06\22

C'BRNE DIARY

Dedicated to Global First Responders

June 2022

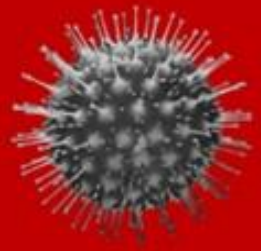
Part B

Pandemic

Epidemic?

War

Alien invasion?



The unexpected always happens!

An International CBRNE Institute publication

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

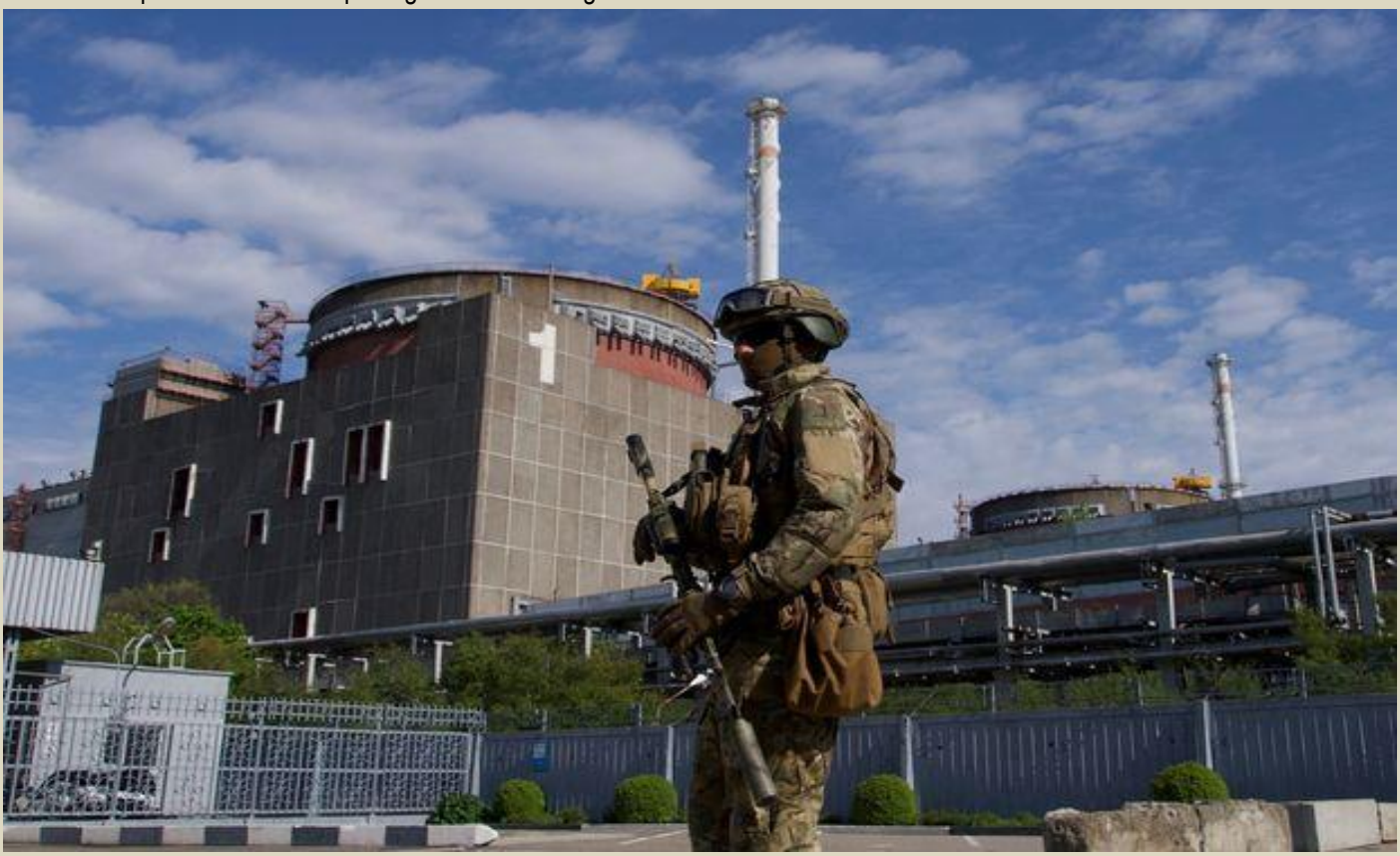
W O M D

C2BRNE DIARY

DIRTY R-NEWS

U.N. Atomic Agency Chief Presses for Access to Zaporizhzhia Nuclear Plant

Source: https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-05-25/card/u-n-atomic-agency-chief-presses-for-access-to-zaporizhzhia-nuclear-plant-g7vHkGVBMtlvYgYQPakd



A Russian serviceman patrols the territory of the Zaporizhzhia Nuclear Power Station in Ukraine at the start of May.andrey borodulin/Agence France-Presse/Getty Images

May 25 – U.N. atomic agency chief Rafael Grossi said he is pressing for access to the Zaporizhzhia nuclear power plant in Ukraine, which is Europe's largest such facility containing six reactors.

"We hope to go there to be able to prevent...a problem, or we end up finding that there are a few hundred kilograms of nuclear weapon-grade material going missing. This is what keeps us awake at night at the moment," Mr. Grossi said at the World Economic Forum in Davos, Switzerland, on Wednesday.

The Zaporizhzhia plant has been under the control of Russian forces since the early days of the Ukraine invasion but Ukrainian staff continue to operate the facility. Mr. Grossi, head of the International Atomic Energy Agency, said **the site contains 30,000 kilograms of plutonium and 40,000 kilograms of enriched uranium.**

Mr. Grossi has already traveled to the Chernobyl nuclear site, which was also occupied by Russian forces before being handed back to Ukraine in March, bringing supplies to the nuclear plant to ensure safety there.

He has repeatedly called for Ukraine and Russia to agree to measures to ensure the safety of Ukraine's four active nuclear sites, including guaranteeing emergency support and supplies can reach the nuclear plants in case of an incident.

Nuclear tragedy in the Marshall Islands

By Sally Clark

Source: https://thebulletin.org/2022/05/nuclear-tragedy-in-the-marshall-islands/

Crater left by the 1954 Castle Bravo nuclear weapons test on Bikini Atoll seen from space (Google, Maxar Technologies, Image Landsat / Copernicus, Data SIO, NOAA, US Navy, NGA, GEBCO).

May 25 – We were innocent 21-year-olds entering an organization called the Peace Corps in 1969. We came from all over the United States, some wanting to dodge the draft, but most of us were embracing a desire to help others. We were thrilled looking out the window of Micronesia Air plane peering down at a beautiful atoll, a thin necklace of green trees and white sandy beaches, floating on the vastness of the Pacific Ocean. As we approached for landing, we buzzed first over the runway to clear all the trucks, pigs, cars, chickens, and people off the landing area. Then we landed, on the rough runway, the pilot forcing the plane into reverse to come to a stop, much to our relief, at the end of the concrete road in Majuro, looking across at the Pacific Ocean.

We stepped off the plane and into an extremely humid hot environment, where we received greetings by the Marshallese placing leis over our heads, so many leis that they were eventually stacked all the way to our chins. Young, naive Americans, we knew little about the area, other than, perhaps, fleeting thoughts that we might find the remains of Amelia Earhart or artifacts from her plane there.

