loyalty to their leader who "smashes with his bold pluck the challenges of U.S. imperialists and their vassal forces."

EDITOR'S COMMENT: It seems that Kim Jong Un is so scared by announced US sanctions that he tests one missile after the other with the last one targeting the U.S. territory of Guam! They are going to kill the man by using stress as a weapon!

United Arab Emirates Intercepts Missile Fired By Yemen's Iran-Backed Houthi Militants

Source: https://nypost.com/2022/01/31/uae-intercepts-missile-fired-by-yemens-iran-backed-houthi-militants/

Jan 31 – **The United Arab Emirates on Monday intercepted a ballistic missile fired by Yemen's Iran-backed Houthi militants as Israeli President Isaac Herzog was visiting — the third attack this month.** The Middle Eastern country's state-run media said the "attack did not result in any losses, as the remnants of the ballistic missile fell outside the populated areas." **A US Patriot missile battery was engaged,** Pentagon spokesman John Kirby said at Monday's briefing, but ground-to-air missiles fired by UAE forces successfully hit the target. "We of course stand with the UAE, Saudi Arabia, and our Gulf partners in defending against threats to their peoples and their territories," Kirby said. The attack came as Herzog was visiting the capital Abu Dhabi where he discussed security and relations with Crown Prince Sheikh Mohammed bin Zayed Al Nahyan. The Israeli president left the country later Monday. "While Israel's president is visiting the UAE to build bridges

and promote stability across the region, the Houthis continue to launch attacks that threaten civilians," State Department spokesman Ned Price said. Houthi military spokesman Yehia Sarei said that rebels targeted "sensitive sites" in Abu Dhabi and Dubai with **Zulfiqar ballistic missiles (photo above) and drones**."

UAE intercepts and destroys three hostile drones

Source: https://www.thenationalnews.com/uae/2022/02/02/uae-intercepts-and-destroys-three-hostile-drones/

Missiles and drone aircraft are on display at a Houthi exhibition in Yemen. Reuters

Feb 02 – Three hostile drones that penetrated UAE airspace were shot down on Wednesday, the Ministry of Defence said.
The interception was "away from populated areas" and happened at dawn, officials said late on Wednesday night.
The MoD reiterated its "full readiness to deal with any threats". It added that it will "take all necessary measures to protect the UAE from any attacks".
The attempted attack came on the same day the US said it would send fighter jets and a warship to the Emirates following the recent Houthi attacks.
Secretary of Defence Lloyd Austin said fifth-generation aircraft and the *USS Cole* would help to tackle the threat from the Iran-backed Yemeni rebels.
Mr Austin said the *USS Cole* would link up with the UAE Navy at sea before docking in Abu Dhabi.
An attack on January 17 killed three oil company workers — Hardeep Singh, Hardev Singh and Mamoor Khan — and injured six others. Missiles fired at the UAE by the Houthis on January 24 and January 31 were intercepted and did not lead to any casualties or damage.

EDITOR'S COMMENT: Testing Iranian cruise missiles on UAE grounds should stop before igniting catacombs of innocent victims both in the UAE and Yemen. Remember an old quote stated by IRA after they attempted to assassinate UK Prime Minister Margaret Thatcher? ("*They [UK] have to be lucky all the time; we have to be lucky only once*!") The overall situation is like a bomb waiting to be exploded burning the entire Middle East and beyond.

Ballistic and cruise missiles in the Middle East: the current landscape and options for arms control

By Dr Hassan Elbahtimy

Source: https://www.iiss.org/blogs/research-paper/2022/01/ballistic-and-cruise-missiles-in-the-middle-east

Jan 28 – The determination of regional actors in the Middle East to procure or develop ballistic and cruise missiles shows no immediate signs of abating, and the possibility of even further regional proliferation has driven calls to explore the application of arms controls to manage regional missile developments. This paper surveys the evolving missile landscape in the Middle East and considers some of the possible options for regional missile control.

Table 1: Ballistic-missile holdings of Tier 1 states

Operator	Missile name	Range (km)	Payload (kg)	Fuel type	Circular error probable (CEP) (m)
Israel	LORA	430	240	Solid	10
Israel	*Jericho 2**	1,800	1,000	Solid	?
Israel	*Jericho 3**	4,000	750	Solid	?
Israel	*Rampage* (air-launched ballistic missile)	?	?	Solid	10
Iran	*Shahab-1*	300	1,000	Liquid	700–1,000
Iran	*Shahab-2*	500	730	Liquid	>1,500
Iran	*Qiam-1*	800	500	Liquid	>1,000
Iran	*Qiam-1* mod. (*Qiam-2?*)	800	500	Liquid	~100
Iran	*Shahab-3*	800–1,000	760–1,000	Liquid	2,500
Iran	*Ghadr-1*	1,600	750	Liquid	300
Iran	*Emad*	1,600	700	Liquid	?
Iran	*Khorramshahr-1/-2*	2,000	500–1,800	Liquid	1,500
Iran	*Tondar*	150	190	Solid/liquid	300
Iran	*Fateh-110*	300	450	Solid	<100
Iran	*Khalij Fars*	300	450	Solid	<100
Iran	*Hormuz-1/-2*	300	450	Solid	<100
Iran	*Fateh-313*	500	350	Solid	<100
Iran	*Fateh Mobin*	500	350	Solid	<100
Iran	*Raad-500*	500	350	Solid	<100
Iran	*Zolfaghar*	700	350	Solid	<100
Iran	*Zolfaghar Basir*	700	350	Solid	<100
Iran	*Dezful*	1,000	350	Solid	?
Iran	*Shahid Haj Qasem*	1,400	350	Solid	?
Iran	*Sajjil-1/-2*	2,000	700	Solid	300

* Service status uncertain

Source: IISS, *The Military Balance 2021*

Missiles have long played a key, if relatively understudied, role in Middle Eastern security dynamics. According to Dennis Gormley's 2017 estimate, over 90% of all missiles used in conflict since the Second World War have been in the Middle East.

Today, the determination of regional actors to procure or develop ballistic and cruise missiles shows no immediate signs of abating. Missiles play a growing role in national defence doctrines in the region and many states are driven to acquire them due to the increasing appreciation of their utility as conventional precision-strike systems, as well as symbols of military prowess. Their frequent use by local and external powers in recent and ongoing conflicts in the Middle East and the possibility of even further regional proliferation have driven calls to explore the application of arms controls to manage regional missile developments.

This paper surveys the evolving missile landscape in the Middle East and considers some of the possible options for regional missile control. These two themes form the paper's two parts. The paper starts by exploring some of the key contemporary trends related to missiles in the Middle East. It examines the various regional powers interested in advanced missiles and the emergence of non-state actors as users and developers of missile technology. It also explores the regional appeal of cruise missiles and considers the growing use of advanced missiles as conventionally armed stand-off weapons. Finally, this section explores the regional interplay between offensive and defensive missiles. The second part of the paper charts some of the recent attempts to develop regional arms controls and considers some of the approaches to missile control, including some cross-cutting themes that any missile control efforts might wish to address.

Table 2: Ballistic-missile holdings of Tier 2 states

Operator	Missile name	Range (km)	Payload (kg)	Fuel type	Circular error probable (CEP) (m)
Algeria	9K720 *Iskander*-E (RS-SS-26 *Stone*)	280	480	Solid	<10
Bahrain**	MGM-140A ATACMS	165–300	174–221	Solid	>50
Egypt	9K72 *Elbrus* (RS-SS-1C *Scud*-B)	300	770–950	Liquid	1,000
Egypt	9K72 *Elbrus* (RS-SS-1D *Scud*-C)	600	770–950	Liquid	<1,000
Qatar	BP-12A (CH-SS-14 Mod 2)	280	480	Solid	?
Saudi Arabia	DF-3 (CH-SS-2)	2,780	2,000	Liquid	1,000–4,000
Saudi Arabia	DF-21 (CH-SS-5)	2,150	600	Solid	300
Syria	OTR-21 *Tochka* U (RS-SS-21 *Scarab* B)	120	482	Solid	<100
Syria	M-600 (license-built *Fateh*-110)*	250–300	450–500	Liquid	500
Syria	9K72 *Elbrus* (RS-SS-1C *Scud*-B)*	300	770–950	Liquid	1,000
Syria	9K72 *Elbrus* (RS-SS-1D *Scud*-C)*	600	770–950	Liquid	<1,000
Syria	9K72 *Elbrus* (RS-SS-1E *Scud*-D)*	700	770–950	Liquid	50
Turkey	J-600T *Yildirim* I	150	480	Solid	150
Turkey	J-600T *Yildirim* II	300	480	Solid	<150
Turkey	MGM-140A ATACMS	300	213–247	Solid	>50
Turkey	*Bora*	280	470	Solid	<10
UAE	9K72 *Elbrus* (RS-SS-1C *Scud*-B)	300	770–950	Liquid	1,000
UAE	MGM-168 ATACMS	300	221	Solid	>50
UAE	9K72 *Elbrus* (RS-SS-1D *Scud*-C)	600	770–950	Liquid	<1,000

* Service status uncertain
** Which variant of the MGM-140A Bahrain purchased is uncertain.
Sources: https://www.govinfo.gov/content/pkg/FR-2018-11-08/html/2018-24403.htm; https://missilethreat.csis.org/missile/ss-21/; http://www.nukestrat.com/us/afn/NASIC2006.pdf, page 8; https://www.dsca.mil/press-media/major-arms-sales/bahrain-m31-guided-multiple-launch-rocket-system-gmlrs-unitary-and; https://twitter.com/Kyruer/status/1235930736043208705.

While missile holdings in the Middle East have grown in terms of the types, ranges and platforms used, this paper focuses its examination on ballistic and cruise missiles of ranges exceeding 250 kilometres. The value and reach of this range can vary in different sub-regional settings but is used here as a rough metric indicating the ability to target across borders, as well as a reflection of a degree of technical capability. While the paper incorporates land-attack missiles, it excludes missiles that are closely tied with battlefield or tactical missions, such as those with shorter ranges as well as anti-ship and air-defence platforms. Similarly, armed uninhabited aerial vehicles (UAVs) are excluded from the analysis. While their use has grown in prominence, particularly in some regional conflicts including in Syria, Libya and Yemen, they form a separate category of weapons with distinct dynamics, and thus pose different questions for arms control.

●▶ **Download the research report**

Dr Hassan Elbahtimy is a Senior Lecturer @ Department of War Studies and Co-director of the Centre for Science and Security Studies (CSSS), King's College London.

Israel's "Laser Wall" – When will it be Feasible?

Source: https://i-hls.com/archives/112932

Feb 02 – Prime Minister Naftali Bennett said Israel will surround itself with a defensive **"laser wall,"** with new missile interception technology to be ready within a year. He was speaking at an Institute for National Security Studies (INSS) conference on Feb. 1.

"This will allow us, in the medium- to long-term, to surround Israel with a laser wall that will defend us from missiles, rockets, UAVs and other threats that will essentially take away the strongest card our enemies have against us," Bennett said.

T he IDF will begin using the laser interception system in the next year, first experimentally and later operationally, starting in the South.

Bennett explained that today a terrorist in Gaza can launch a rocket into Israel that costs hundreds of dollars to make, while the Iron Dome battery shooting down the rocket costs tens of thousands of dollars. "We decided to break the equation."

Israel will offer the laser technology to its regional allies that are also facing threats from Iran and its proxies, the prime minister said.

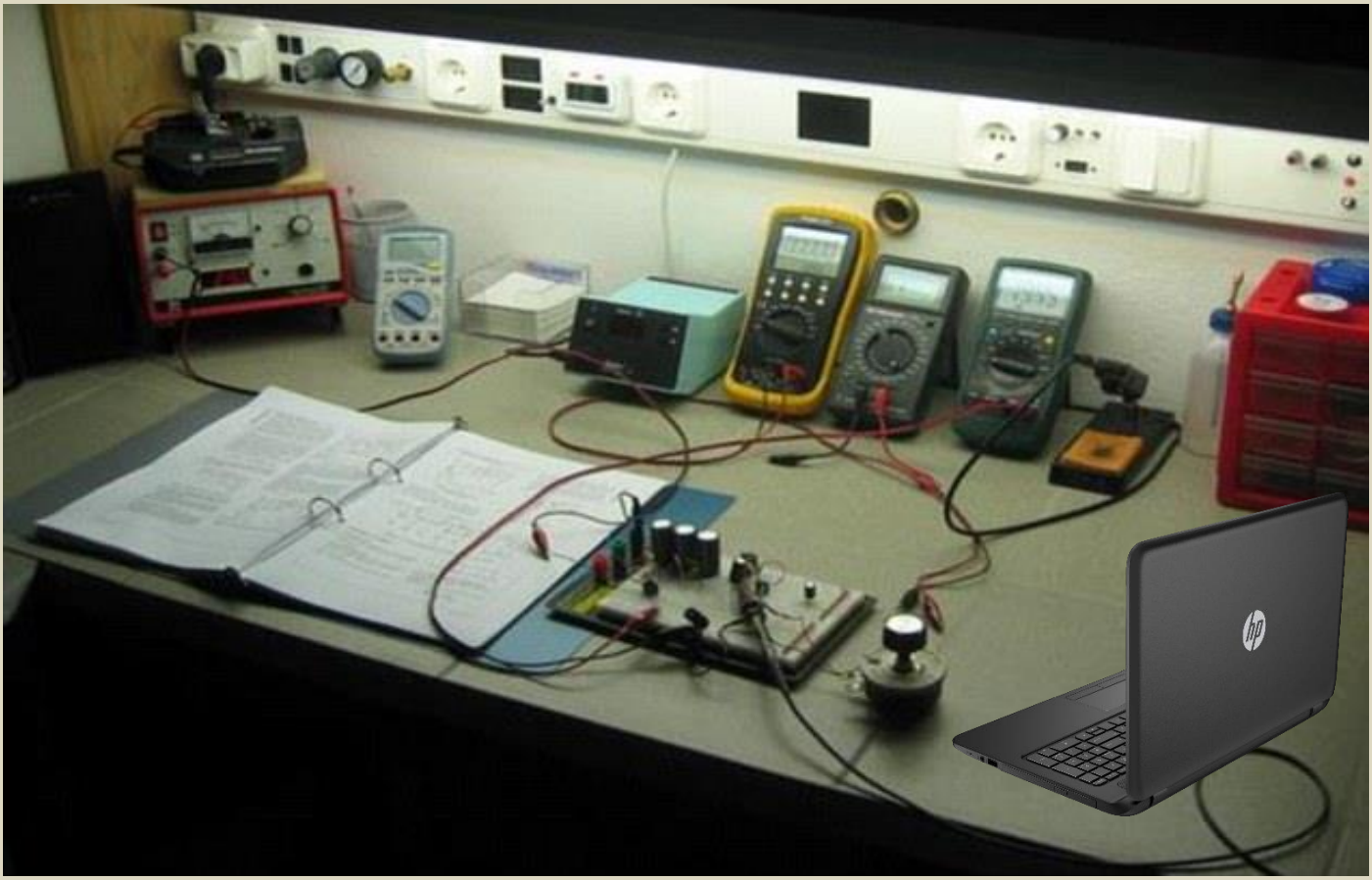
Israeli defense sources said in response that the declaration does not reflect reality. The breakthrough has been proven two years ago in a series of tests; however, it is evaluated that operational feasibility proof would take at least three years, and in several stages, according to maariv.co.il.

Europol coordinates action against bomb manuals available online

Source: https://www.europol.europa.eu/media-press/newsroom/news/europol-coordinates-action-against-bomb-manuals-available-online

Feb 04 – On 1 February, a large-scale Referral Action Day targeting terrorist content online took place at Europol's headquarters. The European Union Internet Referral Unit (EU IRU) at Europol's European Counter Terrorism Centre (ECTC) coordinated the referral activity, which saw the involvement of specialised

counter terrorism units from France, Germany, Hungary, Italy, the Netherlands, Portugal, Spain, Switzerland and the United Kingdom.



The referral activity targeted online content on explosive chemical precursors which were being shared among terrorist supporting networks, including jihadist, right-wing and left-wing terrorist networks.
The action day resulted in **563 pieces of content on 106 websites** and platforms being assessed for referral to online service providers for their voluntary consideration against their terms and conditions.
The content included manuals and tutorials which gave instructions, among other things, on how to make bombs with the use of precursors and how to prepare and carry out terrorist attacks.
This action was part of a series of similar joint actions which have taken place in the past and will continue to be organised frequently.

●▶ **To know more about the work of the EU IRU,** read the dedicated feature story.

In Iraq, the Bitter Legacy of War Still Lies Hidden Underground

Baghdad can't rebuild its infrastructure and agricultural sector when its land remains littered with thousands of explosive devices.

FEBRUARY 12, 2022, 6:00 AM

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

CYBER NEWS

C2BRNE DIARY

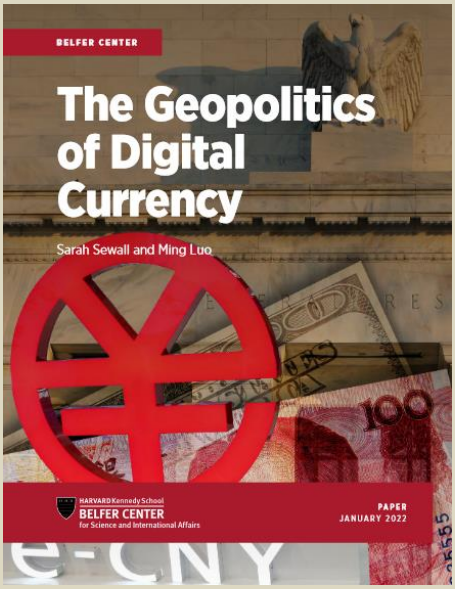
The Geopolitics of Digital Currency

By Sarah Sewall and Ming Luo

Belfer Center for Science and International Affairs | Harvard Kennedy School

Source: https://www.belfercenter.org/sites/default/files/files/publication/Geopolitics%20of%20Digital%20Currency%20-%20Sarah%20Sewall%20Ming%20Luo.pdf

January 2022 – The U.S. Federal Reserve, Treasury Department, and Congress have begun considering the viability of a Central Bank Digital Currency (CBDC), a legal tender national digital currency for consumer use. They are understandably focused on domestic policy issues such as potential impact on U.S. financial stability or expanding public access to financial services. The national security implications of CBDCs are not yet central considerations for U.S. policymakers, but they should be. Digitized currency is data. Digital currency will move across international borders, potentially revealing information harmful to individual, corporate, or national interests. The United States could play a critical role in fostering open and collaborative technologies that protect this data – upholding privacy and security standards while maintaining lawful auditability in a fully digital economic world. But the United States lags other nations in its consideration of a CBDC. China has been working toward a CBDC for almost a decade. It will be first among the world's major economies to widely deploy a retail CBDC. Accordingly, China is well positioned to shape the global standards and processes governing this financial transformation. The results could transcend data privacy and security. New global payment exchanges could undermine components of the international financial system that enhance U.S. financial power and help sustain norms of international behavior. Vulnerable components include the SWIFT2 messaging service, which facilitates the movement of money across international borders and, among other things, is fundamental to the U.S. financial sanctions regime. American leadership will be required to adapt international financial systems to CBDC technologies without compromising U.S. interests. These considerations should inform and accelerate U.S. consideration of a CBDC and prompt greater American engagement in developing global standards and cross-border payments processes.