Our naivete began to diminish when we were told the Atomic Energy Commission was coming to check out the health of the children and adults and of course to give out candy and show a dated movie. We asked questions and learned about the nuclear test over Bikini and the fallout coming down over a neighboring island, whose residents thought it was snow. We were told that the Marshallese ran outside, allowing the fallout to land on their skin, with some children putting it to their

eyes. Luckily many residents sensed danger and ran to the ocean, saving themselves from a future road of at least some fallout ailments.
As we spent more time in the islands, little by little more detailed stories emerged—of still births, high cancer rates, and other radiation-related health issues. Islanders had been moved from Bikini before nuclear tests were conducted; some of the explosions were so great that one of the small islands simply vaporized, leaving a deep cavern. Many Marshallese had to endure being relocated from their blessed atoll to Kili, an island in the middle of the ocean with no lagoon.
Over the years, more and more people spoke out about such atrocities and such disregard for the Marshallese, who were actually called "savages" by a US paper in the 50's. My heart wept as I learned more information about the scope of nuclear testing in the Marshalls.
Between 1946 and 1958, the Marshall Islands region was the site of the testing of nuclear weapons equivalent to the explosive power of 1.6 Hiroshima bombs every day for 12 years—67 in all at the Bikini and Enewetak atolls—a fact that is impossible for me to comprehend.
A resolution is now in front of the Congress asking the United States to prioritize nuclear justice in its negotiations with the Marshall Islands on an extended Compact of Free Association between the countries. The resolution recognizes that the United States nuclear testing program and radioactive waste disposal, including not just contaminated debris from the Marshalls but also material transported from the Nevada Test Site, caused irreparable material and intangible harm to the people of the Marshall Islands. We believe this harm continues to this day. Within this resolution is a call for an apology for what the United States did to the Marshallese and to raise awareness about the need for more action to undo this harm. US Rep. Katie Porter of California and senators Mazie Hirono of Hawaii and Edward Markey of Massachusetts are spearheading this effort, which would formally apologize for the US nuclear legacy in the Marshall Islands and raise public awareness of the issue. Please write or call your representatives and senators, asking them to support House Joint Resolution 73 and Senate Joint Resolution 40.
What happened in the islands is simply incomprehensible to me. The toll on the Marshallese and the environment is impossible for me to grasp. And I have another nagging thought: Why as Peace Corps volunteers were we not warned about the radioactive fallout and the social issues we were being dropped into? Of course, there's the implication that we were being used as pawns to smooth the relationship between the Marshall Islands and the United States and to continue to have the islanders as our friends for strategic reasons.
Who makes these decisions to drop bombs on such beautiful, pristine islands? Who sends 20-year-olds into a potentially radioactive area without warning them? When can we as a human race honor peoples around the world and get out of building weapons and gaining lands for strategic reasons? Please stop. I'm sad and weep and write letters asking for an apology. So sad. Where is our soul?

Sally Clark served as a Peace Corps volunteer in Marshall Islands in Majuro from 1969 to 1971. She then became a high school teacher and the coordinator of global education in her district in Newark, California. Since retirement, she has been a practicing psychologist focused on developmental issues in adults and children.

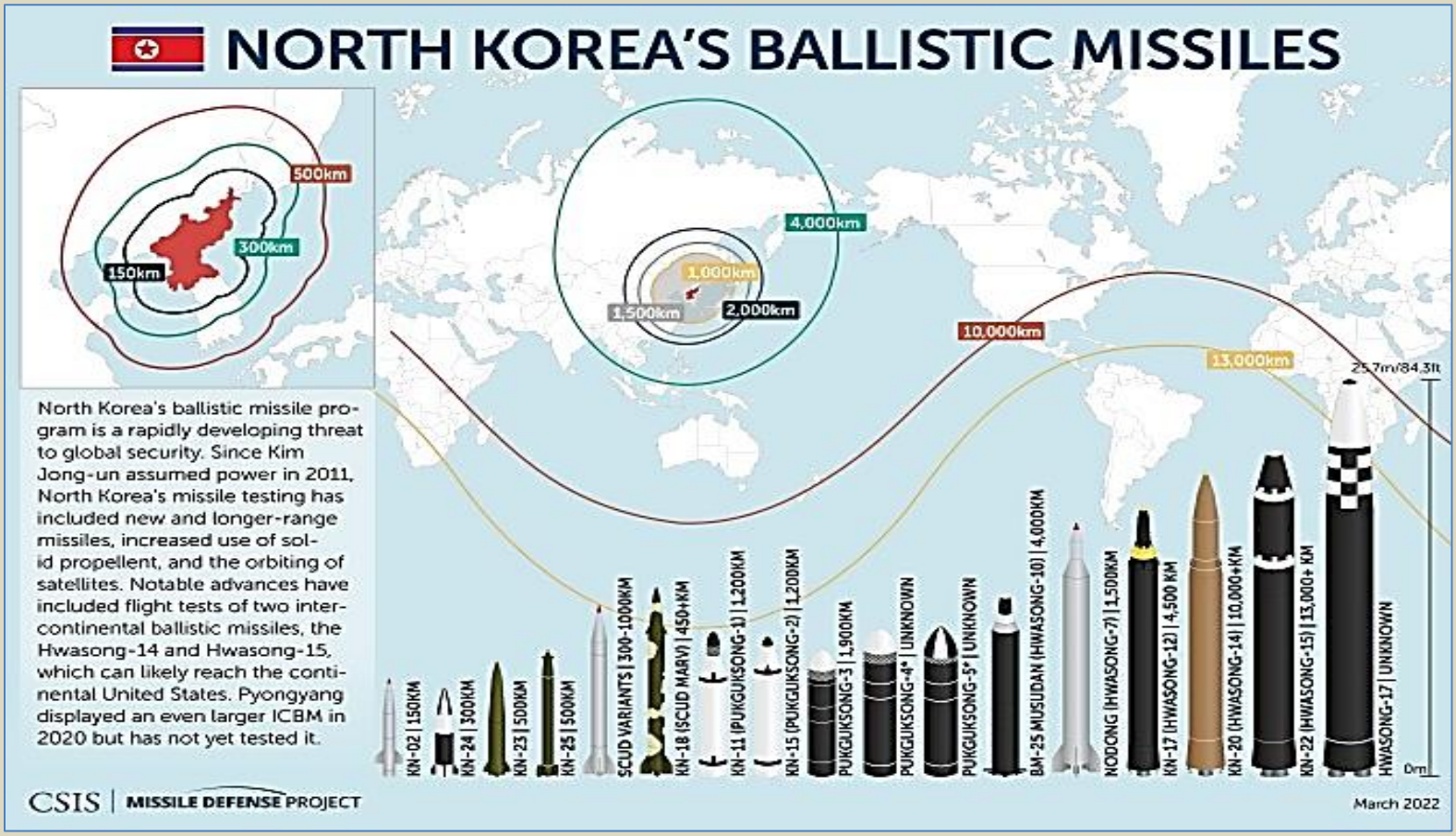
Making sense of North Korea's recent ICBM and (possible) nuclear tests

By Seiyeon Ji and Victor Cha
Source: https://thebulletin.org/2022/05/making-sense-of-north-koreas-recent-icbm-and-possible-nuclear-tests/

May 27 – In a reversal from its earlier position, North Korea test-launched on Wednesday a suspected intercontinental ballistic missile (ICBM) and two shorter-range weapons—only hours after US president Joe Biden concluded his trip to Asia. In April 2018, North Korea's leader, Kim Jong-un, had declared a self-imposed moratorium on nuclear weapons and long-range missile tests after three successful ICBM launches in 2017 demonstrated their potential range to reach the United States.
In contrast, in the first half of 2022 alone, North Korea has conducted more than 18 weapons tests—an alarming development given their frequency and variety. During this period, North Korea not only tested long-range missiles capable of reaching the continental United States, it also launched short-range and intermediate-range missiles, and tactical missiles—as well as submarine-launched, train-launched, hypersonic, and cruise missiles.
Each new North Korean missile test—regardless of its success or failure—brings Pyongyang closer to its goal of developing a credible, survivable nuclear weapons delivery system that can target the US homeland.

Recent missile developments
During its military parade in October 2020, North Korea also revealed the development of a larger Hwasong-17—the world's largest liquid-propellant missile ever built, and deployed on

a road-mobile launcher to date. A missile of this size suggests North Korea's intends to arm the weapon with multiple warheads to overwhelm US national missile defense systems. The military parade also showed that North Korea appears to be indigenously designing launch vehicles for large missiles, including the Hwasong-17. This is significant because the survivability of North Korea's ICBM force will heavily depend on the number of launchers they are about to build.
These developments point to North Korea achieving major technical benchmarks to quantitatively and qualitatively expand its nuclear-capable delivery force.



But North Korea's advances are not just in building better, more capable, and more precise missiles. Its credible missile capability is now being accompanied also by a credible strategy. At the 8th Workers' Party Congress in January 2021, Kim Jong-un laid out—in unusually specific details—his goals for North Korea's weapons development. During his remarks, Kim outlined three major objectives for North Korea's ICBM program likely to be the focus of future missile tests: multiple independent reentry vehicles (MIRVs) capable of hosting several warheads on a single missile, longer-range ICBMs with a 15,000-kilometer capability (about 9,321 miles), and solid-propellant ICBMs. Such new solid-fuel ICBMs take much less time to prepare for launch, making them quicker to turn around in a crisis—which consequently shortens the time the United States and South Korea might have to pre-empt these systems before they are launched.
The development of MIRVs by North Korea would be particularly negative for US security interests. With a limited number of missile defense interceptors designed to cope with North Korean ICBMs, a multiple warhead delivery system would significantly increase the threat to the US homeland. North Korea currently houses at least 10 ICBM launchers, including six launchers that were converted from Chinese *Wanshan* logging trucks and four 11-axle Hwasong-17 launchers. The United States currently has 44 ground-based interceptors that can handle limited ICBM threats from North Korea. As international security analyst Ankit Panda noted, "if you assume a worst-case scenario where [the U.S.] end[s] up using four interceptors per incoming reentry vehicle and you see single reentry vehicles, basically the North Koreans need to build one more launcher to saturate the existing capability."

New nuclear activities

In addition to accelerating the development of survivable nuclear weapons delivery systems, there are now signs that North Korea may resume testing of its atomic bombs. US and South Korean intelligence agencies are on alert for a possible nuclear test by North Korea. On Wednesday, May 25, South Korea's deputy national security advisor Kim Tae-hyo

commented in a press briefing that North Korea has been testing a nuclear-triggering device in preparation for what would be the country's seventh nuclear test. If conducted, this test would mean that Pyongyang is also breaking its self-imposed moratorium on nuclear weapons testing.
The strategic analysis program "Beyond Parallel" by the Korea Chair at the Center for Strategic & International Studies (CSIS) has used high off-nadir satellite imagery to monitor activity in the village of Punggye-ri where all of North Korea's previous six nuclear tests have been conducted. Most recent imageries collected on May 17, 2022, indicated that there was continued expansion of the support infrastructure for the Punggye-ri nuclear testing facility—including changes in lumber piles, renovation of existing buildings, and construction of new buildings in the main administration and support area. Satellite images also revealed progress over the past three months in the refurbishing work and preparations at Tunnel Number 3. Such activity, if completed, will signal that North Korea has prepared for a possible nuclear test. The war in Ukraine may also have affected the doctrine that informs North Korea's pursuit of nuclear weapons and delivery capabilities. At one level, Russia's military attack on Ukraine provides a confirmation to Kim Jong-un that his nuclear pursuits are the best way to deter any external threats. At another—more worrying—level, however, is the possibility of Kim seeing benefits in adopting a nuclear first-use strategy. Putin's threats of nuclear weapons use—or, at least, his unwillingness to rule out their use—in response to any NATO intervention in Ukraine may influence the way Kim thinks about his ability to deter the United States from intervening on the Korean peninsula. In recent statements, Kim already referred to the possession of nuclear weapons as a deterrent and a secondary use as an "unexpected second mission" if outside forces violate its "fundamental interests."

Deterring North Korea
Additional testing—particularly of MIRV capabilities—will be one of the greatest security challenges to the United States and South Korea. While there are no easy options to prevent further advances in North Korea's weapons program, several steps could help altering Kim Jong-un's cost-benefit calculations for his missile development efforts. First, the United States and South Korea should upgrade their defense and deterrence capabilities on the Korean Peninsula. In addition to reactivating the suspended Extended Deterrence Strategy and Consultation Group—as promised in last week's Biden-Yoon summit—the allies should consider other measures to integrate early warning systems, strike capabilities, and the rotation of dual-capable assets to the peninsula. Second, the two allies, along with Japan, should pursue a broad counter-missile strategy that involves detecting and defending against North Korean missiles and launchers, disrupting North Korea's network of capabilities that allow them to fire missiles repeatedly, and destroying the launchers and missiles themselves. This would require the United States and South Korea to invest in capabilities like sensors, advanced command and control systems, and intelligence, surveillance and reconnaissance technology. Third, the United States can encourage Seoul to continue developing its indigenous capabilities to help protect South Korean critical infrastructure from North Korean missile barrages. South Korea's version of the "Iron Dome"—an artillery interception system deployed by Israel—is an example of the types of capabilities it can develop. The United States, Japan, and South Korea should also increase trilateral coordination on missile defense. This would require South Korea to rethink its long-held position that it would not cooperate with Japan and the United States trilaterally on detection, warning, tracking, and interception of ballistic missiles. For its part, the United States should consider shifting the focus of its diplomacy from completely shutting down North Korea's nuclear program to slowing down or halting its missile testing. As North Korea comes closer to its capacity to overwhelm US national missile defenses, such policy reorientation is becoming more urgent. For as long as North Korea refuses to return to the negotiating table, the United States could consider integrating ideas for possible "carrots" and "sticks" in the missile realm into existing potential roadmaps for nuclear diplomacy.

Seiyeon Ji is a research associate at the Office of the Korea Chair at the Center for Strategic & International Studies (CSIS).
Victor Cha is senior vice president and Korea Chair at the Center for Strategic & International Studies (CSIS).

Radiological and Nuclear Hazards Still Exist—A.L.E.R.T. Responding

By Col. (ret.) Ron Fizer
NCT Magazine | 11/20
Source: https://nct-magazine.com/nct-magazine-may-2022/radiological-and-nuclear-hazards-still-existalert-responding

The threat of nuclear use is as real today as in any year since 1945, as nine known countries possess nuclear weapons and the competition between great powers is creating an increasingly strained security environment. Nuclear weapons are not the only potential source of significant radiological hazards. Currently over 440 nuclear reactors operate in 32

countries and there are plans for the construction of many more. The events in Ukraine serve as a stark reminder that nuclear weapons are still a major threat and radiological hazards are a reality in modern combat operations.
The occupation of the nuclear compromised site at Chernobyl highlighted the risks of military operations in a radioactive environment. The area is now at risk for additional damage to the reactor that could release the contained radioactive material in the reactor complex. Additionally, Russian control of the site increased exposure of troops and personnel to radioactive contamination, increased as troops dug positions and disturbed materials during their occupation. The conflict also emphasizes the real threat of nuclear deployment in military operations. Russia possesses one of the largest nuclear arsenals in the world. It is time to implement acknowledge, leverage, exploit, revise, and train (A.L.E.R.T.) protocols to these radiological and nuclear (RN) threats and ensure military operations can prevent or successfully respond to these effects. Widespread adoption of the A.L.E.R.T. system will ensure military operations can prevent or successfully respond to these effects.
Acknowledge The first key step to improve military readiness against RN threats is to acknowledge that there is a threat. While it is generally understood that nuclear weapons fall solidly within the threat category, they are typically considered "low potential for use". This probability is heightened if radiological hazards are encountered during military operations. The danger further increases when a military force lacks the proper equipment, training, and procedures to understand and mitigate the risk from RN hazards.

Leverage
One way to improve is to leverage existing radiological detection capabilities and modernize them. Many of the extant chemical, biological, radiological, and nuclear (CBRN) testing materials are likely to be several decades old. In many cases, commercial radiological detections systems can provide more capable solutions. Modifications can be quicker and provide significantly more sustainable and efficient capabilities to military organizations. Modern detectors also offer the ability to connect to command and control networks and share information across military formations rapidly, promoting better decision making. Radiological and meteorological data from the civilian sector, networked with decision- making tools the military already has, provide a power-couple approach for large operational areas. Protective measures for units informed by plotting radiological hazards with greater precision enhance the operational capacity of all branches of service.
Acknowledge The first key step to improve military readiness against RN threats is to acknowledge that there is a threat. While it is generally understood that nuclear weapons fall solidly within the threat category, they are typically considered "low potential for use". This probability is heightened if radiological hazards are encountered during military operations. The danger further increases when a military force lacks the proper equipment, training, and procedures to understand and mitigate the risk from RN hazards.

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

Ron Fizer is an U.S. Army Colonel (retired) and Fellow at LMI Consulting, Inc. He lends his technical and analytical expertise to solve complex problems related to countering weapons of mass destruction (CWMD) and chemical, biological, radiological, and nuclear (CBRN) defense. A highly regarded technical expert, Fizer is sought by a wide range of clients to rapidly develop integrated capabilities and implement those solutions into their operations to improve readiness and reduce risk. Before joining LMI, he spent 30 years in active duty, serving in various command, staff, and leadership positions across the Army, Joint Staff, and Secretary of Defense staff in tactical, strategic, and institutional support organizations within the United States, Germany, South Korea, and Iraq.