Sarah Sewall is Executive Vice President for Policy of IQT and a Senior Fellow at the Belfer Center. She served as Under Secretary of State under President Obama and Deputy Assistant Secretary of Defense during the Clinton Administration. In the interim decade, Dr. Sewall taught at the Harvard Kennedy School. She recently co-authored "The Innovation Wars: America's Eroding Technological Advantage" in Foreign Affairs.

Ming Luo is a Vice President of Technology at IQT, where he investigates emerging technology spaces—including financial/identity intelligence and agile IT infrastructure—in order to make investments in startup companies to empower the U.S. national security mission. Prior to IQT, Ming was a research engineer at BAE Systems where he focused on wireless networking and cyber ops technologies.

Hidden Cybersecurity Challenges of Smart Buildings

By Amy Mintz

Source: https://www.hstoday.us/featured/hidden-cybersecurity-challenges-of-smart-buildings/

Jan 25 – In October 2021, a rare form of a cyberattack took place on building automation system (BAS) devices at an office building in Germany. Unauthorized access into a building automation engineering firm's BAS system locked the owners out of the system and rendered three-quarters of several hundred BAS devices in the building nonoperational, affecting the lighting, motion detectors, window shutter controllers and more. There was no ransomware demand, nor any trace of digital footprints left behind.

The office building BAS devices were able to be restored after weeks of resorting to manual controls, without any other reported damages. But cyberattacks on smart buildings have the potential to wreak much larger havoc and even loss of life, as many BASs also connect to systems for security and alarm systems, elevator operations and fire safety.

Similar cyberattacks on BAS systems based on KNX technology (a building automation standard commonly used in Europe) have been reported to Limes Security, the industrial

control system (ICS) security firm that recovered and restored the infected BAS system.[1] However, many cyberattacks on smart buildings may go unreported. As shared by David Olive, Founder and Principal of Catalyst Partners, government officials at the Cybersecurity and Infrastructure Security Agency (CISA) and Federal Bureau of Investigations (FBI) have repeatedly acknowledged the reluctance of individuals, businesses and even cities to disclose cyberattacks when they happen, often due to their difficulty in understanding the type, technical impact and cause of the attack and because of concerns about legal liability exposure where the ability to mitigate the impact of customer disruption and potential litigation is too uncertain.

Again, reports of BAS cyberattacks are considered rare, as of now. However, smart buildings have serious potential to be a ransomware target. Smart buildings bridge cyber and physical security, and with the many benefits that such connectivity brings is also the potential for catastrophic damages.

Olive pointed to the relatively small cost to attackers in return for the ransomware amounts they seek, especially when it comes to critical infrastructure owners and operators. In June 2021, CISA published a fact sheet on the growing ransomware threat to operational technology (OT) for critical infrastructure owners and operators. There was a 150 percent increase in ransomware attacks in 2020 compared to 2019, and ransomware payouts rose even higher to 300 percent.[2]

As with many critical infrastructure sectors, the threat of ransomware is also growing as a significant concern in the Commercial Facilities Sector. The Real Estate Information Sharing and Analysis Center (RE-ISAC), overseen by The Real Estate Roundtable, is a public-private partnership between the U.S. Commercial Facilities Sector and Department of Homeland Security (DHS) officials that disseminates information about potential physical and cyber security threats and vulnerabilities to the Commercial Facilities Sector specifically.

However, while the RE-ISAC as well as other organizations and federal agencies such as the National Institute of Standards and Technology (NIST) do issue best practices and security recommendations for cyber risk management, it is ultimately on the smart-building stakeholders involved to designate who shall be responsible to implement security recommendations and maintain the quality of the system over the lifetime of the building.

In this particular cyberattack on the BAS in an office building in Germany, the hackers infiltrated the BAS through an unsecure port, a vulnerability that could have easily been mitigated. The KNX Association has long warned against leaving ports open among their security recommendations for customers.

This gives prominence to an often-overlooked challenge with securing smart buildings. Scott Tousley, former Deputy Director of the Cyber Security Division at DHS Science and Technology, noted that in addition to the technical challenge of securing BASs lies the second challenge of governance gaps and confusion. Who bears the responsibility of

managing the cybersecurity and maintenance of BASs in smart buildings? Aside from larger skyscrapers, many buildings are not operated as active enterprises, and are not well prepared or equipped to properly secure these more complex systems.
Facilities management staff and IT personnel may likely be unknowledgeable in the other's field of expertise, and knowledge of both is essential to adequately secure smart buildings. A study by Phobos Group reported that more than 38,000 BASs in the United States were exposed on the internet – without even a default password. Other statistics shared by security companies are just as concerning, with an audit revealing that nearly 60 percent of BAS customers did not have a firewall installed.[3] This lack of the most basic cybersecurity measures for BASs is beyond troubling.
As emphasized by Tousley, upholding quality levels in smart buildings will require decades of maintenance, and sustaining quality operations over the lifetime of the building will be a real challenge. Believe it or not, some of the legacy IT systems still used by government agencies and commercial entities date back to the 1980s or even older; and the numerous problems associated with such outdated systems include billions of wasted dollars, system outages, malfunctions and defects, and critical vulnerabilities to cyberattacks resulting in data breaches and ransomware attacks.[4]
As reported in *Forbes*, critical vulnerabilities exist within IT, OT and ICS supply chains; and there are many entry points and vulnerabilities in legacy OT systems.[5] Aside from disrupting building operations, OT systems are also targeted as an entry point to compromise corporate IT systems for data breaches. An early known case of this was the Target store hack in 2013, when hackers used the HVAC vendor as an entry point to steal over 40 million customers' payment card information. Another example reads like a blend of a *Mr. Robot* TV episode and the *Ocean's Eleven* movie, when hackers infiltrated a casino's mainframe in 2017 to steal 10 gigabytes of data via sensors in a fish tank connected to the Internet.
Fortunately, as of now, reported cyberattacks on BASs have not resulted in loss of life or significant physical damages. But the escalating threats to smart buildings may not always be "just" data breaches or ransomware demands for payment in exchange to restore data. Unfortunately, as history has shown us, it often takes a catastrophe to trigger action. Hopefully, smart-building stakeholders will take action now to implement the proper cybersecurity measures before a tragic cyber incident occurs.

References

[1] See Kelly Jackson Higgins, https://www.darkreading.com/attacks-breaches/lights-out-cyberattacks-shut-down-building-automation-systems
[2] See Richard Tracy, https://www.forbes.com/sites/forbestechcouncil/2021/07/20/turning-up-the-heat-a-ransomware-attack-on-critical-infrastructure-is-a-nightmare-scenario/
[3] See William Hughes, https://facilityexecutive.com/2021/05/cybersecurity-concerns-continue-for-building-systems/
[4] See Robert N. Charette, https://spectrum.ieee.org/inside-hidden-world-legacy-it-systems
[5] See Chuck Brooks, https://www.forbes.com/sites/chuckbrooks/2021/04/12/3-key-cybersecurity-trends-to-know-for-2021-and-on-/

Amy Mintz is a PhD Candidate in Counterterrorism at Capitol Technology University. Her doctoral research is focused on ways to contribute to the cyber forensics domain by applying counterterrorism techniques to mitigate challenges of protecting critical infrastructure in smart cities. Her academic background includes an M.S. in Digital Forensics and Graduate Studies in Cybersecurity Policy, and Curriculum and Instruction. She recently co-founded the AAPI Institute, a nonpartisan think tank that focuses its research on topics central to the well-being and security of the Asian American Pacific Islander (AAPI) community to educate and raise awareness of these issues.

Ensuring Safe Nuclear Waste Disposal

Source: https://www.homelandsecuritynewswire.com/dr20220126-ensuring-safe-nuclear-waste-disposal

Jan 26 – When it comes to nuclear power, the uranium at the heart of fuel rods is also this power source's Achilles' heel. When power plants shut down or the fuel rods in nuclear reactors become inefficient, the high-level nuclear waste resulting from the spent fuel created from running these plants could stay radioactive for thousands of years. Disposal concepts call for the waste to be isolated a third of a mile belowground for safe storage, enclosed within engineered barrier systems and surrounded by subsurface rock.
But there's still the chance radionuclides might leak out if these systems lose their protective properties as it heats up due to radioactive decay. That means a lot of research effort is focused on the temperature limit up to which these systems and the natural geologic environment can be exposed.
Now geoscientists from Lawrence Berkeley National Laboratory (Berkeley Lab) and two other U.S. Department of Energy (DOE) National Laboratories, Sandia and Los Alamos, are collaborating on the HotBENT project. This international field experiment is evaluating how

well the natural, clay-based material (bentonite) placed around canisters of buried, high-level nuclear waste retains its safety functions when exposed to simulated long-term heating.

"The concern is that heat emitted by underground nuclear waste will change the geophysical and geochemical properties of the bentonite buffer and the host rock," said LianGe Zheng, Berkeley Lab's lead scientist on HotBENT, whose previous computer simulation studies at Berkeley Lab helped initiate the HotBENT research. "For this long-term series of experiments, we will evaluate the thermal, hydrological, chemical, and mechanical changes in the bentonite and how that affects the material's safety function over time."

The HotBENT project led by Nagra (Switzerland's National Cooperative for the Disposal of Radioactive Waste) involves the DOE and partners in Canada, Japan, the U.K., and elsewhere. A demonstrated higher temperature tolerance could allow for more radioactive waste to be safely packed within tunnels in the Earth's subsurface.

Large-scale experiment at the Grimsel Test Site

International Project Development

Although the U.S has not identified a new site for long-term disposal of highly radioactive byproducts of nuclear power since Congress stopped funding the Yucca Mountain site in 2010, Finland has begun constructing a deep underground repository for such waste, and other countries are at some stage of considering repository locations for highly radioactive waste.

The HotBENT field test began in September when scientists started to deploy heaters within the research tunnel at Switzerlands's Grimsel Test Site, a designated underground testing facility for radioactive waste disposal. At power plants, heat generated from radioactive materials normally develops when a type of uranium undergoes a fission reaction, which releases energy in the form of heat and the generation of fission products. The temperature of the four heaters in the HotBENT field test will be slowly raised over the next several months to eventually reach 200 degrees Celsius – twice the current maximum allowable temperature under consideration for similar repositories. The team has set up a large array of sensors to detect temperature and corresponding hydrologic and mechanical changes in the bentonite buffer and the surrounding rock.

Previous research by Zheng suggested that, at twice the widely used maximum temperature, the soft, clay-based bentonite does not lose much of its protective properties. Bentonite is

being studied partly because the natural material would swell when water reaches it within an underground repository (due to groundwater percolation at depth). The clay material's swelling ability can help protect canister waste from escaping because of interactions with fluids that would be less able to travel through swollen bentonite.
Zheng's modeling study, published in *Engineering Geology*, indicated that about two-thirds of the key, swelling-related mineral in bentonite clay (smectite) had degraded at 200 degrees Celsius rather than 100 degrees Celsius. Yet the ability of the bentonite to swell as part of its protective function only decreased by 4% at most in the simulations.
"If the Swiss test site can largely verify the modeling results, then the bentonite buffer may be able to retain much of its protective function at much higher temperatures than previously considered," said Zheng, noting this would allow tighter spacing, and more waste canisters, to be placed inside underground repositories, reducing the size of their overall footprint.

The Laboratory Approach
To supplement the HotBENT field test experiments, scientists at Berkeley Lab, and Sandia and Los Alamos National Laboratories are doing modeling and laboratory work.
Zheng and his colleagues are simulating the field test setup in the laboratory using column tests about one-tenth the size of a single heating element at the Switzerland underground field test site. In the lab, the scientists will be looking at changes in the materials over a year and a half compared to five- and 15- to 20-year periods in the field. A particular focus will be understanding how much smectite degrades into another clay mineral (illite) that lacks the ability to swell.
Meanwhile, colleagues in one of Sandia's nuclear fuel cycle research departments will analyze geochemical changes in bentonite samples sent from Zheng's scaled-down column experiment — and directly from unheated samples at the Swiss test site.
"We want to know if high temperatures cause the minerology of the bentonite buffer to change, potentially affecting its properties like permeability and radionuclide adsorption," said the department's manager, Emily Stein. "It's really important for developing the safety strategy for deep geologic repositories to understand these temperature-related processes."
Sandia scientists led by Carlos Jové Colón will be investigating whether the heating tests at Berkeley Lab alter bentonite's ability to swell, and how the raw material at Grimsel responds to being heated to 60 and 90 degrees Celsius. In addition, they will analyze the bentonite sample's chemical composition, such as for the presence of the breakdown material illite, and analyze structural changes in the clay.
A research group led by Florie Caporuscio at Los Alamos National Laboratory has been studying how a mixture of bentonite and other engineered barrier materials respond to heating. They will also test types of host rock the canisters may be buried within, with the goal to see how the overall combination of materials responds to temperatures of up to 300 degrees Celsius.
"It's important to analyze a range of conditions such as possible host rock materials like the granite, clay rocks, and so on, to inform decisions about the most suitable underground location for these nuclear repositories," Zheng said.

Iranian Cyber Influence Operations against Israel Disguised as Ransomware Attacks

By Boaz Dolev and David Siman-Tov (senior research fellow at INSS)
Source: https://www.inss.org.il/publication/cyber-iran/

Jan 27 – The past two years have witnessed cyberattacks attributed to Iran targeting companies and organizations in Israel that are ostensibly ransomware, but in fact are undertaken as influence operations. Notably, ransomware attacks have been very common in recent years, and have been defined by the White House as a central cyber threat. Still, the use of ransomware attacks for the purpose of influence operations rather than for an economic purpose is a singular phenomenon. This phenomenon is unique to the framework of the conflict between Israel and Iran or its supporters. The following article describes the results of research on ransomware attacks from the past two years that targeted the Israeli private sector with an influence operations purpose. The basis of attributing the attacks to an organized Iranian array will be elaborated, as well as methods of distinguishing imitated ransomware attacks, the Iranian groups involved alongside their tools, strategic insights, and possible ways of coping with the phenomenon. The described research was carried out by the ClearSky Cyber Security company for the Institute for National Security Studies (INSS). ClearSky cooperated with researchers from the field of psychological operations warfare and from the Iran program at INSS.

Challenges and Major Concerns in Health Sector Cybersecurity

By Or Shalom

Source: https://i-hls.com/archives/112896

Feb 01 - Cyberattacks targeting the health sector have intensified following the COVID-19 crisis. The US Department of Health and Human Services and the Office for Civil Rights report published recently has unveiled hundreds of information security events during the last 24 months (attacks that caused harm to systems, information leak, ransom attacks, and more). The attacks targeting the health sector have reflected the capability to cause damage, shut down critical systems, and steal medical records and patient information. These trends require an evaluation and security-bound thinking regarding the assailant and his goals in order to minimize the attack surfaces in this sector.
The requirement to keep operations going on alongside the need to secure the information security triangle (CIA) in order to prevent risks regarding the information integrity, availability and confidentiality raises quite a few planning challenges. These will be elaborated on from various aspects and arenas.

Air gap networks for minimizing risks

The installation and expansion stage (according to the Cyber Kill Chain attack model and the like) can have implications for the organization's cross-cutting functioning ability. As per this method, an attack on an emergency ward receptionist's computer might have cross-cut implications for the management networks. Implications may include patient acceptance processes, and expand to operational networks and critical systems (such as the robotic systems at operating rooms, structure systems, or even systems supporting operating rooms). Air gaps should be planned for dedicated zones as part of the preparedness for cyber crises and in order to ensure the continuity of other wards. Balancing between the convenience of use and user experience and operational security needs requires the use of a range of technologies to support work processes in air-gapped environments.
For example, updating a large number of air-gapped systems could be cumbersome. A solution and a more convenient operational response are required. A one-way diode can offer more flexible operation while monitoring the information direction (one-way), authorized file types and protocols, and transfer timing.

Controlling communication-based components (OTA – Over the Air)

Purchasing advanced technological systems and robotics in the health sector means better medical services. These systems are based on analytics, AI, and ML (as part of the optimization processes), quicker processing, and the optimal use of the big data space. These systems have OTA connectivity in various channels, such as IoT.
This fact enables operational flexibility and mobility of systems within and outside the hospital without using complex cables and connections. During the COVID-19 period, systems can be easily transferred from one ward to another for treating or diagnosing COVID patients that can not reach the specific ward.
On the other hand, from the point of view of cyber, it becomes hard to monitor, manage and control these systems, as each ward can purchase an autonomous system independently of any computing resources or stakeholders (sometimes without their knowledge). There is also the challenge of managing different components from various manufacturers and with a variety of protocols. The key to minimizing risks in this arena lies in the capability of new technologies to detect systems in IoT-based communication (and others), to acquire capabilities in order to obtain control, monitoring, and management (e.g. controlling the processes, timing and mode of communication, protocols, etc.)

Manipulation of medical systems and devices

A Ben-Gurion University research conducted two years ago has proved a threatening attack capability. The researchers showed that hackers can interfere with medical 3D scanning processes by deceiving radiologists and falsifying cancer diagnostic results. The research demonstrated the ability of a hostile actor intervening with communications as man in the middle (MITM) in order to maliciously add or withdraw some radiological findings in 3D images, thus influencing the process of cancer metastasis diagnosis.
Moreover, the research demonstrated the preparations of the attacker at the hospital in a way that enables him to take advantage of access points to the computer infrastructure for secreting a component that allows the attack. This demonstration stresses the need for suitable balance and synergy between the physical access security teams and the cybersecurity teams. They should collaborate in defining the critical computing infrastructure by analyzing the manipulation opportunities also at the physical space (which is even more important in the case of public places, that are more attractive and easy to operate for the attacker).

Records cybersecurity and privacy risks

The attacker is driven by various goals, including commercial espionage, crime, and ransom, as well as the drive to steal organizational data and information, mainly patents, formulas, customer lists, patient lists, and medical records. Attacks are also motivated by the desire to harm research companies (especially developers of medical technologies for COVID), medical startups, etc. The information collection efforts include the internet network as a whole (e.g. using FOCA tools, etc.) as well as focused attacks that cause information leaks from within the organization. A major challenge characterizing the digital organizational environment is the fencing of the risk and the prevention of sensitive information leaks.