Remote detection of alpha and gamma radioactivity using unmanned aerial vehicles

By Dr. Arturo Vargas
NCT Magazine | 11/20
Source: https://nct-magazine.com/nct-magazine-may-2022/remote-detection-of-alpha-and-gamma-radioactivity-using-unmanned-aerial-vehicles

The protection of first responders and the public against radioactive contamination caused by radiological accidents is a matter of enormous importance, especially in the event of terrorist attacks and war scenarios such as the invasion of Ukraine, where radiological facilities and nuclear power plants were affected by the attacks of Russian troops.
Following a nuclear or radiological event, knowledge of how contamination spreads and the area it covers is essential for decision makers who must determine the most appropriate response. In the immediate vicinity of a nuclear or radiological scenario, as well as in case of a large-area ground contamination, and before first responders can enter in the

contaminated area, remote detection of alpha and gamma radioactivity by using unmanned aerial vehicles (UAVs) are an excellent solution to protect operators and early responders against contamination and irradiation.
Since the radionuclides in the scenario are usually unknown and there is no optimal detector-UAV configuration, the end-user should analyze the most likely radiological situation in terms of type of radionuclides and dose rates in order to select the most convenient configuration. In such context, spectrometric gamma detectors that can identify radionuclides are recommended to be mounted on the UAVs. "Classical" dose rate monitors such as Geiger-Muller (GM) tubes can be used for a fast screening to evaluate the dose rate map for further analysis with spectrometric detectors. In the European project "Preparedness" spectrometric detectors were adapted and mounted on selected UAVs based on their flight capabilities. The airborne detectors mounted on the UAVs were tested and calibrated in measurement campaigns. In case of a radiological scenario involving dispersion of alpha emitting radionuclides in the environment, the situation is more complex because, there is no available detection system to measure remotely alpha particle at present. In case of such an emergency, the only option is to evacuate the population from the affected areas and then run diagnostics by hand, thus exposing the emergency teams to considerable risk. Even then, the results of emergency field applications are notoriously ambiguous, time consuming and tedious due to the centimetre range of the alpha particles in air. Currently, in the European project "remoteALPHA", a remote alpha airborne monitor to be mounted in UAVs will be tested in experimental campaigns during the next months.

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

Dr. Arturo Vargas has a nuclear engineer PhD from the Technical University Catalonia (UPC). He joined the Institute of energy technologies (INTE) of the UPC in 1992, working in the research of radionuclide metrology and instrument development and, becoming the INTE Director in December 2021. Currently, he is in charge of the environmental radioactivity subgroup included in the research group "Dosimetry and Medical Radiation Physics", part of the "Environmental dosimetry" Working Group 3 of the European Radiation Dosimetry Group (EURADOS). From February 2015, he has been the elected Chairperson of WG3. At the beginning of his research career, Dr. Vargas studied the radiological risk occurred as a result of inhaling the radon progeny. At this stage, he designed and set up equipment for the measurement of radon gas and the characterization of radioactive aerosol particles arising from its disintegration. Furthermore, he designed and set up the radon chamber at the UPC. Additionally, Dr Vargas has carried out research in the use of unmanned aerial systems (UAS) for radiological emergency scenarios and has been involved in the European project "Metrology for mobile detection ionising radiation following a nuclear or radiological incident – preparedness". At present, he is working in the European remoteAlpha project "Remote and real-time optical detection of alpha-emitting radionuclides in the environment"

Iran Now Has Enough Fissile Material for One Nuclear Bomb: IAEA

Source: https://www.homelandsecuritynewswire.com/dr20220531-iran-now-has-enough-fissile-material-for-one-nuclear-bomb-iaea

May 31 – Iran has enriched enough uranium for making one Hiroshima-size nuclear bomb, the International Atomic Energy Agency (IAEA) said in its quarterly report. The report was viewed by several media outlets Monday, among them the *Wall Street Journal*, Reuters, and Agence France-Presse.
The IAEA says that Iran now has around 43 kilograms (95 pounds) of uranium enriched to 60 percent (in March, Iran had 33 kilograms of uranium enriched to 60 percent).
The 43 kg of 60 percent enriched uranium would yield about 22-25 kg of uranium enriched to 90 percent, which is weapon-grade.
France24 reports that a separate IAEA report, also see by the news outlet, said Iranian officials have not given "technically credible" answers to questions regarding old nuclear material which was discovered at several military and scientific sites in Iran.
Iran's nuclear program was launched under the shah, but in 1992, now under the ayatollahs regime, the program was bolstered for the purpose of building nuclear weapons. Israel and the United States, relying on cyberattacks and covert action, attacked the Iranian nuclear weapons program and the scientists involved in it, but these attacks only caused delays on the margins of the program.
In 2015, Iran struck a deal with the United States, China, Russia and other world powers. The deal rolled back Iran's progress toward the bomb; imposed strict limits on various aspects of the country's nuclear development; and imposed an intrusive inspection regime to verify Iran's compliance with the deal.

In exchange, Iran received some of the money frozen in Western banks since the ayatollahs came to power in 19.
In May 2018, the Trump administration withdrew the United States from the deal, and imposed what it called a "maximum pressure" sanctions campaign on Iran.
Iran used the U.S. withdrawal from the 2015 deal, and the consequent weakening of the inspection regime, to ramp up its nuclear weapons-related activities: building thousands of advanced uranium enrichment centrifuges and moving them to fortified sites under ground; reopening the nuclear reactor in Araq, which will allow it to build nuclear weapons from plutonium; and continuing to improve its ballistic missiles.
The Biden administration has been trying to revive the 2015 nuclear deal, but the indirect talks between the United States and Iran have stalled.

EDITOR'S COMMENT: I have written many times that we will wake up one morning to read the announcement that Iran is a nuclear state. The good thing (for the time being) is that only one piece is not as threatening as two or more – although there is one target for one bomb... So, we still have some time. Some time for what?

Threshold Reached: Iranian Nuclear Breakout Timeline Now at Zero

By David Albright and Sarah Burkhard
Source: https://www.homelandsecuritynewswire.com/dr20220601-threshold-reached-iranian-nuclear-breakout-timeline-now-at-zero

June 01 – Iran has crossed a new, dangerous threshold: Iran's breakout timeline is now at zero. It has enough 60 percent enriched uranium, or highly enriched uranium (HEU), to be assured it could fashion a nuclear explosive.[1] If Iran wanted to further enrich its 60 percent HEU up to weapon-grade HEU, or 90 percent, it could do so within a few weeks with only a few of its advanced centrifuge cascades.[2]
In parallel, within a month, it could produce enough weapon-grade uranium for a second nuclear explosive from its existing stock of near 20 percent low enriched uranium. Whether or not Iran enriches its HEU up to 90 percent, it can have enough HEU for two nuclear weapons within one month after starting breakout.
Within 1.5 months after starting breakout, it could accumulate enough for a third nuclear weapon, using its remaining near 20 percent enriched uranium and some of its 4.5 percent enriched uranium. In 2.75 months after starting breakout, it could have a fourth quantity by further enriching 4.5 percent enriched uranium up to 90 percent. At six months, it could have produced a fifth quantity by further enriching both 4.5 percent enriched uranium and natural uranium. The accumulation for a sixth would take several months longer.
When Iran ended its crash nuclear weapons program in 2003, its biggest bottleneck was its lack of weapon-grade uranium, needing at least a few more years to accumulate enough weapon-grade uranium for a nuclear weapon.[3] Under intense international pressure, it decided in 2003 to downsize and better camouflage its nuclear weapons effort, while pushing to establish a robust capability to enrich uranium. Today, that decision has borne fruit. While it could only yearn for enough nuclear explosive material for five nuclear weapons in 2003, today it can have enough for those five weapons in six months. With its residual and covert nuclear weaponization capabilities, it could test a nuclear explosive underground or deploy a crude nuclear weapon within several months, certainly within six months, and deploy nuclear weapons on ballistic missiles in a year or two.
As Iran has reached a zero breakout timeline, the International Atomic Energy Agency (IAEA) has issued a harsh judgement that Iran is violating its safeguards agreement under the Nuclear Non-Proliferation Treaty, judged as having undeclared nuclear materials and activities, related to past and possibly on-going nuclear weapons efforts. Iran moreover shows no sign of being willing to rectify these violations or provide assurance to the IAEA its nuclear weapons program has ended. In fact, Iran's answers to the IAEA are not only technically noncredible and lack support, but they are also haughty. Iran's actions have placed the international community in an extremely difficult position. Some argue for reentering a nuclear deal, even one weaker than the 2015 nuclear deal, because it will extend breakout timelines. But we now know that what Iran takes apart, it can put back together quickly. Even if Iran downsized its enrichment program, it could quickly reconstitute its capabilities, as seen by its actions from 2018 to present. A deal is also but a short-term fix — the 2015 accord permits the program's expansion in just a few years. And the IAEA's judgement renders any meaningful verification of such a deal impossible, even dangerous, sure to lead Iran to further violations and others to seek nuclear weapons. It is time to recognize that only the toughest type of pressure, akin to that on Russia today, is going to convince Iran not to build nuclear weapons.

References

1. According to the International Atomic Energy Agency (IAEA), Iran has 43.1 kg of 60 percent enriched uranium (uranium mass) in the form of uranium hexafluoride, slightly more than a significant quantity, which the IAEA defines as the "approximate amount of nuclear material for which the possibility of manufacturing a nuclear explosive cannot be excluded."

2. For background, see David Albright and Sarah Burkhard, "Entering Dangerous, Uncharted Waters: Iran's 60 Percent Highly Enriched Uranium," April 11, 2022, https://isis-online.org/isis-reports/detail/entering-uncharted-waters-irans-60-percent-highly-enriched-uranium The Institute's breakout calculator is used to estimate a credible, worst-case breakout times, as in previous reports. The methodology is described in earlier Institute reports.

3. David Albright with Sarah Burkhard and the Good ISIS Team, *Iran's Perilous Pursuit of Nuclear Weapons* (Washington, DC: Institute for Science and International Security Press, 2021)

David Albright is President and Founder of, and **Sarah Burkhard** is Research Associate at, the *Institute for Science and International Security*.

Iran's Current Nuclear-Weapons Status: The Facts

Source: https://www.homelandsecuritynewswire.com/dr20220601-iran-s-current-nuclearweapons-status-the-facts

June 01 – A report published in April by the Institute for Science and International Security, titled Entering Dangerous, Uncharted Waters: Iran's 60 Percent Highly Enriched Uranium, and an interview with the *Jerusalem Post* by David Albright, the report's co-author, offer startling, and disturbing, insights into the rapid, and likely irreversible, progress Iran has made toward developing a workable nuclear weapon since the Trump administration, in 2018, decided to withdraw from the 2015 nuclear deal.

Here are the main points (the direct quotes from the report are indicated by "R"; the quotes from Albright's interview with the *Jerusalem Post* are indicated by "A/JP"; comments from the *Post*'s writer are indicated by "JP"):

- JP: Iran could have four "crude" nuclear bombs, or "devices," within three months if it decides to cross the nuclear threshold.
- R: "[Iran] has enough 60% enriched uranium or highly enriched uranium (HEU) to be assured it could fashion a nuclear explosive… within a few weeks, with only a few of its advanced centrifuge cascades."
- R: "In parallel, within a month, Iran] could produce enough weapons-grade uranium for a second nuclear explosive from its existing stock of near 20% low enriched uranium. Within 1.5 months after starting breakout, it could accumulate enough for a third nuclear weapon, using its remaining near 20% enriched uranium and some of its 4.5% enriched uranium."
- R: Within "2.75 months after starting breakout, it could have a fourth quantity by further enriching 4.5% enriched uranium up to 90%. At six months, it could have produced a fifth quantity by further enriching both 4.5% enriched uranium and natural uranium. The accumulation for a sixth would take several months longer."
- JP: Israeli intelligence and nuclear experts have said that Iran would need another six months to two years to perfect methods for detonation, warhead miniaturization, missile reentry
- A/JP: It is "A common fallacy is that Iran would require 90% HEU, more commonly called weapons-grade uranium, to build nuclear explosives."
- A/JP: Lower levels of enriched uranium were used in nuclear weapons designs by the US in the 1940s as well as by South Africa. Little Boy, the nuclear bomb dropped on Hiroshima, mixed the highest level of enriched uranium with some uranium enriched to as low as 50%.
- A/JP: 60%-enriched devices require a greater amount of high explosives to initiate the detonation process. "At the least, a device made from 60% HEU would be suitable for underground nuclear testing or delivery by a crude delivery system."

Argon Radsim Source App Launch

Source: https://www.argonelectronics.com/radsim-source-app-gamma-radiation-simulators

Argon Electronics has launched the Radsim Source App for the GS series simulation Gamma sources.

When planning a radiological exercise, it is common practice to represent a specific source activity level. Alternatively, the instructor may wish students to detect a particular reading at a known distance from the source that works perfectly within the constraints of the training environment, planned scenario, or exercise area

The Radsim Source App enables detection of a particular reading by hosting customisable simulated activity settings for Argon GS Series simulation Gamma sources.

This easy-to-use App enables the user to:

- Select units of measurement for simulated activity, dose rate, and distances
- Decide upon and set your simulated activity level
- Set the desired reading for the student to experience at a specific distance. This should be in an unobstructed line of sight from the source; the App will then automatically calculate and set the required activity level

Once the simulated activity levels are set, the simulation source remembers them, even when the device is switched off. Settings only need to be reprogrammed if the user's requirements change. Simulation sources can all be set to the same configuration, or they can be set differently.
The App can be used to configure the nine pre-set simulated activity levels for the GS4 series simulation gamma sources.

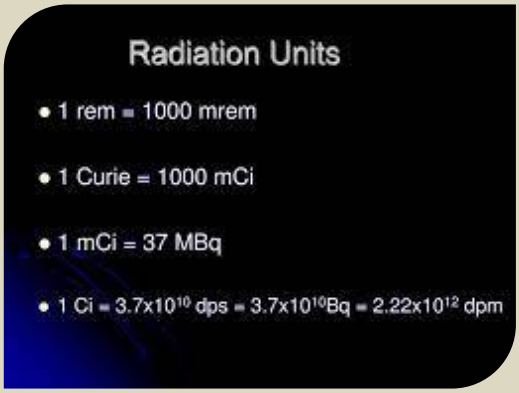
Neutron capability
For exercises that need to simulate Neutron activity to generate readings on the appropriate simulators, the App enables the desired activity or count rate to be set based upon distance from the simulation source – Ideal for use with our HRM simulator

●▶ Download the Radsim Source App product sheet

Apples & Oranges - Understanding Curies & REM in Radiation Sources

By Jeffrey D. Williams
Source: https://domprep.com/preparedness/apples-oranges-understanding-curies-rem-in-radiation-sources/

June 08 – Hazardous materials personnel are faced with a broad range of chemical, biological, and radiological hazards. However, not all hazards are equal, nor are similar quantities. Responders who encounter radiological materials need to know the relationship of quantity and biological impact of specific materials by first understanding the terminology of measurement units.
The world of the hazardous material responder has changed substantially in the past two decades. Past responses tended to be for accidental releases or misplaced sources, whereas recent events have shown a growing capability for intentional releases with political or terrorist motivations. These events – whether involving a vehicle-borne improvised explosive device, the release of hazardous chemicals, or the dispersal of biological agents – have increased the need for all emergency responders and preparedness professionals to expand their skills and scope of actions. This is particularly true for radiological terrorism, which fortunately has not had a real-world event to date.



With the increasing variety of chemical, biological, radiological, nuclear, and high-yield explosive threats comes the need to understand and become comfortable with the specialized terms of each threat scenario. One of the challenges in discussing radiological sources and their impacts is in understanding the size and threat from a source or an event. Two different ways of looking at hazards are: (a) in the quantity of material involved; and (b) in the biological impact of that material.
The first involves understanding the term "curies," whereas the latter involves understanding the term "rem," which is an acronym for roentgen equivalent man. Although both describe an aspect of the scale of an event, the terms relate to different aspects of a source and are not equivalent to each other.

Measuring Quantities of Radiological Material
The unit for measuring the amount, or activity, of radioactive material is the curie (or the becquerel in the International System of Units [SI]). The act of a single atom undergoing decay and changing to another element is one disintegration. Once that particular decay has occurred, an atom that has changed into another isotope or another element will not undergo that same process again, although the new isotope or element may have its own decay process. A curie is defined as 3.7 x 1010 disintegrations per second (dps); the definition of becquerel is 1 dps.
Although curies and becquerels measure the same event, they are obviously significantly different in scale. The practical consequence of this is that small millicurie sources are gigabecquerel sources, whereas curie-sized sources are terabecqueral or petabecquerel sources. This terminology can present problems with the public, and even responders, as these prefixes are not part of traditional experiences in scale. There can even be a psychological impact in these numbers, with a perception that the large prefix represents an inordinate hazard.
A major issue with the measurement of radioactive material is that knowing the quantity does not indicate the level of hazard it represents. Although the term expresses the rate of emissions, it does not factor in the type of radiation (alpha, beta, gamma, or neutron) being emitted – the type of radiation is highly significant in defining the level and scope of hazard of an isotope – nor does it reflect the energetic strength of the radiation. There are critical parameters because a 100-curie (intact) source of alpha-emitting Americium represents a minimal external hazard and can be closely

approached with no risk or harm, whereas a 100-curie Cobalt-60 source, which is a high-energy gamma emitter, would require a safe standoff distance of several hundred feet.