Planning the controls against such a threat should be based on the understanding that information that leaked is not anymore under the organization's control. Therefore, DLP solutions and prevention controls should be applied. The maintenance of DLP systems in large organizational systems with the various digital patterns, such as using mobile devices outside the organization, poses a genuine challenge. In addition, the need to index information, change it and adapt it for categorization and classification turns the event into a dynamic and complex one. There are currently some intriguing technologies, based on AI and ML and automation in mapping sensitive information (on the basis of known patterns from other environments) that can save the organization costs, time, and human resources.

As part of the processes of organizational efficiency, flexibility, and rapid response, health sector organizations and suppliers use mobile devices for storing, processing, retrieving and transferring information, including regarding patients. This mode of operation can be targeted for attacks and exposes the organization to cyber attacks. Of course, this state of affairs has implications for future judicial risks (possible lawsuits), insurance issues, and the organization's reputation.

A NIST publication from 2018 elaborated on securing electronic health records on mobile devices. The publication was accompanied by lab tests (NCCoE) simulating possible realistic attack scenarios and evaluating controls and defense methods. According to one scenario simulated by the researchers, a medical doctor uses her private mobile device for transferring a patient's clinical data. They also simulated an incident in which a patient or a physician send an electronic prescription to the pharmacy. Using private devices opens the way to quite a few manipulations in cyber-attack and fraud.

NIST's publication also referred to encryption requirements in the application of technological controls based on zero-trust architecture regarding the device, entity, and of course, the network.

Or Shalom is a security and cyber expert and consultant to government ministries and defense industries, international business development consultant for companies in the fields of HLS and cyber and leads centers of excellence and advanced training programs in Cyber and HLS for various organizations in the civilian, security, industry, and academic sectors. He holds a master's degree, as well as civil and national qualifications in the realm of HLS and Cyber Security. He has experience in security, innovation, planning and characterization of technological security systems, HLS, and Cyber preparedness.

Cyberattacks on Critical Infrastructure as the New WMD

By Ted P. Delacourt

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/cyberattacks-on-critical-infrastructure-as-the-new-wmd/

Feb 01 – Should the acronym WMD, which stands for "Weapons of Mass Destruction," be updated to "Weapons of Mass Disruption?" I think it is a timely question in this Digital Age as we connect and integrate billions of new digital devices into our lives and business processes and when a cyber-attack against one supply chain provider can lead to cascading effects on entire communities across the globe. Cyberattacks on Critical Infrastructure (CI) can cause mass economic and societal impacts. Fewer strategies than cyber-attacks can offer better plausible deniability and can cause greater anxiety and instability to our society than targeting the systems and networks that enable our day-to-day activities. Consider that 20 years ago terrorists killed 3,000 Americans and disrupted the entire U.S. and global economies with only four planes. Given the growth and ubiquity of technology today we must consider how the exponential growth of cyberattacks on CI might be similarly leveraged by adversaries and criminal actors as Weapons of Mass Disruption, the new WMD.[1]

Cyberattacks take many forms, often progressing through multiple phases as they escalate in severity. Malicious actors often initiate a network intrusion through phishing campaigns or the purchase of compromised user credentials on the dark web. What begins as the hijack of a single user profile expands in severity. Intruders move laterally across internal systems, conducting surveillance and gathering intelligence on network environments before escalating to data theft, service disruptions, and ransomware extortion.

The goals of these actors may be both strategic and economic in nature, and targets may be government and/or the private sector. Cyberattacks perpetrated on CI elements develop into the new WMD when the intended and unintended consequences cause widespread

damage and societal impacts. A disruption of essential services, even if brief, can occupy significant civilian and military resources in a region or entire country.[2]
Russian military doctrine views the battle of the information space, to include cyber activities, as unending.[3] As such, the bar to initiate cyber-attacks appears low and the past two decades have witnessed numerous cyberattacks on CI around the world. The march toward a more interconnected and networked world increases the likelihood that cyberattacks against CI could be used as the new WMD. In this new threat environment, more than ever we need to increase and leverage government and private-sector partnerships to mitigate and neutralize these cyber threats.

Cyber Threat Technology

Cyber threats combine numerous attack vectors and strategies in a single attack. Common attacks include malware, denial-of-service attacks, phishing, structured query language (SQL) injection, and zero-day exploits. Some attacks specifically target critical nodes, software, or people, while others overwhelm internet websites with massive, automated amounts of data requests. Malware attacks install malicious code, transmit sensitive data, and corrupt, destroy or deny access to data by overwriting or encrypting files, often referred to as ransomware. Phishing attacks target users with false messages that request they open a file or access a link that secretly installs malware. SQL injection attacks insert malicious code into servers running SQL database software to reveal sensitive data not normally available. Vectors for SQL injections include inserting malicious code in search boxes of vulnerable web pages. These attack opportunities persist due to inconsistent patch implementation and failure by end users to employ cyber best practices, often called cyber hygiene, which increase the risk of cyber-attack on vulnerable systems. Zero-day exploits, alternatively, may be known vulnerabilities that lack immediate solutions. Even if a zero-day exploit is known, the threat continues until a patch is developed and the end user installs it. The combination of attack vectors with new and old malware options creates opportunities for both intelligence gathering and development of mass disruption strategies of CI operations by and against U.S. adversaries.[4]

Critical Infrastructure Sectors

Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience identified 16 sectors and identified specific federal agencies charged with their security. PPD-21 addressed the reality that advances in technology led to increases in each sector's interconnectivity and reliance on online and networked resources to accomplish their fundamental missions. [5]

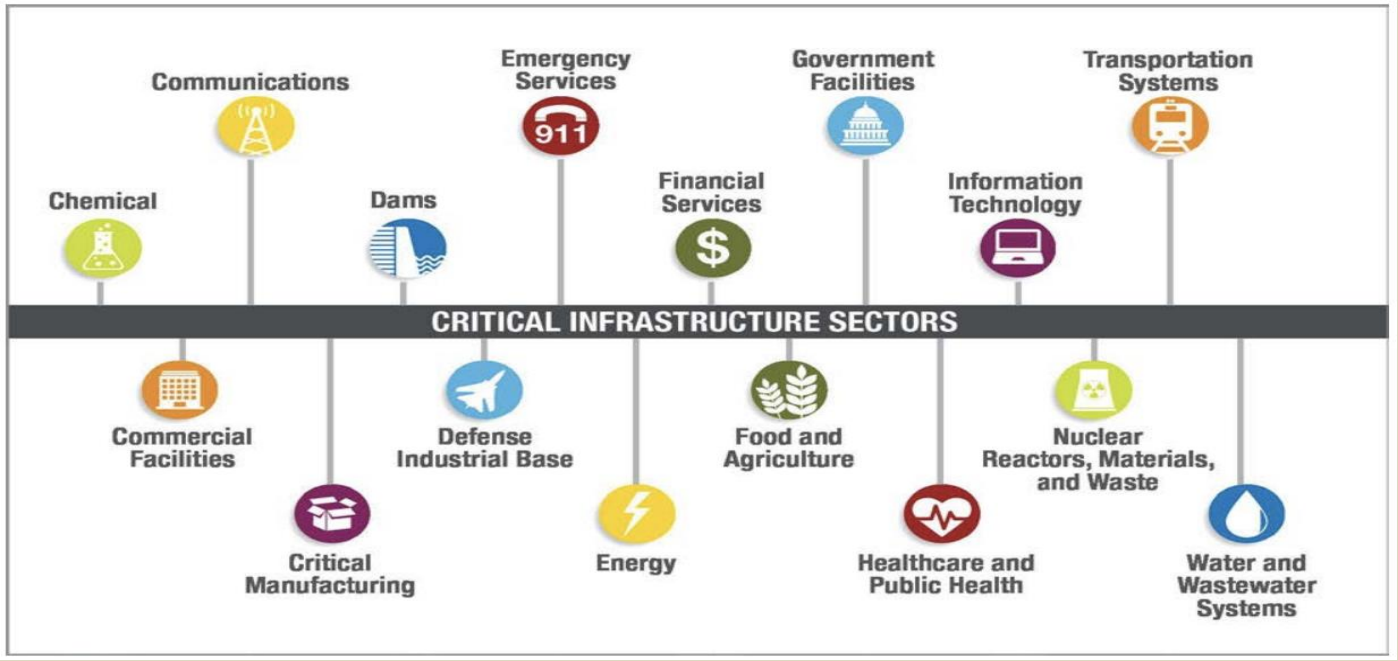


Figure 1 – PPD-21 16 Critical Infrastructure Sectors (Source: CISA.gov) [6]CI elements do not stand alone, but rather are interconnected and interdependent. This interconnectivity makes them vulnerable to direct and indirect cyber threats. An attack on one may initiate a failure in another or cascade to the entire interconnected CI network. The mix of public, private, and non-governmental operations across each CI sector complicates remediation of identified vulnerabilities and information sharing on actual or potential attacks. The ubiquitous nature of these CI sectors and the distribution of their physical and networked assets across a wide geographical area, often spanning the entire country, make CI sectors attractive targets. State, non-state, and criminal actors continually seek victims of opportunity across all CI sectors for monetary and strategic gain.[7]

Past Attacks on Critical Infrastructure

The threat against CI elements is neither theoretical nor improbable. Cyberattacks have occurred independently and as part of multi-domain conflicts involving Russia, China, and others over the past two decades. Connell and Vogler described the Russian military view of cyber operations as part of the larger concept of information warfare, and not a distinct tactic. They assessed that in line with traditional Soviet military thinking, Russian decision-makers view the battle for the information space as unending. Such a doctrinal view of an information space in constant conflict stands in sharp contrast to the U.S. view. Furthermore, Russian decision-making informed by this view likely sets a low bar for the initiation of offensive cyber operations.[8]

In 2008, cyberattacks attributed to Russia disrupted Georgian government websites, financial institutions, private telecommunications companies, and other organizations in the opening stages of the military conflict between the two countries over breakaway regions. Given the limited nature of Georgian information technology at the time, the impact of the cyber operations was reduced. This application of cyberattack methodologies, however, stands as the first large-scale use of cyber operations in support of a military conflict. In this multi-domain example, a cyberattack designed to cause widespread disruption preceded a physical attack. [9]

In December 2015, the Ukrainian Energy Minister attributed the first known power outage caused by a cyberattack to Russian actors, when three power distribution companies were targeted. The timing and coordination among the attacks across central and regional facilities pointed to a high level of sophistication. The subsequent investigation revealed an initial intrusion occurring at least six months prior, allowing the actors to gather intelligence on company operations and likely remediation responses. This surveillance allowed the cyber actors to insert additional malware to wipe key recovery servers and computers to stymie restoration efforts. The attack left approximately 225,000 customers without power for six hours in the middle of a Ukrainian winter. The investigation also revealed the attack could have been larger, and the damage permanent, but the cyber actors chose to limit the scope. This points to the scalability of damage from the spectrum of cyberattack methodologies and their potential as a WMD.[10]

In the spring and summer of 2020, the People's Liberation Army (PLA) of China and the Indian Army were involved in multiple skirmishes in the vicinity of the Actual Line of Control that defines their common border in the Himalayas. One such engagement resulted in the deaths of 20 Indian soldiers. Unwilling to back down, that August the Indian Army seized additional strategic locations. In an apparent tit-for-tat response, hostilities escalated and entered the cyber domain when a power outage struck the power utility in the Indian state of Maharashtra, which includes India's financial capital Mumbai. The attack was attributed to a group known as RED ECHO, potentially a state-sponsored group affiliated with China's PLA Strategic Support Forces. In response to the cyberattack, India mobilized additional troops to the disputed region and expanded the hostilities into the economic domain – India banned Chinese mobile apps, limited Chinese investments in India, and joined an informal grouping of the U.S., Japan, and Australia dedicated to limiting Chinese advancement in Indo-Pacific. In this multi-domain example, the cyberattack causing widespread disruption was a response to the physical attack, which was met with economic sanctions.[11] Such an attack against such a large power grid and financial capital could be characterized as a WMD attack.

In their 2021 study, Izycki and Vianna defined a cyberattack as an operation conducted with a kinetic intent or result. Using this definition, they identified seven significant cyber-attacks between 2010 and 2019. Their results are illustrated in the table below.[12]

Campaign	Starting Year	Attribution	Countries Affected	Targets
Stuxnet	2010	US and Israel	Iran	Uranium enrichment plants
Dragonfly 2.0	2015	Russia	Switzerland, US, Turkey and Ukraine	Electricity, nuclear, water supply and aviation sector
Shamoon	2016	Iran	Saudi Arabia	Aramco and Saipem S.p.A.
BlackEnergy	2017	Russia	Ukraine	Electricity distribution network
NotPetya	2017	Russia	Ukraine, but with global effects	Finance, transportation, energy, and healthcare
Industroyer	2017	Non-attributed (Russia)	Ukraine	Electrical substations
Triton/Trisis	2017	Russia	Saudi Arabia	Oil companies

Table 1 – Campaigns Against CI with Physical Consequences/Intentions (Source: Izycki and Vianna)

The attributions noted by Izycki and Vianna, if accurate, highlight how various actors employed cyber weapons across a wide range of political conflicts and actors. The authors concluded that the small number of campaigns highlighted the rarity of what they termed "kinetic attacks" against CI assets. Cyberattacks on CI sectors like those noted by Izycki and Vianna have the potential to cause massive disruptions and societal displacement if the underlying interconnected computer systems were destroyed or disabled for extended periods.[13]

Discussion of the Threat

Cyberattacks on interdependent CI sectors have the potential for secondary and tertiary effects in addition to the cascade of physical disruption that follows.[14] Beyond impairing physical assets, cyber-attacks on the foundational services of a society also function as psychological and strategic weapons. CI disruptions may undermine confidence in the state to provide security or basic services. Such attacks may serve as existential threats to unstable regimes. As strategic weapons, cyberattacks on CI causing mass disruptions have the potential to tie up significant military and economic resources at the same time the nation faces a military threat. Such attacks have the potential to fully occupy the time and attention of decision-makers as well as field commanders, causing them to miss or ignore other pending threats. This exemplifies the multi-domain use of cyberattacks.[15] Recently, plans purportedly developed by units within Iran's Islamic Revolutionary Guard Corps (IRGC) leaked to a British reporter described various cyberattack strategies for cargo ships, building HVAC systems, and fuel pumps manufactured in the U.S. and sold worldwide. If authentic, such plans highlight in detail how CI sectors might be attacked via the cyber domain.[16]

Based on the attacks studied, the threshold for initiating a cyberattack appears low, and not all attacks produce an immediate or identifiable impact. Attacks may occur unnoticed, with bad actors lying dormant within systems for an extended time period. The nature of an attack may change over time, in that an intrusion may progress to an intelligence-gathering operation and data theft, before escalating into a denial-of-service or ransomware attack. The progression of an attack may change depending on the nature of the actor. The goal of non-state or criminal actors in conducting cyberattacks may be profit-driven or center on causing economic damage, while state actors may favor intelligence gathering and the creation of strategic options or outcomes. In the case of North Korea, the goals may be both financial and intelligence gathering, as they gather technical knowledge and the financial means to purchase necessary materials and equipment. The ubiquity of networked systems and the wide availability of cyber intrusion tools leave no country or critical infrastructure sector immune.[17]

Determining attribution for an attack is difficult. The use by cyber actors of Virtual Private Networks (VPNs), leased server infrastructure, and the cross-border nature of the internet complicate attribution efforts. Intelligence services can be reluctant to publicly disclose sensitive techniques and classified information in order to explain attribution conclusions. Additionally, public prosecution of these malicious actors may risk disclosure of investigative techniques, particularly in national security investigations. Complicating the matter further, cybercriminal organizations frequently operate from countries unwilling to arrest and extradite malicious actors to the United States. As a result, there appears to be limited consequences levied on adversaries for intrusion or intelligence-gathering activities. For example, in July 2021, in the same week the U.S. and NATO allies publicly identified the Chinese Ministry of State Security (MSS) as the perpetrator of the hack of the Microsoft Exchange email server uncovered three months prior, the U.S. Department of Justice filed motions to dismiss visa fraud charges against five Chinese scientists accused of concealing their ties to the PLA. This public shaming of cyber aggression by the MSS did not include economic sanctions against China, while a similar public disclosure in April 2021 about Russia included economic sanctions its cyber actions related to election interference.[18]

Conclusions and Judgments

Cyber intrusions utilize a volume attack scenario, leveraging automated software to continually probe end points and network connections for vulnerabilities. Hackers count on the incomplete implementation of software patches and poor cyber hygiene to provide illicit access. The assessment, based on this research, is cyberattacks on CI will continue to grow in number and frequency and continue to escalate in severity. As the world becomes more reliant on systems connected to the internet the attack surface expands. CI sectors are no exception, and their interconnectivity creates a risk of a failure cascade. Furthermore, cyberattacks are becoming automated and more anonymized. Consequently, if we have not yet met the threshold, we may soon, where cyberattacks against CI with large-scale impacts may be characterized as WMD.

The interwoven nature of CI sectors crosses international boundaries. To address the disruptive threats of cyberattacks against CI, facilities and their control networks must be hardened and continuously monitored for intrusions and anomalous activities. PPD-21 specifically identifies what was to be protected and which agency was to lead efforts for each sector. The identification, analysis, and mitigation of malware and the illicit marketplaces where it is sold remains of critical importance. Cyberattacks weaponize CI infrastructure to cause widespread disruption in addition to serving as an enabler for other adversarial intelligence activities.[19]

●▶ **References are available at the source's URL.**

Supervisory Special Agent **Ted P. Delacourt** is a federal civilian working in the Mission Critical Engagement Unit, Cyber Division, Federal Bureau of Investigation. SSA Delacourt has over 17 years of experience in law enforcement, counterterrorism, and intelligence issues. He holds a Bachelor of Science of Business Administration with a concentration in Accounting from Georgetown University, McDonough School of Business; a Master of Business Administration with concentrations in Finance and Economics from the University of Chicago, Booth School of Business; and a Master of Science and Technology Intelligence from National Intelligence University, Oettinger School of Science & Technology Intelligence.

Assessing military cyber maturity: strategy, institutions and capability

By Greg Austin

Source: https://www.iiss.org/blogs/research-paper/2022/02/assessing-military-cyber-maturity

Feb 03 – Few governments have reached an enduring consensus on just how quickly and how deeply reforms to their military cyber forces must be made. While consensus points have been reached, these are usually tested within a short period of time by international circumstances and technological trends. The main dilemma is whether military cyber strategies and capabilities need more than routine development as just one more element of military power, or whether they warrant radical development pathways and a higher priority than others.

One of the most profound influences on the evolution of a country's military cyber forces and strategies is politics. This paper offers insights into how the governance and organisational factors of domestic politics facilitate or inhibit the dissemination of cyber concepts and capabilities throughout military forces beyond the main signals or cyber intelligence agency.

There are at least three reasons to analyse military cyber maturity. The countries currently pursuing such capabilities are not satisfied with the development levels in policy and strategy they have so far reached. There is increasing potential for crippling cyber-attacks on key elements of military capability or supporting infrastructure. And no country has yet succeeded in the broad dissemination of cyber capabilities through its armed forces in ways that leading military planners would like.