Understanding Biological Terms of Radiological Material

Curies describe a source's strength in terms of the rate of decay of a source; describing the strength in terms of the impact of that radiation on a human body is the dose. There are three terms that are frequently, if inaccurately, used interchangeably: (a) the roentgen; (b) the rad; and (c) the rem. The terms are distinct and refer to three noticeably different measurements, a distinction frequently lost in the semantics of the terms.

The roentgen, which is a measure of exposure to radiation, is a measure of the amount of energy deposited in a volume of air that results in the production of a specific rate of ionization. Exposure in this sense is not the same as the common usage of the term ("I've been exposed to chlorine gas"). However, it does convey some of the same sense of having been in contact with the radiation, even if not in contact with the source itself. The term "rad" is used to define a dose, and stands for radiation-absorbed dose. It represents the amount of energy deposited and absorbed by a body (the SI unit is a gray [Gy] and 100 rad =1 Gy). The amount of energy deposited does not depend on either the type of the radiation or the energy of the radiation, just on the energy per mass absorbed.

Although rad does not depend on the type of radiation deposited on a body, the impact of that energy on a biological unit is dependent on the type of radiation. The rem is a dose equivalent and accounts for the difference in biological impacts based on particle size (the SI equivalent is sievert [Sv], where 100 rem = 1 Sv). The larger particles of alpha and neutron radiation do greater damage at the point of impact because their energy is deposited in a small space. The lighter beta particle or the energy-only gamma have a more linear energy deposition form, allowing energy to be deposited over a greater volume and, therefore, with less intensity. A quality factor allows the conversion of rad to rem by accounting for the type of radiation and the differing effects. As an example, a 10 rad dose of gamma results in a 10 rem of exposure, and a 10 rad dose of alpha results in 200 rem of exposure.

There is a further complexity in defining the impact of radiation on the human body. Although ad and rem account for the radiation type and the doe equivalent respectively, both assume and external whole-body impact from intact, external sources. Yet, in both medicine and accidental releases, radiation can enter the body by different pathways and can have significantly different impacts on different tissue systems. This is the effective does and accounts for biological uptake, organ selectivity, etc. Regardless of radiation energy or type, internal exposure is always worse than external exposure due to the sensitivity of the tissues involved.

It is clear that describing source strength in terms of curies or rem provides two very different descriptions looking at very different aspects. It also is clear that, for both terms, that number by itself does not provide a full picture of the hazard presented by the source. The type of radiation and its energy level affect the usefulness of both terms. In understanding radiation measurement, no single term or aspect gives a full picture of the hazard, so the more information available, the better the opportunity to correctly evaluate the hazard for the scene.

Jeffrey Williams has served over the last 20 years as an environmental engineer in the U.S. Department of Defense. He also has served on two different emergency response teams, during which assignments he became an expert on radiological dispersal devices and various related topics. He has been a speaker at a number of public and private forums on topics ranging from environmental regulations to radiological preparedness. Prior to assuming his DoD post, he worked on the design and construction of hazardous-waste disposal sites for industrial facilities. He holds a Bachelor's degree in Nuclear Engineering and a Master's degree in Environmental Engineering from the University of Maryland as well as a Master's degree in Legal Studies from the University of Baltimore. He also has studied at the Massachusetts Institute of Technology's Center for Advanced Engineering Studies.

Protecting Nuclear Waste Containers from Metal-Corroding Microbes

Source: https://www.homelandsecuritynewswire.com/dr20220608-protecting-nuclear-waste-containers-from-metalcorroding-microbes

June 08 – With Canada getting closer to moving all its spent nuclear fuel to a single facility, and encasing each fuel container in bentonite clay, researchers are studying whether that clay could support microbial life – which could eat away at the metal containers.

"I've found that microbial life always surprises us," says Myrna Simpson, one of the researchers and a professor in University of Toronto Scarborough's department of physical and environmental sciences. "Microbes will grow in the strangest places."

The proposed storage facility, called a deep geological repository (DGR), would sit 500 to 800 metres underground in one of two Ontario sites. Every room storing nuclear waste will

be packed and sealed with bentonite clay, a swelling material that helps dissipate heat and reduces water movement when packed tightly.
But the clay is mined from a natural deposit in Wyoming and will inevitably arrive embedded with tiny bits of organic matter. Microbes will also be in the clay and rock surrounding the facility, and in groundwater that may pass through it. Some of that microbial life may produce sulfide, a chemical compound that could lead to corrosion of the metal containers holding the used fuel.
To test if the microbes can grow, the group building Canada's DGR, the Nuclear Waste Management Organization (NWMO), brought together Simpson and professors Josh Neufeld and Greg Slater from the University of Waterloo and McMaster University, respectively. Their five-year study was recently awarded $2.8 million in funding from the new NSERC Alliance grant program.
"My lab has the capability to study the organic matter chemistry, but what does that mean in terms of the microbiology?" says Simpson. "By combining forces with professors Neufeld and Slater, we can put results together in a holistic manner."
The team will study samples of groundwater and surrounding rock at the two proposed sites for the DGR, near Ignace in northern Ontario and in southwestern Ontario's South Bruce area. Their results will add to a data set that will help the NWMO decide on a location, along with other aspects of the project.
"If we find conditions that promote microbial growth, then this information can be factored into the DGR's design to minimize potential risks," Simpson says.

Researchers to Replicate Conditions Deep Underground

Canada has about three million bundles of used nuclear fuel, which contain the solid uranium that powers nuclear reactors. They're stored in above-ground containers at seven facilities across the country, with 90,000 added every year. The containers only last about 50 to 100 years, but used nuclear fuel must be stored for one million years before its radiation levels return to that of naturally occurring uranium ore. For Canada – and almost every country that commercially produces nuclear power – the solution is a DGR.
A DGR is a network of tunnels that connect rooms of used nuclear fuel. Canada plans to place every fuel bundle in a specialized metal container, which will then be encased in a box of highly compacted bentonite clay. Boxes will be stacked one wide and two high, then all empty spaces in the room will be packed with clay and sealed with a wall of it.
"The microbes are going to drive the chemistry," Simpson says. "If the chemistry changes, then you have an entirely different scenario in terms of stability. This is something we will test collaboratively."
The research team is being led by Neufeld, who will study the ways bentonite clay can support microbial life. Slater will complement his research with insights into microbes that might become active. Meanwhile, Simpson will study how organic matter found in the clay and DGR may react to microbial life.
Though their research can't fully simulate being 500 meters underground, Simpson says most conditions of the DGR can be replicated in the lab or studied in equivalent geological settings. The team can simulate how the clay is packed, density, temperature, salt content of the groundwater and other conditions of the facility.
"Working with professors Neufeld and Slater will yield new and integrated knowledge regarding how microbes can grow and co-operate underground, and what conditions prevent their activities," Simpson says. "This partnership has many benefits and I'm excited to be a part of this team."

Global nuclear arsenal set to grow for first time in decades

Source: https://www.theguardian.com/world/2022/jun/13/global-nuclear-arsenal-set-to-grow-for-first-time-in-decades

June 13 – The global nuclear arsenal is expected to grow in the coming years for the first time since the cold war, and the risk of such weapons being used is the greatest in decades, a leading conflict and armaments thinktank says.
Russia's invasion of Ukraine and western support for Kyiv has heightened tensions among the world's nine nuclear-armed states, the Stockholm International Peace Research Institute (Sipri) thinktank said on Monday in a new set of research.
While the number of nuclear weapons fell slightly between January 2021 and January 2022, Sipri said that unless immediate action was taken by the nuclear powers, global inventories of warheads could soon begin rising for the first time in decades.
"All of the nuclear-armed states are increasing or upgrading their arsenals and most are sharpening nuclear rhetoric and the role nuclear weapons play in their military strategies," Wilfred Wan, the director of Sipri's weapons of mass destruction program, said in the thinktank's 2022 yearbook. "This is a very worrying trend."
Three days after Moscow's invasion of Ukraine, which the Kremlin calls a "special military operation", President Vladimir Putin put Russia's nuclear deterrent on high alert. He has also warned of consequences that would be "such as you have never seen in your entire history" for countries that stood in Russia's way.