Few governments have reached an enduring consensus on just how quickly and how deeply reforms in the armed forces must be made to satisfy national security needs. While consensus points have been reached, these are usually tested within a short period of time by inter-national circumstances and technological trends. The main dilemma is whether military cyber strategies and capabilities need more than routine development as just one more element of military power, akin to artillery or submarines; or whether they are sufficiently transformative of military power to warrant radical development pathways and a higher priority than others.

This paper provides an impact matrix which can be used by governments, their armed forces and research analysts to understand the ways in which military cyber reforms can be facilitated or inhibited by governance and organisational processes.

●▶ **Download the research report**

Greg Austin is a Senior Fellow for Cyber, Space and Future Conflict based in the Singapore office of the IISS.

NSA Releases 2021 Cybersecurity Year in Review

Source: https://www.homelandsecuritynewswire.com/dr20220208-nsa-releases-2021-cybersecurity-year-in-review

Feb 08 – The National Security Agency the other day released the 2021 NSA Cybersecurity Year in Review to highlight how the agency continues to address threats to the U.S. most critical systems.

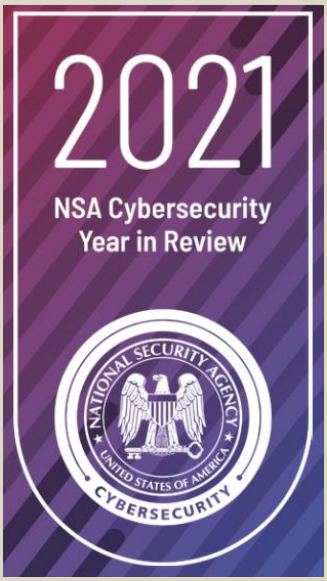
The Year in Review shows the scope of the NSA's cybersecurity mission, "from securing key Department of Defense weapons and space systems, to collaborating with industry analysts to better protect the Defense Industrial Base, to issuing actionable cybersecurity guidance that helps network defenders protect our most sensitive systems from adversary threats," the NSA says.

"While many of our mission successes must remain classified, I'm proud that we can showcase how NSA Cybersecurity helps contribute to securing the nation in this report," said Rob Joyce, NSA Cybersecurity Director.

"The successes really show the value NSA Cybersecurity delivers through its foreign threat intelligence insights, partnerships and expertise."

Highlights include:

- Working with partners to respond to national-level threats, such as SolarWinds and multiple ransomware attacks on U.S. critical infrastructure
- Standing up the NSA Cybersecurity Collaboration Center, an unclassified space where NSA Cybersecurity experts collaborate with industry and interagency partners to reduce the attack surface to the Defense Industrial Base and ensure the nation's sensitive intellectual property, military research and innovative technical economy are protected at scale
- Discovering and disclosing vulnerabilities to industry, such as critical vulnerabilities to Microsoft Exchange
- Releasing 23 public cybersecurity reports that help net defenders secure systems from threats and vulnerabilities, including a dozen in partnership with U.S. and allied partners
- Working with the Department of Defense and U.S. military services to assess, prioritize and mitigate vulnerabilities in critical U.S. weapons and space systems
- Delivering updated cryptographic devices to protect National Security Systems from potential adversary quantum computing attacks
- Combining with the National Science Foundation to host 156 K-12 summer cybersecurity camps that educated more than 3,500 students and more than 800 educators



●▶ Click here to check out the full 2021 Year in Review, and visit the NSA's library for the cybersecurity information and technical guidance listed above.

Air Force asks industry to model and simulate electromagnetic warfare effects that destroy electronics

Source: https://www.militaryaerospace.com/power/article/14233438/electromagnetic-warfare-highpower-microwaves-destroy-electronics

Feb 09 – U.S. Air Force high-energy weapons experts are reaching out to industry to find companies able to model and simulate the effects of electromagnetic warfare weapons intended to destroy or disable enemy electronics, improvised explosive devices, unmanned aircraft, and similar systems.

Officials of the Air Force Research Laboratory Directed Energy Directorate at Kirtland Air Force Base, N.M., issued a broad agency announcement (FA9451-22-S-0001) on Monday for the High Power Electromagnetics (HPEM) Modeling and Effects project.

High-power microwaves offer technologies that enable low-collateral-damage military applications, counter electronic effects, counter improvised explosive devices, and counter weapons of mass destruction. Focused beams of microwave energy can protect aircraft and ships against incoming missiles, and to help attack electronic targets. Researchers are developing sophisticated compact devices that convert stored electrical energy into high-power bursts able to penetrate structures and destroy electronics.

This potential $80 million project seeks to characterize the effectiveness of potential HPEM weapons by developing tools and generating vulnerability data to feed those tools.

The HPEM Modeling and Effects project consists of several future calls on specific areas of interest, which will be issued over the next five years.
The vulnerability data consists of the likelihood of destruction or disruption of enemy electronics when subjected to high-power electromagnetic energy. The project also investigates how to predict and model the fundamental mechanisms that cause these disruptions or failures.
Companies interested should monitor SAM.gov online at https://www.sam.gov/content/homefor contracting opportunities under the HPEM Modeling and Effects program. The HPEM Modeling and Effects projects encompasses 14 technical in two broad areas: effects and numerical simulation.
Effects will involve empirical effects testing; HPEM weapons effectiveness modelling; fundamental HPEM effects research; battle damage assessment and recuperation time; emerging technologies like HPEM sources, diagnostics, and sensors; and evaluation tools for effects databases.
Numerical simulation involves vii. developing simulation codes for HPEM systems and components modeling; using codes in developing HPEM systems and components; developing simplified high-performance computing and analysis tools; digital engineering of HPEM systems and components; multi-scale materials modelling; developing HPEM engagement-level codes; engagement and mission level modeling of HPEM systems; and validating all software.
Air Force researchers say they expect to award one contract for each call.

Islamic State evolves 'emoji' tactics to peddle propaganda online

Source: https://www.politico.eu/article/islamic-state-disinformation-social-media/

Feb 10 – The Islamic State has a new weapon in spreading hate speech and violent content online: the emoji.
Over the past two months, Facebook pages in Arabic, Kurdish and English have used these digital images to sidestep Facebook's content rules. Emojis have been used instead of words like "weapon," "explosion" and "rocket" to champion the Islamic State's terrorist attacks across the Middle East and farther afield.
These pages, posing as mainstream media organizations with mundane names like World News and Media Point, have collectively racked up hundreds of thousands of likes, shares and comments, based on research shared with POLITICO.
The fake news outlets are part of a sophisticated digital disinformation campaign that includes deploying different tactics across Facebook pages, Twitter accounts and Telegram channels. Islamic State-affiliated channels, all told, have almost 80,000 followers.
Some of the social media content has been available since June 2020, primarily focusing on spreading hate speech in Iraq and Syria by sharing news about ISIS attacks from the group's official mouthpieces.
Much of the ISIS content reviewed by POLITICO is still online — and none of it should be available on social media, based on platforms' own rules against terrorist content.

"They are linked to a wider unofficial ISIS news ecosystem that has figured out specific evasion tactics, even despite [social media] takedowns, to thrive and to continue to do so," said Moustafa Ayad, executive director for Africa, the Middle East and Asia at the Institute for Strategic Dialogue, a think tank that tracks online extremism. Ayad discovered the terrorist groups across all three platforms and shared his findings with POLITICO.
"ISIS supporters have figured out a way to use multiple platforms in an increasingly sophisticated way," he added. "Why would they develop an emoji code to describe certain things on Facebook and not use that same emoji code on Telegram? It's about using different tactics."

Different tactics for different platforms
The groups are weaponizing blindspots within each social media platforms' content policies to promote a hateful and violent ideology, according to two national security officials and three researchers who track online jihadist material.
For Facebook, that includes replacing terrorist language with emojis. For Twitter, that involves toning down the content in English compared with what's posted in Arabic. For Telegram, it means copying directly from official ISIS material. It's an evolving cat-and-mouse battle with tech companies and national security agencies.
The combination of different platforms also allows jihadist groups to reach the widest possible audience while portraying themselves as part of a legitimate political organization. Alternative networks like Telegram provide a place to coordinate tactics, while a more mainstream platform like Facebook is used to disseminate often toned-down propaganda so that such messaging can circumvent the platform's content-moderation tools.
"They are very sophisticated. They are very aware of what they are doing," said Ayse Deniz Lokmanoglu, a postdoctoral fellow at Northwestern University's Center for Communication and Public Policy.
In response, Facebook declined to comment but said it was investigating the accounts. Representatives for Twitter and Telegram did not respond to requests for comment.
Tech companies, even when they've been slow to remove material from Western extremists, have aggressively removed tens of thousands of accounts with close ties to ISIS, the Taliban or other jihadist groups, often working closely with national security agencies to weed out such material.
It has not always been successful. Internal Facebook documents, made public by Frances Haugen, a company whistleblower, disclosed how the company repeatedly failed to protect its Arabic-language users from terrorist-related material. In response, Meta, Facebook's parent company, said it had invested heavily in content moderation based in the Middle East.
Still, extremists have quickly evolved to stay ahead of the game, taking advantage of little cooperation between the tech companies to clamp down on campaigns that rely on several social media networks.
Meili Criezis, a graduate fellow at American University's Polarization and Extremism Research and Innovation Lab who tracks ISIS online propaganda, said these groups often use backup social media accounts in case their main channels are removed.
"They always have a backup channel that you would be able to link from one to another," added Criezis, who was not associated with the work provided to POLITICO by the Institute for Strategic Dialogue, but who independently uncovered part of the same ISIS-linked digital disinformation campaign.
"For ISIS, it's important because they see themselves as a global caliphate. So that's why these media channels, such as Twitter, Facebook, and Telegram, are important to keep on," she said.

Syrian prison break
In late January, ISIS militants carried out a violent prison break in Hasakah, Syria — and showed their digital disinformation apparatus in action.
On Telegram, the fake media outlets began sharing a specific ISIS hashtag the terrorist group was using to coordinate its messaging around the attack, which led to 10 days of fighting within the Syrian city. They also repurposed photos and other social media content directly from the jihadists' official propaganda machine, often keeping the ISIS logo on the social media posts shared within Telegram.
On Twitter, the Arabic-language accounts were openly supportive of the prison break, both sharing the ISIS hashtag and praising the "Caliphate State." Yet in English, where the social media company's online content tools are more advanced, those accounts were more muted, merely referring to the militants as "Muslims coming together."
On Facebook, the pages relied on their emoji codebook to herald the attack, splicing in the digital images to describe terms associated with ISIS. They also posted a lengthy video of the prison break, which has garnered almost 90,000 views, taken from the viewpoint of the militants as they scattered into the Syrian city.
The accounts, channel and pages on all three social networks repeatedly shared each other's content, as well as that of affiliated social media users who spread the material to a wide online audience.

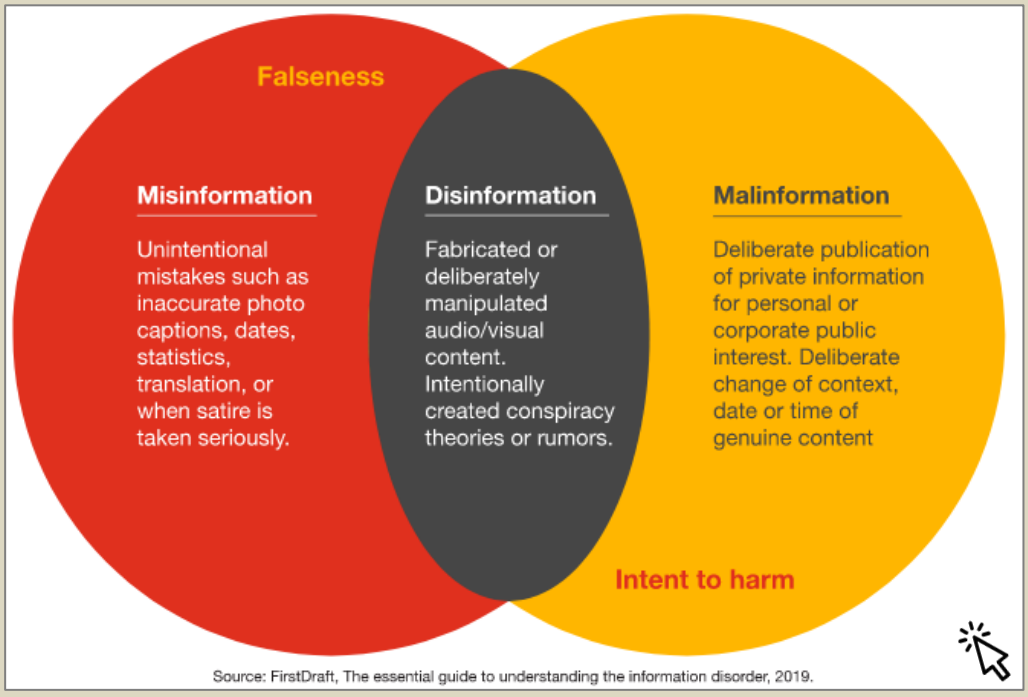
"What is going on here is something completely new," said Ayad, the Institute for Strategic Dialogue researcher who discovered the network. "It's a multiplatform, multilingual tactic that's using fake news organizations and different content strategies. The goal appears to be to sustain an online presence without being detected."

The Three Leading Cyber Risks: Misinformation, Disinformation, and Fake News

Source: https://www.homelandsecuritynewswire.com/dr20220216-the-three-leading-cyber-risks-misinformation-disinformation-and-fake-news

Feb 16 – Misleading information has emerged as one of the leading cyber risks in our society, affecting political leaders, nations, and people's lives, with the COVID-19 *pandemic having only made it worse*. However, it also affects something we rarely stop to consider: business. But how do organizations prepare against such threats? A new study, in *Business Horizons*, published by Elsevier, maps out the risk factors associated with misinformation, disinformation and fake news—proposing practical ways to manage risks in the parlance of business.

Industry 4.0 has brought about a metamorphosis in the world of business. The new revolution demands the integration of physical, biological and digital systems under one roof. Such a transformation, however, comes with its own set of risks. Misleading information, including misinformation, disinformation and fake news, often has damaging effects on the public image of political leaders and, as the COVID-19 crisis has clearly shown, on the general public and the economy. However, the consequences of misinformation on business organizations have been far less explored.



"Information has always played an irrefutable role in economics," said **Dr. Pythagoras N. Petratos** of Coventry University's Business School, whose research, examines the various forms of misleading information, identifying the cyber threats associated with them, and providing recommendations on tackling such risks. "We need to pay attention to the quality of information disseminated into the world, now more than ever, as spreading misinformation has become a lot easier with the advent of digital transformation.

"My research attempts to bridge the divide between academic research and real-world practice of cyber risk management."

The fake news "infodemic" that spread alongside the COVID-19 pandemic also affected the finance sector. For instance, during the lockdown period of 2020, there was a huge surge in fake news and illegal activity related to the financial and other markets. Financial firms had to train their staff to deal with fraudulent online schemes and reports.

Deliberate spreading of disinformation has also been responsible for swaying the outcome of elections. Cyber attackers have used misleading information on social media for procuring campaign finances as well as personal and financial information of people and corporations. These actions undermine a nation's security and make them vulnerable to geopolitical risks.

To deal with these cyber risks, businesses and authorities need to establish cybersecurity practices and policies that can evolve and adapt to the multifaceted cyberthreats. Executives and leaders should be trained to recognize cyber threats when they see one. To enable faster recognition, firms need to embrace modern computing software that fits their work criteria and can detect, report, and effectively manage cyber threats.

Anti-misinformation strategies such as having human fact-checkers for websites or artificial intelligence for bot detection on social media could be used to prevent the damage caused by propagation of misleading information. Partnerships between private and public sectors

can also mitigate cyber risks by forming a united front with better cyber defenses and funds to invest in cyber security technologies. All in all, the study provides a primer on the risks associated with misleading information in the sphere of business and the ways to avoid them, highlighting the fact that businesses are not immune to them either.
"Fake news is not a new phenomenon, but the COVID-19 pandemic, the ongoing digital transformations, and advances in big data have exacerbated it. Business executives and leaders across an array of industries, organizations, and nations, as well as the public, need to become aware of such risks and find innovative ways to manage them," concludes Dr. Petratos.

Constructing the Cyberterrorist – Critical Reflections on the UK Case

Author: Gareth Mott (2021; 152 papes)
Source: https://www.routledge.com/Constructing-the-Cyberterrorist-Critical-Reflections-on-the-UK-Case/Mott/p/book/9781032086286

This book maps and analyses the official British construction of the threat of cyberterrorism. By using interpretive discourse analysis, this book identifies 'strands' from a corpus of policy documents, statements, and speeches from UK Ministers, MPs, and Peers between 12 May 2010 and 24 June 2016. The book examines how the threat of cyberterrorism was constructed in the UK, and what this securitisation has made possible. The author makes novel contributions to the Copenhagen School's 'securitisation theory' framework by outlining a 'tiered' rather than monolithic audience system; refining the 'temporal' and 'spatial' conditioning of a securitisation with reference to the distinctive characteristics of cyberterrorism; and, lastly, by detailing the way in which popular fiction can be ascribed agency to 'fill in' an absence of 'cyberterrorism' case studies. He also argues that the UK government's classification of cyberterrorism as a 'Tier One' threat created a central strand upon which a discursive securitisation was established. This book will be of interest to students of Critical Security Studies, terrorism studies, UK politics, and international relations.

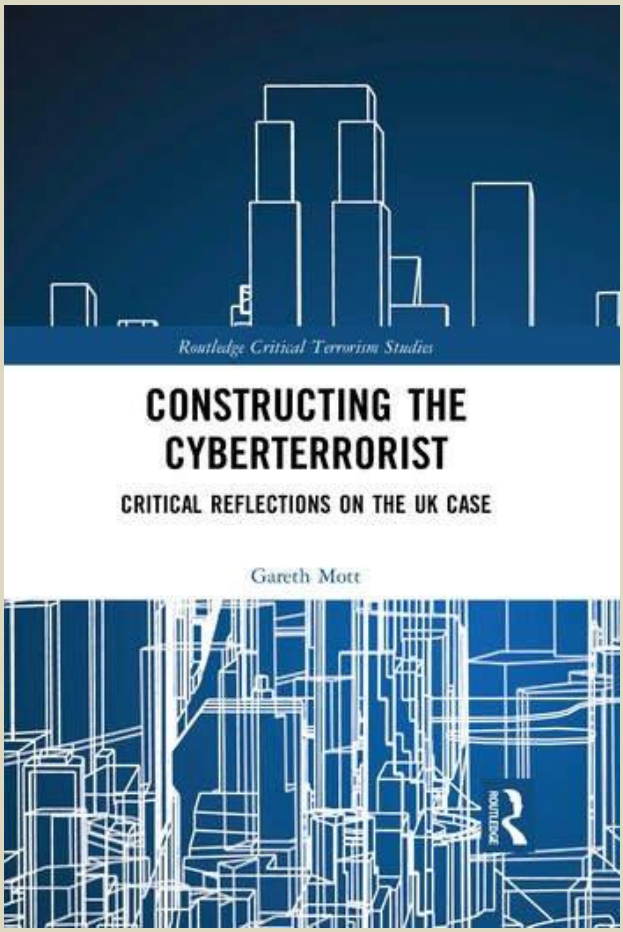


Table of Contents
Introduction: locating the 'cyberterrorist' within cyberspace and academia
1. Interpreting the construction of hypothetical threatening actors in cyberspace
2. The discursive construction of the threat of cyberterrorism to the UK
3. Running out of time: cyberterrorism as a temporally distinct threat
4. Locating the cyberterrorist: cyberterrorism as a spatially unique threat
5. Narrating the cyberterrorist: from fiction to reality
Conclusion

Gareth Mott is a lecturer in security and intelligence at the University of Kent, UK.