Russia has the world's biggest nuclear arsenal with a total of 5,977 warheads, 550 more than the United States. The two countries possess more than 90% of the world's warheads, though Sipri said China was in the middle of an expansion with more than 300 new missile silos according to the latest estimate.
Sipri said the global number of nuclear warheads fell from 13,080 in January 2021 to 12,705 in January 2022. An estimated 3,732 warheads were deployed with missiles and aircraft, and around 2,000 – nearly all belonging to Russia or the US – were kept in a state of high readiness.
"Relations between the world's great powers have deteriorated further at a time when humanity and the planet face an array of profound and pressing common challenges that can only be addressed by international cooperation," Sipri board chairman and former Swedish prime minister Stefan Lofven said.

EDITOR'S COMMENT: I was always wondering how many nuclear warheads are necessary to destroy a county? 10, 100, 500, 1000? So, why 5,000 or 6,000? Interested to destroy the entire planet as well?

HazMat Training Equipment: 10 Effective Tools To Consider

By Steven Pike
Source: https://www.argonelectronics.com/blog/hazmat-training-equipment-10-effective-tools-to-consider

May 30 – There is a great deal to choose from when sourcing HazMat training equipment. While this seems like it can be beneficial for instructors and team leaders, ultimately it can be challenging and confusing to wade through all of the options available.
With that in mind, we've narrowed down ten HazMat training products which will not only benefit your students, but also deliver significant returns on investment.

1. AccuRad PRD Simulator
We used our simulation training expertise to accurately emulate the look and feel of Mirion's real detector. In fact, our user interface components, including front and top displays, indicators, sounder, and vibrator are exactly the same as the actual detectors, we even incorporated the radar mode and wireless interfaces.
Our AccuRad-SIM responds to Radsim electromagnetic sources that safely simulate ionising radiation. This effectively eliminates regulatory, environmental, and health and safety concerns for you and your students. It also opens up the ability to use the simulation sources anywhere, in the open or within buildings.

2. RadEye GF-10
Our relationship with ThermoFisher, combined with our own simulation experience, has led to the development of the RadEye series of training simulators which are extremely close to that of the actual detectors.
Like the AccuRad, the RadEye GF-10 SIM responds to Radsim electromagnetic sources that safely simulate ionising radiation. The simulator enables you to create scenarios with highly realistic simulation of the shielding effects of different materials. Its configurable menu settings allow you to work with inverse square law, dose, and dose rate alarm settings. It allows for consistent, repeatable performance, wherever and whenever you want.

3. HRM
Working with Sensor Technology Engineering, we've developed an HRM series of training simulators which allow you to practise radiation detection including neutrons without the use of dangerous radiological materials.
The HRM-SIM replicates the self-contained gamma-ray and thermo neutron radiation detector for use in the interdiction and localization of nuclear materials. It is so realistic that students can practise the effect of user body shielding to determine source position, enabling you to ensure that in emergency situations, survey teams have experience with this important concept.

4. ADM-300 SIM
If you're looking to train for Canberra/Mirion ADM 300-series radiological survey missions, you'll definitely want to consider the ADM-300 SIM. Your team will have access to a detector with the same look and feel as the real thing, without the need to involve any ionising radiological sources.

It responds to safe simulation Gamma and Beta contamination sources and can be used to demonstrate effective shielding with different materials, including (but not limited to) glass, wood, and concrete. For larger scenarios, the ADM-300 SIM is compatible with our wide-area PlumeSIM real experience training system.
Alongside ADM300A-SIMs' ability to simulate both GM detectors, safe simulation Beta sources can be used to simulate contaminated PPE. Our decontamination controller then allows you to simulate the effect of both partial and full decontamination.

5. RDS100/PDR77/CDV718 Safety Training Probes

Used with your own meter, this Alpha, Beta and Beta Gamma 3-Probe simulator set is a training system that enables your students to experience the operational features of real Mirion / Canberra probes, without the associated radioactive materials or regulatory constraints.
This kit comprises three simulation probes for use with the real RDS100/PDR77 and CDV 718 meters:

- BG-SIM-P for training in the use of the Beta Gamma Probe
- A-SIM-P for practising Alpha contamination monitoring.
- B-SIM-P to practise Beta contamination monitoring.

This simulation probe kit allows you to safely teach critical search, reconnaissance, sentry, survey and decontamination skills, alongside the practical understandings of shielding and inverse square law.

6. UDR13/14 Simulators

Our collaboration with Mirion/Canberra has resulted in a high fidelity radiological dosimeter simulator which incorporates the menu structure and software processing of an actual UDR series dosimeter. The UDR 13/14 simulators maintain all detector functionality, permitting dose management training without the need for a real radiological source.

7. RADSIM 44-9-SIM Radiation Safety Training Probe Simulator

Instructors looking to train with contamination monitoring with Ludlum's 44-9 GM pancake-type detector should consider the RADSIM 44-9-SIM. This versatile simulator detection probe enables your students to experience Ludlum 44-9 GM's operational features without the need for real radioactive materials or sources. It responds to safe magnetic sources that simulate short range alpha or beta radiation, opening up to the possibility of training in a wider variety of locations, including within public buildings. Instructors can safely and effectively teach survey/location and decontamination skills when and where they want. Additionally, an instructor remote controller is provided in order to simulate the effects of partial or complete decontamination, or to simulate probe failure.

8. LCD 3.3 JCAD Chemical Hazard Detection Simulator

If you're looking to train with Smiths Detection LCD3.3 and LCD3.3FR, (known as M4A1 JCAD within the US Military), Argon's LCD 3.3-SIM may be right for you. This tool is ideal for HazMat simulation training exercises, with the same menu structure as the actual detector (including certain language options), and cumulative dose and dose alarms.
Additional features include the realistic effect of wind direction and temperature. It also simulates depletion of sieve packs and batteries, and user changeover of sieve packs. This tool not only simulates the real detector, but it also monitors and reports correct use of the instrument.

9. AP4C Chemical Hazard Detection Simulator

The AP4C-SIM detector simulator, built for training for the Proengin AP4C,
responds to safe electronic sources that simulate chemical vapours and toxic industrial substances. With this simulator, you can avoid using simulants which can harm the environment, detectors, and health, while still building practical knowledge of HazMat response. Furthermore, Argon's powerful simulation hazard platform enables you to replicate orthogonal detection based upon flame photometry and ion mobility spectrometry.
AP4C-SIM simulates response to all substance channels, including explosive atmosphere, and responds to electronic environmentally friendly simulation sources. The low cost of ownership – no preventative maintenance, regular calibration, or consumables are required – makes this a strong return on investment for any HazMat instructor looking to train with the Proengin AP4C.

10. MultiGAS-SIM Simulator

This innovative approach to implementing Multigas training operates on an Android smart device, which is attached to the MultiGAS-SIM interface module. A bluetooth connection between the Android mobile and MultiGAS-SIM interface allows the device to respond to independently deployed Long Range Vapour Source (LRVS) simulation gas emitters.

The LRVS simulation gas emitters are easy to use and programmable to represent a wide variety of hazardous substances and scenarios, most notably the depletion of oxygen measured by the O2 sensor.

These training tools can significantly improve CBRN and HazMat training learning outcomes. The ability to ensure Real Experience Training wherever and whenever needed with realistic measurements is extremely valuable for most training scenarios.

Argon's simulators are constantly evolving and we are always creating new ranges of learning technology which can help responders achieve Real Experience Training.

To learn more about HazMat training, including an overview of definitions, download our Guide to HazMat Definitions, Regulations, Risks, and Scenarios.

IAEA - Manual for First Responders to a Radiological Emergency

Source: https://www.iaea.org/publications/7606/manual-for-first-responders-to-a-radiological-emergency

The aim of this publication is to provide practical guidance for the first responders who will respond during the first few hours to a radiological emergency and for the national officials who would support this early response. This publication provides guidance in the form of action guides, instructions and data that can be easily applied by a State to build a basic capability to respond to a radiological emergency.

Related publications

2022 Emergency Preparedness and Response Information Management System (EPRIMS)

2022 Arrangements for the Termination of a Nuclear or Radiological Emergency

2022 Preparedness and Response for a Nuclear or Radiological Emergency Involving the Transport of Radioactive Material

2021 Considerations in the Development of a Protection Strategy for a Nuclear or Radiological Emergency

2020 Arrangements for Public Communication in Preparedness and Response for a Nuclear or Radiological Emergency

2020 Pocket Guide for Medical Physicists Supporting Response to a Nuclear or Radiological Emergency

… and more!