How a Saudi woman's iPhone revealed hacking around the world

By Joel Schectman and Christopher Bing
Source: https://www.reuters.com/technology/how-saudi-womans-iphone-revealed-hacking-around-world-2022-02-17/

Feb 17 – A single activist helped turn the tide against NSO Group, one of the world's most sophisticated spyware companies now facing a cascade of legal action and scrutiny in Washington over damaging new allegations that its software was used to hack government officials and dissidents around the world.
It all started with a software glitch on her iPhone.
An unusual error in NSO's spyware allowed Saudi women's rights activist Loujain al-Hathloul and privacy researchers to discover a trove of evidence suggesting the Israeli spyware

maker had helped hack her iPhone, according to six people involved in the incident. A mysterious fake image file within her phone, mistakenly left behind by the spyware, tipped off security researchers.

Saudi activist Loujain al-Hathloul makes her way to appear at a special criminal court for an appeals hearing, in Riyadh, Saudi Arabia March 10, 2021. REUTERS/Ahmed Yosri

Soon after her release from jail, the activist received an email from Google warning her that state-backed hackers had tried to penetrate her Gmail account. Fearful that her iPhone had been hacked as well, al-Hathloul contacted the Canadian privacy rights group Citizen Lab and asked them to probe her device for evidence, three people close to al-Hathloul told Reuters.

The discovery on al-Hathloul's phone last year ignited a storm of legal and government action that has put NSO on the defensive. How the hack was initially uncovered is reported here for the first time.

Al-Hathloul, one of Saudi Arabia's most prominent activists, is known for helping lead a campaign to end the ban on women drivers in Saudi Arabia. She was released from jail in February 2021 on charges of harming national security. read more

After six months of digging through her iPhone records, Citizen Lab researcher Bill Marczak made what he described as an unprecedented discovery: a malfunction in the surveillance software implanted on her phone had left a copy of the malicious image file, rather than deleting itself, after stealing the messages of its target.

He said the finding, computer code left by the attack, provided direct evidence NSO built the espionage tool.

"It was a game changer," said Marczak "We caught something that the company thought was uncatchable."

The discovery amounted to a hacking blueprint and led Apple Inc (AAPL.O) to notify thousands of other state-backed hacking victims around the world, according to four people with direct knowledge of the incident.

Citizen Lab and al-Hathloul's find provided the basis for Apple's November 2021 lawsuit against NSO and it also reverberated in Washington, where U.S. officials learned that NSO's cyberweapon was used to spy on American diplomats.

In recent years, the spyware industry has enjoyed explosive growth as governments around the world buy phone hacking software that allows the kind of digital surveillance once the purview of just a few elite intelligence agencies.

Over the past year, a series of revelations from journalists and activists, including the international journalism collaboration Pegasus Project, has tied the spyware industry to human rights violations, fueling greater scrutiny of NSO and its peers.

But security researchers say the al-Hathloul discovery was the first to provide a blueprint of a powerful new form of cyberespionage, a hacking tool that penetrates devices without any interaction from the user, providing the most concrete evidence to date of the scope of the weapon.

In a statement, an NSO spokesperson said the company does not operate the hacking tools it sells – "government, law enforcement and intelligence agencies do." The spokesperson did not answer questions on whether its software was used to target al-Hathloul or other activists.

But the spokesperson said the organizations making those claims were "political opponents of cyber intelligence," and suggested some of the allegations were "contractually and technologically impossible." The spokesperson declined to provide specifics, citing client confidentiality agreements.

Without elaborating on specifics, the company said it had an established procedure to investigate alleged misuse of its products and had cut off clients over human rights issues.

Discovering the blueprint

Al-Hathloul had good reason to be suspicious - it was not the first time she was being watched.

A 2019 Reuters investigation revealed that she was targeted in 2017 by a team of U.S. mercenaries who surveilled dissidents on behalf of the United Arab Emirates under a secret

program called Project Raven, which categorized her as a "national security threat" and hacked into her iPhone.
She was arrested and jailed in Saudi Arabia for almost three years, where her family says she was tortured and interrogated utilizing information stolen from her device. Al-Hathloul was released in February 2021 and is currently banned from leaving the country. Reuters has no evidence NSO was involved in that earlier hack.
Al-Hathloul's experience of surveillance and imprisonment made her determined to gather evidence that could be used against those who wield these tools, said her sister Lina al-Hathloul. "She feels she has a responsibility to continue this fight because she knows she can change things."
The type of spyware Citizen Lab discovered on al-Hathloul's iPhone is known as a "zero click," meaning the user can be infected without ever clicking on a malicious link. Zero-click malware usually deletes itself upon infecting a user, leaving researchers and tech companies without a sample of the weapon to study. That can make gathering hard evidence of iPhone hacks almost impossible, security researchers say. But this time was different.
The software glitch left a copy of the spyware hidden on al-Hathloul's iPhone, allowing Marczak and his team to obtain a virtual blueprint of the attack and evidence of who had built it. "Here we had the shell casing from the crime scene," he said.
Marczak and his team found that the spyware worked in part by sending picture files to al-Hathloul through an invisible text message. The image files tricked the iPhone into giving access to its entire memory, bypassing security and allowing the installation of spyware that would steal a user's messages.
The Citizen Lab discovery provided solid evidence the cyberweapon was built by NSO, said Marczak, whose analysis was confirmed by researchers from Amnesty International and Apple, according to three people with direct knowledge of the situation.
The spyware found on al-Hathloul's device contained code that showed it was communicating with servers Citizen Lab previously identified as controlled by NSO, Marczak said. Citizen Lab named this new iPhone hacking method "ForcedEntry." The researchers then provided the sample to Apple last September. Having a blueprint of the attack in hand allowed Apple to fix the critical vulnerability and led them to notify thousands of other iPhone users who were targeted by NSO software, warning them they had been targeted by "state-sponsored attackers." It was the first time Apple had taken this step.
While Apple determined the vast majority were targeted through NSO's tool, security researchers also discovered spy software from a second Israeli vendor QuaDream leveraged the same iPhone vulnerability, Reuters reported earlier this month. QuaDream has not responded to repeated requests for comment. read more
The victims ranged from dissidents critical of Thailand's government to human rights activists in El Salvador.
Citing the findings obtained from al-Hathloul's phone, Apple sued NSO in November in federal court alleging the spyware maker had violated U.S. laws by building products designed "to target, attack, and harm Apple users, Apple products, and Apple." Apple credited Citizen Lab with providing "technical information" used as evidence for the lawsuit, but did not reveal that it was originally obtained from al-Hathloul's iPhone. NSO said its tools have assisted law enforcement and have saved "thousands of lives." The company said some of the allegations attributed to NSO software were not credible, but declined to elaborate on specific claims citing confidentiality agreements with its clients.
Among those Apple warned were at least nine U.S. State Department employees in Uganda who were targeted with NSO software, according to people familiar with the matter, igniting a fresh wave of criticism against the company in Washington.
In November, the U.S. Commerce Department placed NSO on a trade blacklist, restricting American companies from selling the Israeli firm software products, threatening its supply chain. read more
The Commerce Department said the action was based on evidence that NSO's spyware was used to target "journalists, businesspeople, activists, academics, and embassy workers."
In December, Democratic Senator Ron Wyden and 17 other lawmakers called for the Treasury Department to sanction NSO Group and three other foreign surveillance companies they say helped authoritarian governments commit human rights abuses.
"When the public saw you had U.S. government figures getting hacked, that quite clearly moved the needle," Wyden told Reuters in an interview, referring to the targeting of U.S. officials in Uganda. Lina al-Hathloul, Loujain's sister, said the financial blows to NSO might be the only thing that can deter the spyware industry. "It hit them where it hurts," she said.

What to Expect with Cyber Surprise

Source: https://www.homelandsecuritynewswire.com/dr20220222-what-to-expect-with-cyber-surprise

Feb 22 – The cyber domain has three critical characteristics which differentiate it from the kinetic domain: it is connected across the globe; it is pervasive in the economic life-blood of the world; and it is asymmetric in its ability to enable power projection.
Paul Rosenzweig writes in *Lawfare* that "Never before has the world faced a kinetic war with that background of baseline vulnerability."

What, then, can we expect from a strategic surprise which we expect Russia to launch as part of its campaign in Ukraine? Rosenzweig notes that the degree of surprise often varies. Some surprises, like the attack on Pearl Harbor, are deep strategic surprises. The 9/11 attacks were similarly disorienting. But other surprises, like the Bengals victory over the Chiefs in the Super Bowl, or (for those who follow soccer), Leicester winning the English Premier League in 2016, were surprising, but not so completely unanticipated that they are deeply disruptive.

He writes

> Governments and the private sector will, of course, expect the normal level of surprise. There will be denial of service attacks and the surprise will only be where and when. Likewise, we can expect disinformation campaigns, false flag operations, and even disruptions to Ukrainian critical infrastructure.
>
> As Jason Healy has put it, the possibilities of surprise in cyberspace are almost limitless. But if the defenders have done their jobs well, their responses will be as good as they can, in practice, be. That may or may not be sufficient to the task—but the surprise factor will be only a small component of the overall success or failure.

What then, of the bigger strategic surprise? Here of some of them:

> *What if Ukraine's weapons don't work?* It's possible that many of the more sophisticated weapons rely on computer systems that can be disabled.
>
> *Will deep fakes play a role in the upcoming conflict?* What, for example, might happen if a video of Ukrainian President Zelenskyy surfaced in which he abdicated his office?
>
> *What if Russia decides to expand the cyber battlefield?* What is the Western response if, say, Putin decides to punish Lithuania for providing support to Ukraine?
>
> *What if Russia decides to hold at risk critical international initiatives?* In this time of pandemic response, for example, the supply chain for vaccine production and distribution is both extremely important and extremely fragile.

But the unique characteristics of the cyber domain make it impossible to predict, with any degree of certainty, what a digital surprise will look like. "We are about to see what war in the cyber era really looks like and, truthfully, nobody can tell you what will happen next," Rosenzweig concludes.

There Is No Cyber "Shock and Awe": Plausible Threats in the Ukraine Conflict

Source: https://www.homelandsecuritynewswire.com/dr20220222-there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukraine-conflict

Feb 22 – People are talking about cyberwar again. Russia's massive military buildup along Ukraine's borders holds the potential of triggering the largest-scale military clash since World War II – and many analysts say that there is a potential for destabilizing and devastating cyberattacks preceding, accompanying, and following Russia's military actions.

Lennart Maschmeyer and Nadita Kostyuk, writing in *War on the Rocks*, note that Jason Healey predicts that if Russia invades, "the opening salvo is likely to be with offensive cyber capabilities." William Courtney and Peter A. Wilson from RAND warn of the "massive employment" of cyber warfare tools to create "shock and awe causing Ukraine's defenses or will to fight to collapse."

They note further that, accordingly, the United States and the United Kingdom have deployed cyber warfare teams to help Ukraine defend against an impending strategic cyber strike against critical infrastructure. Some go further, suggesting that Russia may not need to use military force at all, because cyberstrikes can "achieve much the same effect from across the border." This assessment is apparently shared by policymakers working on countering the Russian threat to Ukraine, with an (anonymous) senior Biden administration official recently stating as much.

The add:

> These predictions suggest that cyber operations will provide significant strategic advantages to Russia either as complements to military force, or as standalone instruments — or at least that policymakers and commentators think that they will. Current warnings of escalating cyber warfare conjure deep-seated fears of cyber doom and the recurring specter of a "cyber Pearl Harbor" strategic surprise attack. In practice, however, cyber warfare has been a failure. Our research shows that cyber operations have remained irrelevant on the battlefield, while standalone operations to weaken Ukraine through election interference, critical infrastructure sabotage, and economic disruption largely failed to contribute to Russia's strategic goals of making Ukraine abandon its pro-European Union and pro-NATO foreign policy. Consequently, current fears of cyber warfare defy not only Russia's track record in Ukraine, but also strategic logic. Given that Russia's cyber operations have failed to produce significant strategic value to date, why would we expect this to suddenly change now? Or, to put it more pointedly: If cyber operations offer such effective and potent instruments, why did Russia go through the trouble (and costs) to mobilize its troops? Current predictions of cyber onslaught do not offer a persuasive answer.

> Giving in to these fears risks fighting phantom threats, playing into Russia's hands by distracting from the need to counter its military threat and sowing fear and confusion — at least among Western audiences. A level-headed analysis of the threat that distinguishes what is theoretically possible from what is practically feasible is urgently needed. Our research suggests that, contrary to hysteria, cyber operations will remain of secondary importance and at best provide marginal gains to Russia.

They conclude:

> Cyber operations are not strategically irrelevant, nor are surprise cyber strikes of strategic relevance impossible. Rather, in assessing their threat we should distinguish what is possible in theory from what is feasible, and thus probable, in practice.
> ….
> Exaggerated fears of hypothetical cyber strikes — either used as substitutes or complements to military operations — distract from the clear and observable threat of invasion and, in doing so, may trigger misallocation of valuable resources needed to respond to it. Perpetuating such fears also risks playing into Russia's hands by exaggerating its cyber capabilities and distracting from the need to prioritize efforts to counter its military threat.

The four biggest cyber threats hanging over our future

Source: https://www.israel21c.org/the-four-biggest-cyber-threats-hanging-over-our-future/

"It's not a question of whether the hackers are going to get through. They will. It's just a matter of how."

Feb 23 – There are those who say a "cyber pandemic" is inevitable. And there are those who say we're in it right now.
Gil Schwed, founder and director of Israel's cybersecurity pioneer, Check Point Software Technologies, belongs to the latter camp.
Cybercriminals already have the sophisticated tools to infect the websites of government organizations and major companies, Schwed argues. And we can't rely on offense. Rather, he says, "We have to defend against [attacks] from day zero," like a vaccination against illness.
A recent Allianz Risk Barometer survey revealed that companies in 89 countries are more concerned about ransomware attacks, data breaches or major IT outages than they are about supply chain disruption, natural disasters or the Covid-19 pandemic.
And no wonder: In the fast-changing online landscape, tantalizing opportunities for bad actors pop up like mushrooms overnight.
"It's not a question of whether the hackers are going to get through. They will. It's just a matter of how," says Edo Yahav, VP R&D and general manager of SafeBreach Israel in Tel Aviv.
Israel's approximately 450 cybersecurity companies play a significant role in predicting and protecting against cybercrime, in large part because the Israel military serves as a unique incubator for talent and innovation in this sector.
"I don't think anyone else in the world has this type of advantage," says Liel Strauch, director of cybersecurity research at PerimeterX of Tel Aviv and Silicon Valley.
Within the emerging metaverse, what are the biggest cyber risks experts expect to be battling in the coming years?

Beware of bots

PerimeterX secures ecommerce, media and travel websites against automated fraud and client-side attacks, detecting and proactively managing risks to web applications, says Strauch.
For example, the company's Bot Defender deflects attacks by bots — bits of software programmed to do anything from taking over an account to snatching up and scalping limited-edition items like sneakers. (Read more about sneaker bots here.)
The increasing popularity and value of limited-edition items and unique NFTs (non-fungible tokens) is attractive to attackers, says Strauch.
"We can assume we'll see bots attacking NFT sales and the metaverse in general in order to gain profit in cryptocurrency or converted to actual money," she tells ISRAEL21c.
"Another thing we have seen gaining traction with attackers … is supply chain attacks," she adds.
A supply chain attack is when a hacker infiltrates a website through the "blind spot" of software vulnerabilities in third-party vendors running on that site with access to its data. Google Analytics is an example of a third-party vendor.
"This will be one of the main ways for attackers to gain access to data of different enterprises," says Strauch.
Through the third party, attackers inject a piece of code to different JavaScripts that run on a website, collecting users' personal information such as credit card numbers.
"Since this creates a lot of profit for cybercriminals, we can assume supply chain attacks will increase in coming years," she says.

The unfolding metaverse will drive a lot more traffic to the digital world, providing more opportunities for bad actors to profit – and therefore more opportunities for cybersecurity companies to profit, Strauch predicts.
What is the metaverse? Also called "Web 3.0," it's a collection of technologies that adds an immersive 3D dimension to our digital interactions.
On the bright side, the shift to the metaverse means that "everything happens in the same world, similar to how it was easier to deal with physical 'skimming' when it happened on ATMs and you knew exactly where it was going to happen and what to do," says Strauch.
"Now that everything will be transferred to digital assets it will help companies invest more in technologies to protect those digital assets."

Avoiding account takeovers

"One of the main trends we see is account takeovers," says Elad Cohen, VP Data Science for Riskified, one of four cybersecurity firms we featured in our recent report on anti-fraud technologies.
"We ran a survey showing that at least 17 percent of consumers had one of their accounts taken over. We believe there's been a five-fold increase in attempts over the last three years. In 2021, one in 140 logins was an account takeover attempt. We anticipate this will continue increasing."
Ecommerce companies face a dilemma: Customers prefer a purchasing process that's as easy ("frictionless") as possible, for example when their password and credit card number are saved on the website. Using password-free authentication (such as SMS messages with a temporary code to type in) adds friction and leads to lost sales.
However, the more frictionless the process the easier it is for hackers to take over the account.
"There is always a balance between ease of use and difficulty for hackers to crack," Cohen says.
Plus, loyalty points or discounts that lure return customers to use their stored account add value and vulnerability that further entice hackers.
"It makes the potential for account takeover much more lucrative. And once the fraudster has credentials for an account, it's easier to monetize it," says Cohen.
Ephraim Rinsky, who handles product marketing for account security at Riskified, adds that stealing credentials is only getting easier.
"Two years ago, to break into an account I'd have to go on the dark web and shop around for credentials. Today, you can buy credentials on Telegram groups or even on the normal web. A teenager sitting at home can get credentials to log into an ecommerce site within a minute."
Merchants will need ever more sophisticated fraud-prevention technologies to block fraudsters, especially if the password-stealer uses bots that, as Riskified often sees, make up to 40,000 attempts per hour to break into accounts across many ecommerce sites.
"If you close one door in authentication fraud, fraudsters will open the next one," says Rinsky. "It's a cat-and-mouse game."
While Riskified and others work behind the scenes to solve vulnerability problems across authentication methods, everyone can help protect their own accounts simply by never reusing a password, say Cohen and Rinsky.

Watch your digital wallet

Smart password management may also be the best protection against cybercrimes targeting digital assets, says Shy Datika, founder and president of INX, which offers regulated trading platforms for digital securities and cryptocurrencies.
The CB Insights report "12 Tech Trends to Watch Closely in 2022" reveals that although illicit activity affects less than 1% of crypto transactions, crypto crime reports are rising.

"These include hackers stealing coins from investors, individuals falling for crypto investing-related scams, and more. … in December 2021, cybercriminals stole $150M in cryptocurrency from exchange BitMart as a result of a security breach involving stolen private keys," the report states.
Read that closely and you will understand why Datika says cybercrimes involving cryptocurrency are "just stupid, regular hacking."
"If someone is hacking your phone or computer and stealing your password and using it to enter your hot wallet, that is not a cybercrime relating to crypto. It's simply done by stealing passwords," he says.
While a small percentage of crypto-related crimes (Datika estimates 10-20%) occur during the transfer of cryptocurrency between a "cold" (physical) wallet and a "hot" (Internet-connected) wallet, Datika points out it's impossible to hack the blockchain directly.

As for scammers who fool people into sending cryptocurrency to the scammer's digital wallet, it's another old trick applied to a new form of money. And it's likely to increase as cryptocurrency becomes more popular.

Ransomware, quantum computing

"In the upcoming years, large enterprises like financial and healthcare companies will see more of the same types of attacks but much more complex — for example, a lot more ransomware," predicts Edo Yahav of SafeBreach, the most widely used continuous security validation platform.

"Why? Because it works and it's lucrative. Companies usually pay the ransom because they don't want to lose their data. As long as it pays off, it will continue and it will get more complex to stop it," says Yahav.

"Due to the ability to work from home or from anywhere, the need to support a very dynamic workplace means more tools must be introduced into the mix. Additional tools and complexity lead to human errors and hackers can take advantage of that," he adds. "This is why companies need to keep assessing and evaluating their arsenal."

The rise of quantum computing in the next decade poses another big threat, Yahav says. Quantum computers can break the encryption algorithms that secure online commerce, communications and financial services.

"It will change the security industry by keeping large enterprises on their toes. They will need to identify and secure their most valuable assets with the right software instead of trying to secure everything," says Yahav.

Israel will continue being a significant source of cybersecurity solutions for new and upcoming threats, he predicts.

"The security mindset is embedded within Israel," he says. "Unless something dramatic changes in the Middle East, we'll see more and more security mindset in Israeli youngsters and thought leaders."

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

& Robotic

DRONE NEWS

Pakistan, Turkey, China working on a joint drone program?

Source: https://www.globalvillagespace.com/pakistan-turkey-china-working-on-a-joint-drone-program/?amp

Jan 24 – Reports claim that Pakistan is coordinating on a joint drone program with Turkey and China. The countries are working on a joint unmanned drone program, which includes loyal wingman unmanned combat aerial vehicles (UCAVs).
One of Pakistan's leading defence experts Aerosint Division PSF revealed the news in a series of tweets.

"We have confirmed from official sources that Pakistan, China, and Turkey are currently working on a joint unmanned drone program that features 'Loyal Wingman' UCAVs," the tweet read.
According to details, the drones have the ability to conduct ISTAR (intelligence, surveillance, target acquisition, and reconnaissance) and neutralize aerial threats while keeping fighters at standoff distances.
The defence expert also said that the three countries are developing components of the MUM-T (Manned-Unmanned Teaming) system together. The drones would be able to fly independently and in support of manned aircraft, as well as in swarms.
Important to note, while this may be an important development, it is being believed that the joint UCAV will not materialize before 2025.

Pakistan's strong military relations with Turkey & China

Lately, Turkey's combat drone technology is making waves in the international community, especially after Azerbaijan's victory in the Nagorno-Karabakh conflict. During the six-week conflict, Azerbaijan deployed Turkish Bayraktar TB2 drones which gave it an edge over Armenia. As a result, many countries began eyeing Turkish drones owing to their successful military capabilities.
Pertinent to mention, Pakistan and Turkey enjoy friendly ties with strong bilateral cooperation in trade and military.
In August 2021, Pakistan's National Engineering and Science Commission (NESCOM) signed a contract with the Turkish Aerospace Industries for the joint production of "ANKA Unmanned Aerial Vehicles."
Meanwhile, Pakistan and China are "iron brothers." Pakistan often turns to China to boost its military arsenal. Earlier this month, reports emerged of Pakistan approaching China to acquire helicopter gunships. Pakistan also approached China for the procurement of the J-10C to counter the Indian Air Force's purchase of the Dassault Rafale.

Autonomous drones may be the ultimate scarecrows ... for pigeons

Source: https://newatlas.com/drones/autonomous-drones-pigeons/

Jan 25 – Much as we may like pigeons, they can make quite a mess of buildings and other structures, potentially posing a health hazard. According to new research, autonomous drones may be ideal for harmlessly chasing the birds away.
In the recent study, a team at Switzerland's EPFL research institute started by installing a weatherproof pan-tilt-zoom video camera on the roof of the EPFL SwissTech Convention Center. The building was already known for attracting large numbers of pigeons, which cover the roof with droppings that frequently have to be washed off.
Over a period of 21 days, the camera was used to observe the amount of time that pigeons typically stayed on the roof. Utilizing a neural network that was running on a linked ground station computer, the camera was also able to detect where and how many pigeons were present – it could even estimate their GPS coordinates.
After the three-week period, **a Parrot Anafi quadcopter** was added to the mix. Over the course of five days, whenever the camera spotted pigeons on the roof, it relayed their location to the drone. The aircraft then took off,

autonomously flying to the area and then hovering in place, chasing the birds away. Due to safety regulations, a human operator had to authorize each takeoff, although this hopefully won't be necessary once the system is developed further.
Over the five-day period, the drone was automatically deployed a total of 55 times. Doing so was found to significantly reduce the amount of time that pigeons stayed on the roof, and to reduce the number that landed there in the first place.
The system is described in a paper that was recently published in the journal *IEEE Explore*, and can be seen in use in the video below.

Myanmar's Rebels Get Resourceful With Improvised Drones

By Nick Waters
Source: https://www.bellingcat.com/news/2022/01/20/myanmars-rebels-get-resourceful-with-improvised-drones/

Jan 20 – Over the Christmas and New Year period, two videos were posted by two separate groups, each showing makeshift explosive munitions being carried and dropped by small drones. In the first video, posted in late December by the Karenni Generation Z Army (KGZ), a small team is shown launching a DJI Phantom drone modified with a release mechanism and armed with a small munition. The second video, posted by the Aung San Force-MPDF on 2nd January, shows six strikes, as well as footage from drones observing what seem to be indirect fire attacks.
According to the news website Myanmar Now, the KGZ is a rebel group active in the Kayah State in the country's east. The Aung San Force, meanwhile, is reported by Myanmar Now to be a self-organising resistance group. Both were reportedly formed in the aftermath of the February 2021 coup, which resulted in protests and a brutal military crackdown.
It is unclear if any other anti-coup groups in Myanmar have employed similar tactics. A number of militias of varying size and capability have formed in the year since the Myanmar military took control of the country despite Aung San Suu Kyi's National League for Democracy winning a landslide in elections.
These militias pale in scale, experience and capability when compared to more organised ethnic rebel groups, some of whom have been operating in Myanmar for decades. And while some of these more established groups are reported to have assisted anti-coup outfits, the dynamics that underpin these relationships remain complex, ever evolving and are not uniformly replicated across the country.
That being said, analysing the deployment of such weapons remains a useful exercise, allowing us to observe the innovations, influences and tactics employed by some sub-state armed groups in Myanmar.

"Aung San Force" Video
This video shows six strikes carried out by drone; the accompanying post suggests it was taken during operations in the Sagaing Region in the country's northwest and then posted to social media on January 2. While we don't see the drone itself, we do get a decent look at the munitions, as well as the effect they have on the ground.

A screengrab of footage from a drone video posted to the Facebook page of the Aung San Force-MPDF.

Although the quality of the video limits analysis, it's possible to draw some firm conclusions about their nature. The munitions themselves appear to be either the same or of very similar design to each other. The Aung San Force does not appear to have modified a conventional munition, as the Islamic State did with 40mm grenades and the PKK have done with 30mm grenades. The fins at the back and a plunger at the front of the munitions strongly indicates they have a simple point-detonating fuze. Some of these examples appear to be covered in a wrap of some kind.

Munitions filmed dropping from a drone and posted to the Facebook page of the Aung San Force-MPDF.

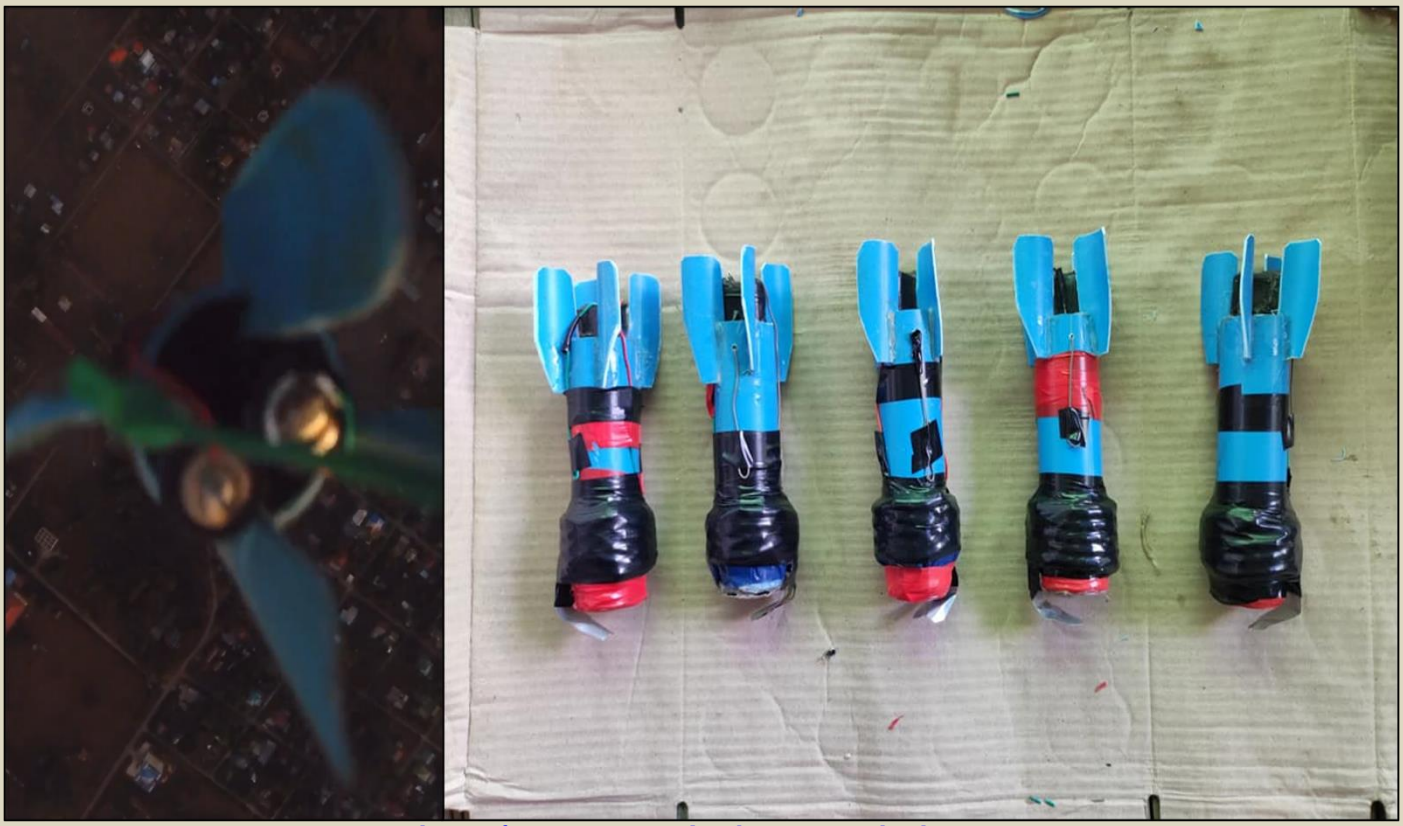
While these are relatively small, simple munitions, they clearly do the job they were designed for, producing a small blast on the ground. Their similarity to one another also indicates a relatively consistent manufacturing process. It is clear that thought has been put into the design and production of these munitions, rather than simply being an ad hoc attempt at weaponisation.
This is in contrast to other attempts at weaponisation of drones elsewhere in the world that have varied from well planned and effective to ineffective and suspiciously slapdash.

KGZ Video

The KGZ video is less obviously instructive. Although we see the drone and the munition, the quality of the video is such that it's difficult to make many useful observations about either from this clip by itself. Indeed we don't even see the moment of impact of the bomb, making any assessment of effectiveness (or if they even detonated) impossible.
A panning aerial view of buildings, presumably filmed by the drone itself could be geolocated to the area around a police station in Demoso, a town in Kayah State.
The drone is a DJI Phantom, versions of which were used widely by the Islamic State, and has been modified with a release mechanism to drop the bomb.

Footage posted by KGZ fighters shows a weapon being attached to a small drone.

Although we don't see too much of the munition used by the KGZ in the video, a post on their Facebook page displays clear images of devices that appear to match those on the drone.
As with the Aung San Force bombs, they do not appear to be modified conventional munitions, but rather improvised from scratch. A strip of metal foil is visible at the tip with wires leading to the base where what appear to be batteries are embedded. This indicates a crude electric contact fuse. When the munition makes impact with the ground, the foil will crush onto the front of the munition, completing the circuit and detonating the bomb.



Photos of munitions posted at the KGZ Facebook page.

While electric initiation mechanisms, such as electric contacts attached to opposing arms of a clothes peg, have been used by other armed groups to initiate IEDs, this seems a poor choice for a drone bomb. The passing wind could either detonate this kind of munition in flight, or bend it out of alignment so it does not detonate at all. This may be why the KGZ video does not show any explosion.
Despite appearing to be more of a novelty rather than a fearsome weapon, bombs, even small ones, dropped by recreational drones can be very effective despite being unguided. This was most aptly demonstrated by the Islamic State which carried out hundreds of such drone attacks in 2017. Notably, these attacks disrupted Iraqi troops during the Mosul offensive, with Islamic State utilising their makeshift air force to drop custom-made drone bomblets onto a multitude of targets, including vehicles and infantry, to deadly effect. Although vastly different organisations to the Islamic State, it appears some anti-coup groups have been experimenting with similar tactics.
Yet the use of these weapons, and the means by which their deployment has been communicated, also speaks to another purpose. According to Richard Horsey, an advisor on Myanmar to the International Crisis Group (ICG), footage of this kind can be a powerful tool in the information battle too. He noted that these videos have gone viral on Facebook in Myanmar, allowing anti-coup groups to demonstrate their capabilities and provide hope to their followers.
While such devices can have an impact on the battlefield, as already demonstrated in other conflicts, they are not going to win the war, Horsey said. But they can boost morale and encourage viewers sympathetic with the aims of these groups to provide money that may let them purchase more drones or weapons.

Nick Waters is an ex-British Army officer and open source analyst. He has a special interest in the conflicts in Syria, as well as social media, civil society, intelligence, and security.

Cybersecurity and Drones: How to Address the Security Threats

By Anastasios Arampatzis

Source: https://www.tripwire.com/state-of-security/contributors/aarampatzis/

Jan 30 – The Unmanned Aerial Systems (UAS) industry has become a massive technological playground worldwide. Their extensive applications make UAS very popular for the public and the private sector. Armed forces, agricultural industry, law enforcement, meteorological agencies, medical services, environmental companies, and oil refineries are but a few out of the excessive list of UAS users. UAS manufacturers spend a significant amount of money to research and develop high-tech and smart systems from aircraft-size military UAS to hand-size mini drones. The use in almost every aspect of human activity adds value to the need of UAS evolution, but it also increases security risks. Imagine what can happen when smart and cheap drones that anyone can easily purchase from a local hobby store become weapons at the hands of adversaries and cyber criminals. From that perspective, are drones a major threat when it comes to cybersecurity? And if so, what measures should be taken to counter them?

Drones Evolve

If I discussed drones with my friends a few decades ago, they would probably say that I was watching too many sci-fi movies. Today, drones are part of our lives. U.S. Federal Aviation Association (FAA) based on survey trends, overall market growth, and operational information forecasts an outbreak of drone registrations in the forthcoming years.

When we talk about drones, we need to consider two factors:

- Not only do they consist of the airborne platform, but they also include the control station that's necessary for safe and efficient operation communication links.
- They have become numerous, cheaper, and more complex.

Taking the above into consideration, it is obvious that drones are a serious risk for flight safety and security. We have discussed in a previous blog the threat that drones pose to flight safety. To minimize the risk, software applications have been developed to manage and organize drone flight traffic. Besides a major flight safety concern, drones can become a serious cybersecurity threat.

The Cybersecurity Threat of Drones

Apart from airworthiness and flight safety issues, drones affect the cyber domain and the security of data. Forbes points out that the malicious use of these platforms in the cyber domain is an inevitable fact, and it can no longer be pushed aside. Last Christmas, we

witnessed U.S. government posing export restrictions to one of the largest drone manufacturers in order to protect national security and foreign policy interests.
Since drones are remotely controlled, they can be hijacked by bad actors. The Department of Homeland Security (DHS) stated, "Given their rapid technology advancement and proliferation, the public safety and homeland security communities must address the fact that drones can be used nefariously or maliciously to hurt people, disrupt activities, and damage infrastructure." Major cyber domain threats caused by drone activity are:

- **GPS spoofing.** A way to take control of a drone. Attackers feed drones with false GPS coordinates and take full control of the platform. Security researchers have demonstrated how a hijacked drone can be used to hijack other drones, ending in a drone swarm under the control of cyber criminals. It is easy to realize that in such a case, the threat potential increases drastically and can be compared to the way botnets perform DDoS attacks, taking over a significant amount of systems and Internet of Things (IoT) devices.
- **Downlink intercept.** Allows a criminal accessing all transmitted data between the drone and the controller. Since the majority of commercial drones systems interact with their base using unencrypted communication channels, they can become vulnerable to exploitation by a cyber criminal who can intercept and have access to sensitive data drone exchanges with the base such as pictures, videos, and flight paths.
- **Data exploitation**. Critical infrastructure is protected in the terms of digital and physical security. The use of drones can overcome physical security limitations and cybersecurity protections, for a mini computer mounted on a small drone can approach undetected sensitive areas and carry out nefarious operations, mimic a Wi-Fi network to steal data, hijack Bluetooth peripherals, perform keylogging operations to steal sensitive passwords, as well as compromise access points, unsecured networks, and devices,

How to Mitigate the Threat
To mitigate the cybersecurity risks posed by the drones, we need to consider the following:

- How to secure the platform and the data exchanged
- How to counter drone platforms

Securing Drones

When it comes to drone cybersecurity, it is wise to be proactive. That's why you have to consider securing your platform as you would do with any network device. Kaspersky proposes some useful tips:

- Update the drone's firmware and apply a manufacturer's patches.
- Use strong passwords for the base station application.
- Use updated anti-virus software for your drone controller device.
- Subscribe to a VPN service to encrypt your connection.
- Limit the number of devices that can connect to the base station.
- Use the "Return to Home" (RTH) mode to ensure drone recovery from a hijack situation.

Counter Drones

Drones fall under the remit of the Federal Aviation Administration (FAA) as UAS. That means that you cannot take them down or jam their communication. This kind of countermeasures apply only to the military sector where different operational procedures are enforced when an unknown drone enters the perimeter of a military base.
Countermeasures should focus primarily on space protection. It is vital to be able to efficiently detect drones. High frequency radars, thermal cameras, RF scanners, acoustic sensors, and sophisticated machine learning and AI algorithms are used for this purpose. However, drones' small size and low speed makes their detection difficult within a highly cluttered environment.
Other techniques involve geofencing software, which creates a virtual border around an area, prohibiting unauthorized drone flight. Finally, the military sector makes use of counter drone systems called "effectors."

The Future

Drones will continue to evolve; in the near future, they will dominate various commercial and public sector areas such as deliveries, crops and livestock monitoring, border control, defense, surveillance, mapping, and security services. As so, it's vital to secure them properly to reap the benefits of their use and to prevent becoming adversarial weapons in the hands of opportunistic state cyber threat actors.

Anastasios Arampatzis is a retired Hellenic Air Force officer with over 20 years' worth of experience in managing IT projects and evaluating cybersecurity. During his service in the

Armed Forces, he was assigned to various key positions in national, NATO and EU headquarters and has been honoured by numerous high-ranking officers for his expertise and professionalism. He was nominated as a certified NATO evaluator for information security. Anastasios' interests include among others cybersecurity policy and governance, ICS and IoT security, encryption, and certificates management. He is also exploring the human side of cybersecurity - the psychology of security, public education, organizational training programs, and the effect of biases (cultural, heuristic and cognitive) in applying cybersecurity policies and integrating technology into learning. He is intrigued by new challenges, open-minded and flexible. Currently, he works as a cybersecurity content writer for Bora - IT Security Marketing. Tassos is a member of the non-profit organization Homo Digitalis.

Sensors – the More the Better

Source: https://i-hls.com/archives/112926

Feb 02 – A secure platform for managing visual asset inspection data from drones will provide enterprises with an improved, integrated analysis capability. A recent collaboration will provide visual data management and analytics platform to securely deliver data and actionable insights.

SkyCam Aviation provides visual data collection services using fixed-wing aircraft and employs multi-sensor technology to provide robust imagery to support a wide range of applications. The Optelos cloud-based visual data management and AI analytics platform that transforms geo-visual data into actionable insights.

Using the Optelos platform will enable to easily view data from SkyCam's 6-sensor platform which includes 4k (50mm-1200mm lenses), FLIR, SWIR, and hyperspectral sensors, as well as spectral detection of both methane and diesel.

For infrastructure inspection, SkyCam's data gathering provides00 extreme detail, allowing AI analysis down to 1/4". The platform allows capturing vast amounts of data, which can then be streamed onto the Optelos platform for management and analysis, or combined with any AI engine.

In addition to managing all collected inspection data, the platform also provides robust visualization of all data sources, high-resolution images and videos, detailed Orthomosaic 2D maps (map-quality images combining many smaller images), and accurate 3D models (Digital Twins).

The integrated analysis capability provides both direct measurement capability as well as supports AI-powered inspections, according to optelos.com.

Meet New Underwater Player

Source: https://i-hls.com/archives/112991

Feb 07 – The underwater drone market is opening up, from specific drones for extensive scientific research and commercial uses to military drones. Underwater drones are now being used by aquaculture, underwater pipes and infrastructure maintenance, seafloor and ocean life survey, environmental studies, ocean weather monitoring stations, and the shipping maintenance industry.
While current underwater drones can dive for hours and hit medium to low depths, the **DIVE-LD drone** developed by Anduril can go alone on missions for a remarkable total of 10 days, reaching full ocean **depth diving up to 6,000 meters**.

The dual-use platform, developed for defense and commercial uses, is tailor-made for littoral and deep-water survey, inspection, and ISR. According to the company, it is ideal for a variety of missions such as undersea battlespace intelligence, surveillance and reconnaissance, mine counter-warfare, anti-submarine warfare, seafloor mapping and more. It allows for rapid configurations to meet mission-specific needs.

The drone, shaped like a medium-sized submarine, is 3-D printed, a fact that contributes to the low manufacturing time and costs.
While the drone can be customized to execute anti-submarine warfare and undersea combat zone awareness, it can also be built for scientific purposes. It only takes just a few weeks, not months or years, to build a tailored version for each customer, and the drone does not require an off-shore ship for launch. The 19 feet long and four feet wide drone can carry a three-tonne payload, according to screenrant.com. The unique 3D printed outer-body technique is sided with a unique manufacturing method for the core internal components and the buoyancy systems that keep the drone afloat and steady.
The drone can be controlled via cellphone, tablets, computers, and even through immersive Virtual Reality commands.

ISIL procured equipment to weaponize drones through Turkish-based companies: report

Source: https://www.turkishminute.com/2022/02/07/l-procured-equipment-to-weaponize-drones-through-turkish-based-companies-report/

Feb 07 – **Three Turkish-based companies supplied the Islamic State in Iraq and the Levant (ISIL) with materials to assemble and weaponize drones, according to a report by the Birgün daily, citing the findings of Turkey's Financial Crimes Investigation Board (MASAK).**

ISIL is known to have a drone program depending on off-the-shelf technologies and do-it-yourself modifications. The group reportedly makes intensive use of drones for reconnaissance and armed strikes.

According to the report by Bahadır Özgür of the Birgün daily, acting on information sent by Turkey's security forces, MASAK drafted a report in 2021 on the assets of dozens of people considered by authorities to be related to ISIS.

İbrahim Hag Geneid, a Syrian, founded the companies Altun İnci Construction, Elferah Construction and Mavi Yelken Hardware, through which he sold equipment to ISIL operatives who then used the materials to assemble armed drones, the report said.

Geneid was in contact with Babar, one ISIL's drone experts who sent shipments to Syria using Turkey's southern Mersin port and was killed by a US strike in 2017, the report said.

The report added that the Turkish government granted Geneid citizenship in 2017.

According to the report, Altun İnci Construction, founded in 2014, shipped millions of dollars' worth of equipment to Babar.

A 2020 report by the US Department of Defense inspector general had said Turkey is still a transit country for logistics, finance and weapons for ISIL despite the country's efforts to step up the crackdown on the terrorist organization. The 136-page report,

submitted to the US Congress, included the claim, based on remarks from the US European Command, that Turkey is still used as a base by ISIL, particularly for money transfers.
Turkey declared ISIL a terrorist organization in 2013 and has been attacked by the jihadist group multiple times since then. A total of 315 people were killed and hundreds more were injured in at least 10 suicide bombings, seven bomb blasts and four armed attacks organized by ISIL in the country.

Users of Unmanned Aircraft Need to View Risk Mitigation More Holistically

Source: https://www.homelandsecuritynewswire.com/dr20220215-users-of-unmanned-aircraft-need-to-view-risk-mitigation-more-holistically

Feb 15 – A recently published study has found that users of unmanned aircraft, also known as drones, need to take a more holistic approach to identifying and mitigating potential risks before undertaking a flight.
The study, authored by Massey University's School of Aviation lecturer Dr. Isaac Henderson, examined the prevalence of key operational risk mitigations amongst 812 users of unmanned aircrafts (also known as drones) in New Zealand, their confidence in identifying and complying with airspace requirements, and their ability to read Visual Navigation Charts (VNCs) and use AirShare (a tool that shows airspace requirements).
The study found that the only risk mitigation that virually all users applied was conducting a pre-flight check of their aircraft. However, less than a quarter of users typically log their flights on AirShare, check the VNC for the area of operation (useful for seeing airspace requirements and potential dangers in the operating area), check Notices to Airmen that have been issued (these contain aeronautical information that is time-sensitive), or conduct a Job Safety Assessment of the operating area (where you consider potential ground-based and airborne risks in the area and how they will be managed operationally).
Just over a quarter used air band radio to help enhance awareness of what was happening in the airspace around them. While a majority of users did typically apply Model Flying New Zealand (MFNZ) site-specific requirements, these are only applicable when operating at MFNZ sites, which are identified on VNCs so that manned aircraft pilots are aware of the potential for aeromodellers to be flying in the area. Outside those sites, other risk mitigations also need to be applied to ensure that airspace requirements are adhered to and risks are adequately managed.
Dr. Henderson says that users should view risk mitigation more holistically. "It was surprising to see such a low number of users applying risk mitigations where they check airspace requirements or actively consider airborne and ground-based risks. While many in the sample were MFNZ members who followed their own internal procedures for operating at their own sites, it is important that other risk mitigations are applied when operating outside of those sites."

Watch: Iran's Two New UAVs

Source: https://i-hls.com/archives/113114

Feb 15 – Two new advanced and sophisticated drones joined the Iranian Armed Forces on Feb. 12, The Iranian Minister of Defense, Brigadier General Ashtiani, said: "Undoubtedly, drone industry is considered as one of the outstanding and reliable points in increasing authority and defense power of the Islamic Republic of Iran."
"Today, the role of drones is undeniable in battlefield, war, various intelligence and operational missions including surveillance, optical and signal reconnaissance, combat, etc. and this strategic product is one of the main systems in all scenes of land, air, sea combat," he was cited by mehrnews.com.

Cyprus on the air soon

Source: https://www.swarmly.aero/

Swarmly is a startup aerospace company with its HQ and manufacturing facilities in Limassol, Cyprus. Despite being a young and dynamically growing company, company's team is comprised of experienced professionals with expertise in aerospace, operations, law enforcement, and engineering fields.

Swarmly built the first Integrated VTOL Avionics System (IAS) in the world -- R8 Hermes. Hermes can be installed into any airframe equipped with just a propulsion system and instantly provides redundant BVLOS communications, EO/IR imaging, photogrammetry, payload deployment, flight control, GNSS anti-jamming, ADS-B, emergency location, and ground control capabilities. Swarmly's Poseidon line of VTOL UAS is built around the concept of tight integration of best-in-class components from the world-leading manufacturers of UAS airframes, electric and hybrid propulsion components, and payloads with R8 Hermes IAS. Company's manufacturing facilities is equipped with best tools and machines, including one of the largest 5-axis CNC milling machines in the world. Swarmly's production capacity allows for a full cycle manufacturing of all products in house fast.

Extensive Counter-Drone Efforts in the Arab Gulf

Source: https://i-hls.com/archives/113026

Feb 22 – Following several successive drone and missile attacks on the UAE capital Abu Dhabi, most of which have been claimed by Yemen's Iran-backed Houthi rebels, the U.S. Embassy in the UAE warned U.S. citizens of "reports of a possible missile or drone strike" over Abu Dhabi and asked them to take safety measures.

The commander of U.S. Central Command (CENTCOM) has announced that the U.S. has been working with the UAE to develop counter-drone solutions and thwart attacks before they can be launched, according to wam.ae.
The UAE is armed with THAAD and Patriot PAC-3 missile defense systems. But drones remain a potent threat.
Meanwhile, in Kuwait, US soldiers with the 4th Infantry Division trained with the Mobile Low, Vehicle Integrated Defense System (M-LIDS) vehicle-mounted counter-drone system last month as part of the multi-national anti-ISIS formation Combined Joint Task Force – Operation Inherent Resolve in Iraq and Syria.
The Mine-Resistant Ambush Protected vehicle-mounted system uses a combination of sensors to detect aerial threats before disabling them, either through electronic jamming or destroying them with a 30mm cannon or the Coyote small drone.
The system is only a temporary solution for the joint forces, as the military is narrowing its counter-drone options from 40 to 8, and the M-LIDS is not on the list, according to thedefensepost.com.

Terrorist drone attacks: could new technology stop the threat?

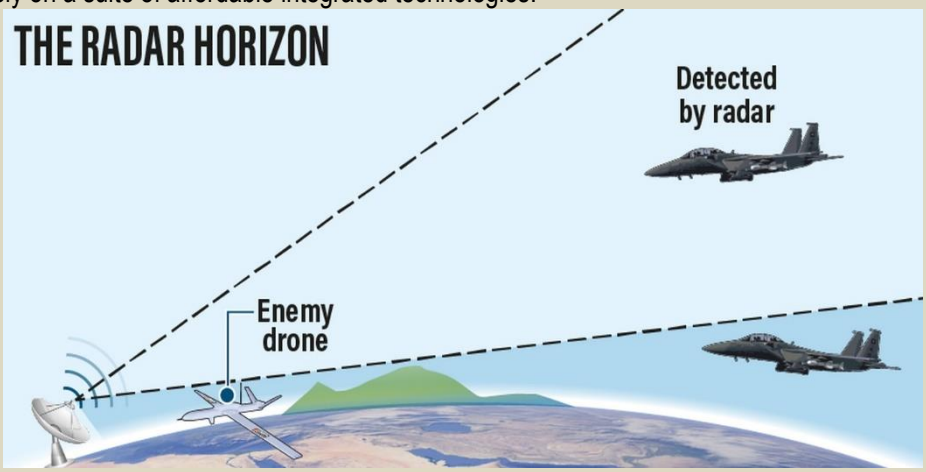
Source: https://www.thenationalnews.com/world/2022/02/23/terrorist-drone-attacks-could-new-technology-stop-the-threat/

Coyote interceptors reached a number of milestones over the summer test period. The Coyote Block 2 overcame threats at longer range and higher altitude than similar class devices, gaining US Army approval for use. All photos: Raytheon

Feb 23 – Easily available, difficult to detect and hard to intercept, small drones pose a challenge to even the world's most advanced militaries.
When Iraqi tanks had ISIS cornered during the battle of Mosul in 2017, the extremists disabled a US-made M1A1 – a 60-tonne behemoth and one of the world's most formidable armoured vehicles – by using a makeshift drone to drop a small grenade next to the commander's hatch.
A drone costing less than $1,000 was able to defeat a tank worth $4 million in an incident that underscored how effective even civilian drones could be in the hands of terrorists who can easily turn them into weapons.

The demonstrated creativity of militant actors suggests that an effective single system solution will remain elusive
Austin Doctor, US National Counterterrorism Innovation, Technology and Education Centre
Terrorists and paramilitary groups across the region, from Yemen's Houthi rebels and Iran's Islamic Revolutionary Guard Corps to Hezbollah and Iraq's militias, have come to regard drones – whether purpose-built or weaponised – as a vital tool in their attacks aimed at destabilising more powerful foes.
But a host of new ideas and technology promises to turn the tide against the use of low-cost drones in conflicts and give state militaries new ways to provide security against unconventional attacks.
From high-tech laser beams and microwave radiation attacks, to bespoke radar systems and electronic signal jamming, modern militaries will be able to call on a whole arsenal of ways to counter the drone threat.
Older systems are also being re-purposed, from fighter jets with powerful "look down, shoot down" radar and helicopters are being given new weapons to hunt unmanned aircraft.
Some new systems are already being used to thwart attacks in the Middle East.

New ways to counter drones
As drone attacks have become more common – including those targeting Saudi Arabia, US forces in Iraq and recently, the UAE – some of the world's best defence technology experts are competing to defeat the threat.
No solution seems too outlandish.
In May, US tech company Epirus claimed that its high-powered microwave system disabled 66 small drones in mid-flight, frazzling their electronics.
In June, Israel's Elbit systems took down several unmanned target aircraft using a laser mounted on a light aircraft.
Companies are also already fielding drones that hunt other drones as well as a host of new, bespoke radar systems and lasers to stop the small aircraft.
Some of these ideas have been years in the making.
The US Defence Intelligence Agency has held an annual counter-drone exercise since 2002 called Black Dart, which has grown into a major contest between contractors.
But it is only recently, after a spate of terrorist drone attacks that US efforts have gone into high gear.
Black Dart's live fire exercise has led to the deployment of a counter-drone laser system on a warship, among other innovations.
Could the days of terrorist drone swarm attacks be over?
"In the case of counter-drone systems, there is no silver bullet," says Austin Doctor, an expert at the US National Counterterrorism Innovation, Technology and Education Centre.
"The variety of drone types deployed by militant forces, and the demonstrated creativity of militant actors suggests that an effective single system solution will remain elusive," he says.
"Instead, a sustainable approach will likely rely on a suite of affordable integrated technologies."
The landscape of counter-drone tech suggests this is exactly what is happening – an array of different methods working in tandem to counter the different drone options available to terrorists.



Why are drones such a problem?
In part, the challenge has arisen from the rapid proliferation of civilian technology – for example, Houthi-drones thought by the UN to have been made with Iranian help had copied engines made by a German civilian company.
One of the main reasons why drones are so difficult to defend against is that they fly extremely low, while most defensive radars are designed to detect high-flying aircraft or missiles.
Imagine a radar beam aimed at the sky searching for a ballistic missile or enemy plane. The missile flies on an arc that can reach tens of kilometres into the atmosphere – or even thousands of kilometres into space. Fighter planes like the F-15 can cruise at 65,000ft, nearly 20 kilometres high.

Now, imagine the radar beam is lowered to detect something low-flying. At some point, the curvature of the Earth, as well as valleys, mountains and buildings come into play.
Just as a torch cannot shine around a corner, radar beams cannot curve around the Earth.
That means an attacking missile, plane or drone can creep up on the enemy using these blind spots called the "**radar shadow**".
At very low altitude, drones can hug the terrain in a way that would require extreme skill and endurance for human pilots.
Aside from the radar horizon challenge, most drones have a small radar signature due to their size, and a low heat signature, making them harder to detect using infrared sensors.
But new approaches are eroding this advantage.

How drones are already being intercepted
Existing air defence systems have already been used to counter drones.
The American C-Ram system, which fires a stream of high-explosive cannon shells at 4,500 rounds a minute, was originally designed to intercept rockets and artillery. It has already been used to shoot down drones attacking US forces in Iraq, but comes with risk if used in populated areas.
Similarly, the US PAC-3 Patriot missile systems, designed to intercept missiles and aircraft, can now also be used to take down drones, albeit at a high cost per interception.
In Israel, the Iron Dome system uses AI-assisted technology to shoot down rockets, but has also been used against drones.
Again, the high cost of using such a system to defend against drones – each interceptor missile is said to cost about as much as a brand-new Nissan Patrol ($50,000) – means the Israelis are interested in finding a cheaper system.
Other approaches involve seeking out drones as they creep through the radar shadow – the blind spots in air defence systems often exploited by drones.
The Raytheon Coyote Block 2 for example, uses drones to hunt drones.
It is likely that Coyote has already been used at Al Asad airbase, a joint Iraqi-Coalition air base in western Iraq which has frequently been attacked by "kamikaze drones", assaults widely attributed to Iran-backed militias.
New electronic jamming systems are in operation. Michael Knights at the Washington Institute for Near East Policy, a think tank, believes they have probably defeated drone attacks in Iraq.
When photographs of downed drones appear in Iraq, it is sometimes possible to assess how they are dispatched, Mr Knights says.
There can be visual clues that show a drone was brought down by a laser.
"Each type of kill has a thermal component. What you want to see is a burn hole on the bottom front," he says, referring to the use of laser systems.
In June, US forces in Iraq said they had deployed Claws, a high-powered laser mounted on the back of a lorry, to tackle smaller quadcopter armed drones.

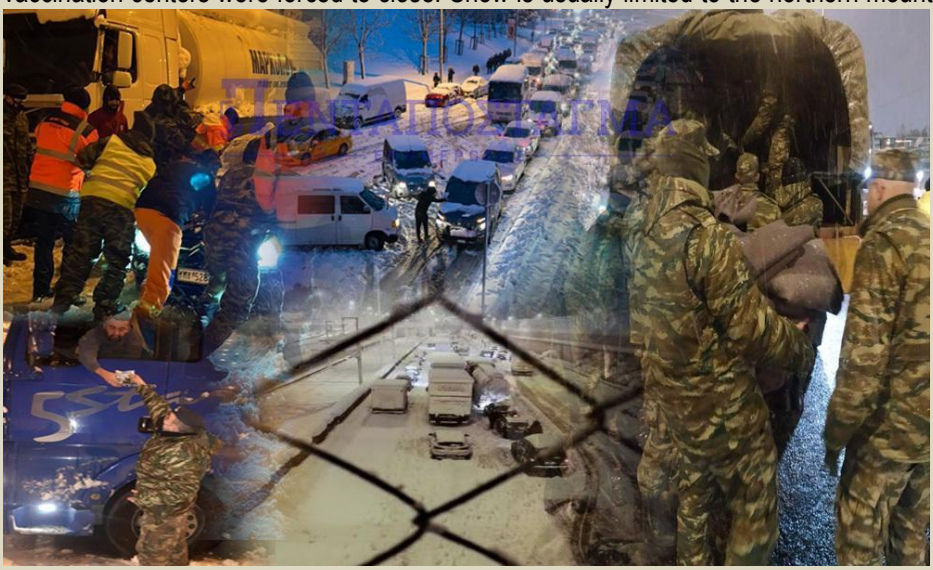
Turning the tide
The deployment of Coyote and similar systems could be a serious hindrance to military operations of Iran's proxies.
In June 2020, a UN report blamed Iran for supplying drones to Houthi militias in Yemen, which destroyed critical oil infrastructure at Abqaiq, Saudi Arabia, in September 2019.
In the promotional video for the Coyote system, one of the drones destroyed has a triangular, or "delta" wing shape, similar to the drone type used at Abqaiq and in a lethal attack on the *MT Mercer Street* commercial ship in July.
"They're getting quite annoyed," says Mr Knights, referring to Iran-backed groups.
"We had them claiming fake drone attacks, as it doesn't produce visible evidence of interception. So, better to claim a false attack than undertake a real one."
If drones used by Iran-backed groups represent a cheap option, it makes sense to counter them with inexpensive technology.
"Narrowing the cost ratio remains one of the primary challenges to developing an effective and sustainable counter unmanned aerial vehicle infrastructure," Mr Austin says. Compact laser weapon systems, which are cheaper than missile interceptors, are a big step forward, he says.
Raytheon emphasises the cost-effectiveness of new systems, saying Coyote interceptors could eventually cost as little as $5,000 each, leaving systems like the $1bn Patriot to defend against more expensive, fast moving ballistic missiles.
But some analysts caution that even if militias take a hit from the use of counter-drone systems, the threat the groups represent will persist. "I feel we shouldn't fall into panacea talk," says Phillip Smyth, a fellow at the Washington Institute.
"The US and Israel have plenty of anti-rocket and anti-guided missile systems. However, the weapons continue to get launched and new strategies with old weapons systems will be developed."


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

The only solution (for Greece)

By the Editor-in-Chief

Jan 28 – Large parts of Greece were covered in a blanket of snow Monday (Jan 24). It was an unusual occurrence for the southern Mediterranean countries, but the second time that it has happened in two years. The rare snowstorm — called "Elpida" or "Hope" in Greek [what a stupid name …] — brought the Greek capital Athens to a standstill. Overnight temperatures fell to -14^{0}C. Schools and vaccination centers were forced to close. Snow is usually limited to the northern mountainous regions of Greece, rarely falling with such intensity in Athens. The Greek government declared a holiday for parts of the country, including the capital, to keep people from going outside. Thousands of drivers in the city (along the private road Attiki Odos and the E75 National Highway) were stuck in their cars for hours with rescue workers braving the cold to free the stranded motorists. Many motorists in Athens were stuck in their cars for up to 15 hours. The military was asked to support the civil protection personnel. A snowstorm in February last year left four people dead across Greece as well as cutting power for thousands of residents for several days. Kostas Lagouvardos, research director at the National Observatory of Athens, told ANT1 TV that the capital had not seen back-to-back winters like this since 1968. Snow fell on several Aegean islands, including on the beaches of popular tourist spot Mykonos.



The overall situation was chaotic. The state, despite most praised preparedness and coordination meeting, was not prepared and involved entities accused each other regarding responsibilities and level of effective mobilization. Main road arteries within the capital were finally open but smaller side roads across the Attiki Prefecture will take days not to say weeks to return to normal. I live in a suburb village of Athens just 38 km away from Syntagma Square at an altitude of 623m. We also were covered by snow (~50cm) and I expect to be able to go to the nearest village in a week or so. I do not live on Mount Olympos (2.917m); I

live just 50min from Athens downtown. Thank God, this time we had electricity and water but big parts of the capital did not for hours/days.

An adverse physical phenomenon that is not rare in many EU countries caused major disturbance to thousands of people and halted normal life for many days. Unfortunately, it is not the first time that this happens whether it is snow, heavy rain, and flood, extremely hot weather, an earthquake – fortunately, we did not experience a tsunami so far! In all instances, the progress of the phenomena required the intervention of the military. So, let's make it official! Let the Hellenic Armed Forces General Staff run all the natural disasters and extreme weather phenomena and give them the funds allocated to the newly formed Minstry of Climate Crisis and Civil Protection

(what a title!) without viable results. This is a brave decision that will disappoint certain gov chair holders but Greece comes first!

Nobody Saw It Coming: How Scenarios Can Help Us Prepare for the Future in an Uncertain World

By Mann Virdee and Megan Hughes

Source: https://www.homelandsecuritynewswire.com/dr20220201-nobody-saw-it-coming-how-scenarios-can-help-us-prepare-for-the-future-in-an-uncertain-world

Febr 01 – Several months after the collapse of Lehman Brothers and the start of the global financial crisis in 2008, it was reported that Her Majesty, Queen Elizabeth II, caught economists at the London School of Economics off guard with a simple question: "Why did nobody see it coming?"

As the world began to grapple with the COVID-19 pandemic, this question would again have been at the forefront of policymakers' minds around the world. It prompted other questions too. What would the world look like today had we been better prepared for a global pandemic? How can we build resilience against unknown future threats?

The problem with planning for the future is that it is fundamentally uncertain, and predictions often fall flat when compared with reality. However, this gap—between the limits of what we can know about the future and the need to plan for it—has led to the development of a variety of tools for futures thinking. Many of these tools are employed by researchers at the RAND Europe Centre for Futures and Foresight Studies (CFFS), and one of the most critical is scenario planning.

Scenarios are not about predicting the future. They are, rather, a rigorous and methodical way to consider several imagined future situations, or contexts, which could come to pass. Generating scenarios typically involves identifying a set of influential "drivers of change" whose outcomes may be predictable, such as demographic changes. Combinations of these drivers create a range of plausible future states.

However, the scenarios don't have to become reality to be useful to decisionmakers. Scenarios help decisionmakers think strategically by incorporating uncertainty into policymaking, challenging conventional wisdom and core assumptions in current thinking. By identifying potential trajectories that may not have been considered, scenarios can help to prepare and innovate for the future.

For example, a foresight study conducted by RAND Europe and DAMVAD Analytics helped inform the Research Council of Norway's (RCN) contribution to their government's long-term plan for research and higher education.

The study developed two sets of scenarios, one for Norway in a national context and the other in a global context. For each of these sets, four distinct future scenarios out to the year 2040 were developed. Through these scenarios, researchers helped identify 20 priority research and innovation (R&I) "missions" that the RCN could consider implementing in the future with other stakeholders, such as enhancing Norway's world-leading capabilities and expertise in future maritime technologies. The scenarios helped researchers to examine what might happen in the next 20 years in RCN's different strategic areas and the wider R&I system in Norway and allowed them to further identify potential structural measures that could aid the development of a resilient R&I environment.

In another study for Innovate UK, RAND Europe used future scenarios to explore what British infrastructure could look like in 2035 and how potential future congestion problems might be addressed by technology.

Future travel scenarios were developed based on combinations of factors, such as high economic growth or slower-than-anticipated economic growth, increased use of digital substitutions for travel, and lack of access to advanced technologies because of income inequality. This scenario work identified key recommendations for government agencies looking to encourage efficient and effective transport. One recommendation was to address barriers to innovation for autonomous vehicles, such as future liability and safety regulatory issues.

Scenarios are a useful tool for informing policy, guiding strategies, and accommodating future change. Using scenario planning to target potential problems or areas for development and building resilience can pinpoint robust policies that could be viable across a range of future states.

However, when working with scenarios, users can face certain pitfalls. Scenario planning is sometimes mistaken for a method that can predict the future. Also, in conducting scenario planning, certain scenarios can be viewed as preferred or more likely—but this is to misunderstand the purpose of scenarios. Scenarios do not provide certainty, rather they equip decisionmakers with readiness to address uncertainty.

Everyone can benefit from thinking strategically about the future and at CFFS, researchers help organizations from all parts of society use scenarios to be able to make better decisions today. RAND Europe established the CFFS to capitalize on its expertise in futures and foresight studies and help clients discuss and address challenges. Scenario planning could

be an indispensable tool for decisionmakers looking to prepare for extreme events, whatever shape they may take. It might not be possible to predict what is coming, but we can be ready for it.

Mann Virdee and **Megan Hughes** are researchers at *RAND* Europe and the RAND Europe Centre for Futures and Foresight Studies.

Top 10 Habits for Better Crisis Preparedness

By Andrew (Andy) Altizer

Source: https://domesticpreparedness.com/commentary/top-10-habits-for-better-crisis-preparedness/

Feb 02 - Imagine an important grant application deadline approaching next month, delaying the submission for a couple weeks, but then a critical incident happens (perhaps, something like a pandemic) that diverts attention for weeks, months, or much longer. The routine tasks that require action are not performed in a timely manner, and the deadline for that grant application is now gone. Developing some small habits like prioritizing would have significant effect on productivity and effectiveness of response and recovery efforts for a future crisis.

When time permits, in-depth quantitative research offers valuable information for disaster preparedness and response. However, the foundation of preparedness is rooted in the day-to-day activities that prevent small events from becoming big crises and help manage large events that cannot be avoided. As such, the following little habits can have big effects both operationally and administratively for any emergency or disaster.

Key Habits to Better Preparedness

By incorporating the following 10 habits into daily routines, emergency preparedness professionals will be better prepared to manage and adapt to any sudden or evolving events.

Ten small habits can have big effects both operationally and administratively when preparing for any emergency or disaster.

1. *Prioritize* – It is vitally important to prioritize. As Stephen Covey (author of *The 7 Habits of Highly Effective People*) pointed out, "put first things first." It is also important not to neglect less important but necessary tasks. These less important – or perhaps not as urgent – responsibilities can become problematic when suddenly faced with a sustained situation that demands significant amounts of time.
2. *Save all contacts and cellphone numbers* – It is difficult to predict exactly when help will be needed and from whom. Trying to find the right contact when needed can be an exhausting and time-consuming process when time management is crucial. So, the best practice is to immediately save any new contact. It is an invaluable trait to always have the right contact and phone number at the ready whenever needed.
3. *Get out of the office* – This is not a new piece of advice, but a critical one. Getting out of the office enhances situational awareness, builds relationships, and often provides the subtle motivations that drive emergency preparedness efforts.
4. *Write it down* – Emergency preparedness professionals are often overwhelmed with tasks and changing priorities, so it can be easy to forget obligations. Relying on an electronic calendar is great, but sometimes having a physical list of tasks posted in strategic locations can serve as a better daily reminder that is more difficult to ignore.
5. *Build relationships* – Relationships should be vertical as well as horizontal. One of the tenets of the emergency management profession is to build relationships, with an emphasis on collaboration. However, it is vitally important to continue expanding these relationships with people several levels down. Chiefs, directors, managers, etc. will retire or suddenly leave. As their subordinates move up, how they perform their new roles and treat others may depend on how their superiors treated them.
6. *Build capacity* – Emergency managers plan for the worst, but limited resources often collide with competing and more timely needs – especially when planning for less likely scenarios. Building capacity should begin now and continue until all necessary resources are acquired. For example, when planning for a shelter, there may not be enough funding to purchase 50 cots. Preparedness does not require an all or nothing approach. Start with 10-15 cots this year and continue each year until there are enough for a fully equipped shelter. As an old Chinese proverb says, "The best time to plant a tree was 20 years ago. The second-best time is now."
7. *Tie in the Overarching Organizational Mission With Every Task* – Often, simply highlighting public safety or continuity of operations can provide critical reminders to ensure that emergency management functions remain a priority within the organization.
8. *Dress for the Day, but Have a Change of Clothes* – Be prepared for sudden and unexpected changes. There are plenty of people who still do not know what emergency managers do daily. The emergency manager's role is evolving and is often misunderstood, with many people still confusing "emergency management"

with "safety and security." Wearing cargo pants and an emergency management polo is a small, but important, way to demonstrate that emergency management is an integral part within the overall organizational professional staff. In addition, be ready to pivot when suddenly thrust into responding to a crisis out in the rain while when wearing a coat and tie.

9. *Expect to Be Audited* – Sometimes emergency managers procure items that raise red flags to those not familiar with the responsibilities and duties of the job. These red flags may generate an audit. Planning for a worst-case scenario does not fit neatly within the normal supply needs. In addition, most equipment purchases are often subject to auditing. However, auditing may include plans as well as equipment. Emergency preparedness professionals should welcome any audit that will strengthen these plans and the overall operation.
10. *Think transparency* – Keep in mind that most written communications and documents are subject to open records. Although transparency should be the standard, avoid including any personal opinions in emails and social media.

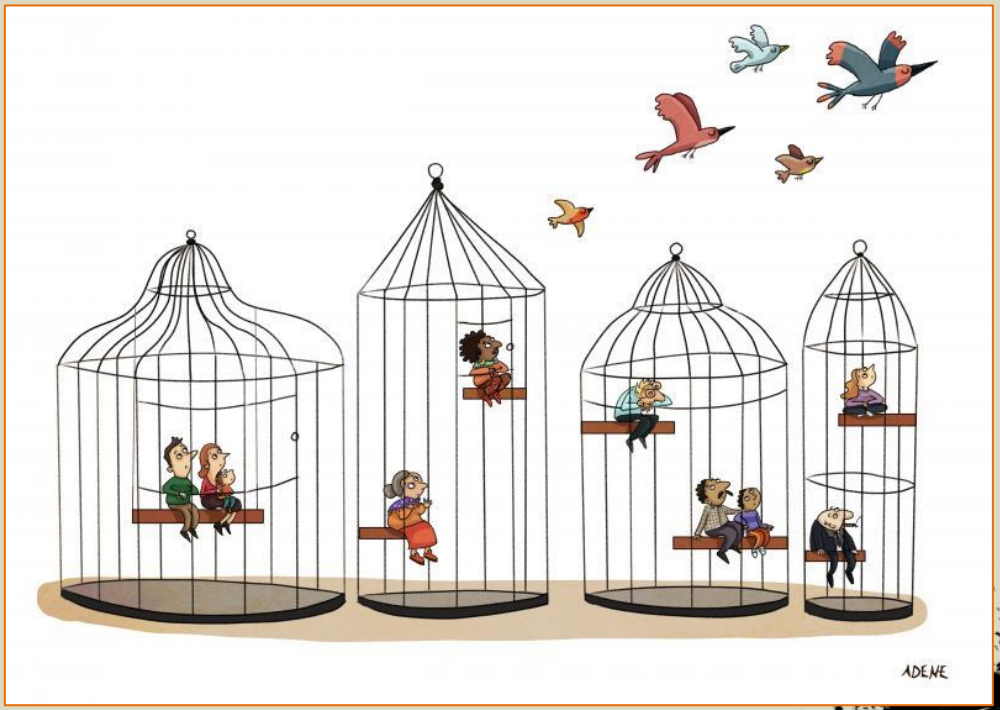
Additional Tips to Maintain Perspective

In addition to the habits above, there are a few more tips that can help emergency preparedness professionals develop more robust professional perspectives:

- Emergency management demands leadership. Egos do not belong in community-based professions. Become a good listener, build and maintain trust, and never forget the importance of empathy. Give credit often, and fully embrace the enormous benefits of teamwork.
- Do not forget to be a good follower. This is especially important within the Incident Command System, where emergency managers are seldom the incident commander but are always critical in supporting roles.
- Finally, have a family plan for times when work takes priority. Not only will such planning prove valuable to family members, but it also will reduce personal stress levels during stressful times. Remember that taking time off is not only deserved but is also needed at times.

Now, with the grant application, knock it out as soon as time permits. Do not wait for downtimes or breaks in schedules because these opportunities are rare. Update "to do" lists to ensure that daily habits provide ample opportunity to knock out less pressing tasks – like submitting a grant!

Andrew (Andy) Altizer is the director of emergency management at the Department of Public Safety, Kennesaw State University. He previously served as the director of emergency preparedness at Georgia Tech, and as the critical infrastructure protection program manager at Georgia Emergency Management Agency. He has a Master of Arts degree in Higher Education Administration from the University of Missouri, and Bachelor of Science degree in Criminal Justice from Truman State University. He also has over 10 years of military experience, including in Afghanistan in 2002.



Because international CBRNE First Responders need a common roof!

https://www.ici-belgium.be/