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

EXPLOSIVE NEWS

Mobius report – Female BLA Suicide Bomber Targets Chinese University Staff, Karachi, Pakistan

Source: https://terrogence-global.com/2022/06/mobius-report-female-bla-suicide-bomber-targets-chinese-university-staff-karachi-pakistan/

On April 26, 2022, a female suicide bomber initiated her vest PBIED near the entrance gate of the Institute for Chinese Studies at Karachi University, in southern Pakistan. The blast occurred as a minibus transporting a number of Chinese university staff, including the director of the institute, passed by the bomber's location en route to the university, accompanied by a security detail of Pakistani Rangers on motorcycles. The blast claimed the lives of the occupants of the minibus – three Chinese citizens and the Pakistani driver – and injured several others. Later that day, the Baloch Liberation Army issued a statement of responsibility, stating the purpose of the attack was to harm Chinese interests in the country, and also revealed the identity of the perpetrator – according to the organization, the first woman to carry out a suicide bombing on its behalf. The incident received substantial media coverage in Pakistan and around the world, and highlighted the work of the BLA's Suicide Squad, which seems to be focused on carrying out high-quality operations against key interests of the Pakistani government, an important element of which is Chinese intervention in the country.

The women-extremism nexus

Source: https://www.pakistantoday.com.pk/2022/06/08/the-women-extremism-nexus/

June 09 – The recent incident of terror committed by woman at Karachi University is not unprecedented. Multiple cases of similar acts have been witnessed in Pakistan's history involving women participants. If we try to delve into the historical records, we will find a long list of attacks primarily committed by women extremists. It shows that women have always been at the cutting edge either by facilitating or by actively involving themselves in such criminal behaviour.

But the dilemma here in Pakistan is that the security organizations have overlooked the role played by women in such violent and extremist initiatives by considering them anomalous while focusing solely on male radicals. In this way they are paving the way for this kind of behavior to become a norm.
Closer examination of the matter suggests that on one hand women's radicalization turns out to be beneficial to the recruiting organizations. While on the other hand women perceive it as a panacea to the multidimensional sufferings they face under the prevailing socio-political order.
The most effective and long-lasting benefit terrorist organizations may get out of women recruits is their role as socializing agents for their children and other family members by instilling in them the spirit and passion required by the terrorist organizations to substantiate their agenda. Young and innocent minds are injected with poisonous and hateful ideologies against the state or system which these rebel's counter. And this process starts from childhood when young minds are delicate and could easily be moulded.
It is also worth acknowledgement that women are relatively less likely to be susceptible of being caught by the security officials while they are in the process of suicide bombing or any other such act, which brings a considerable benefit to the extremist organizations at a relatively lower cost. This is particularly true in the case of Pakistani society owing to its respect for Islamic dress like burqa which goes unchecked by the security officials. Owing to these and other benefits conferred from the part of women terrorist organizations are motivated to recruit them as participants.
Participation of women in these organizations could partly be attributed to the society's denial of empowerment which ends up in releasing the heat of anger through violent behaviour. This view is also shared by the prominent researcher in the field of terrorism, D. Mia Bloom, in her famous book *Bombshell: Women and Terrorism*. According to her, terrorism is the tool of the oppressed against the powerful for their sufferings.
A fnother widely held belief is that the increasing involvement of women in extremist organizations is largely because of their intent to take revenge in case they have witnessed the murder or other suffering of their beloved ones, including parents and other close relatives.
But the current scenario is depicting neither of the above narratives in that, a multitude of such cases witnessed today assert that most of the violent acts are committed by women who are highly educated and who have no record of marginalization and poor treatment. Neither have their family members been killed or tortured in the hands of state or security officials. This trend could partly be attributed to the notion that these women were inspired from the ideologies of the extremist organizations, started following them and went to the extent of sacrificing their own lives as well as other people around them. The recent incident at Karachi University provides a good example where an educated woman, pursuing an MPhil degree, and having a normal lifestyle, blew herself up along with four other innocent people.
A similar incident was witnessed in 2015 in Lahore where a woman named Noreen Laghari was arrested prior to her suicide attack attempt. She was found to be a follower of the violent extremist organization, Daulat e Islamia. Noreen Laghari was pursuing her MBBS and belonged to an educated family, her father being a professor at a well-known university.
The departure of Bushra Cheema with her four children to Syria to join ISIS in 2016 is not hidden from anyone where she was manipulated in the name of religion. There are a lot of such women like Bushra who could easily be susceptible to such tactics driven by terrorist groups.
It is a very demanding task to instill in such mature minds a counter-narrative and motivate them to substantiate it. So, the conundrum that how terrorists carry out the skillful management of educated minds is still waiting to be solved.

Lebanon's Minefields | Clearing the hidden remnants of war | UN Story

Source [+video]: https://videos.un.org/en/2022/06/15/lebanons-minefields-clearing-the-hidden-remnants-of-war-un-story/

June 15 – Zeina Saleh is a young Lebanese woman working in mine clearance and explosive ordnance disposal (EOD) in southern Lebanon.
Women working in the field of demining are rare. Zeina Saleh is amongst those very few women working under extremely risky conditions to realize her vision of a mine-free Lebanon. Zeina's works to allow the safe passage of UN peacekeepers along the blue-line, contributing to development and peace in her country.
Zeina also helps raise awareness about the impacts and dangers of landmines, and conducts trainings on Explosive Remnants of War (ERWs) and Improvised Explosive Devices (IEDs) for UN personnel in Lebanon.

In November 2019, Zeina, along with six other young women working for the United Nations Mine Action Service, received the UN Secretary-General Award for addressing the gender imbalance in the field of explosive ordnance disposal (EOD).

Some 160,000 square km of territory of Ukraine require mine clearance operations

Source: https://ua.interfax.com.ua/news/general/839602.html

June 16 – Around 160,000 square kilometers of the territory of Ukraine need to be examined for the presence of explosives, Deputy Defense Minister of Ukraine Hanna Maliar has said.
"Some 160,000 square kilometers of the territory of Ukraine today need to be examined for the presence of explosives. A national agency for mine clearance operations has been set up under the chairmanship of the defense ministry of Ukraine. It is already operating and coordinating communication between all government agencies and international mine clearance organizations," Maliar told a press briefing hosted by the Ukraine media center in Kyiv on Thursday.
She emphasized that the area of 160,000 square kilometers entails the status of one of the most polluted countries in the world.
"Ukraine hopes for further assistance of Geneva International Centre for Humanitarian Demining," Maliar said.

Landmines still a threat to more than a million Cambodians

Source: https://www.khmertimeskh.com/1094384/landmines-still-a-threat-to-more-than-a-million-cambodians/

June 15 – More than one million people still live in fear and work in areas contaminated by landmines, ERW and other UXOs while financial support is needed so that the country can reach its mine-free goal by 2025, a senior official said.
Ly Thuch, first vice-president of Cambodian Mine Action and Victims Assistance Authority, said yesterday that despite prevailing peace, people still live in fear and work in such contaminated areas.
Thuch's remark was made yesterday at the Regional Workshop on Residual Risk Management Frameworks for Southeast Asia held in Phnom Penh to draw information out of the experienced presenters and to share the participants' thoughts and experiences on residual risk management.
Participants included officials from Vietnam, Laos and Thailand and the workshop, which ends tomorrow, touched on residual contamination and reasonable effort in land release.
Thuch said that thanks to Prime Minister Hun Sen's win-win policy, the country has enjoyed peace since 1998 when the Khmer Rouge soldiers were reintegrated into the government. However, the people are facing landmines and ERW threats on contaminated land.
"For the last 30 years with international donors' support and our heroes in the national and international organisations we were able to release roughly 2379 square kilometres of landmine/ERW contaminated land for productive purposes such as agriculture, resettlement, roads, schools, and other social infrastructure," he said.
"On this land, over 1.1 million anti-personnel mines, more than 26,000 anti-tank mines, and nearly three million explosive remnants of war including cluster munitions were found and destroyed, benefiting almost 7.5 million people," Thuch said.
Because of the clearance and explosive ordnance risk education, the number of annual casualties had been brought down from 4,320 cases in 1996 to 44 cases in 2021, he said.
"To meet our obligations to our people, we need to clear approximately 736 square kilometres of known mine contaminated land by 2025," he noted. "We are constantly looking at the risks and how we can manage it in the best way possible while having one main goal in our mind, the safety of every Cambodian."
"We improved and continue to improve our management information system, not only to collect data but to analyse what we are doing and improve our planning," he added.
The government declared Kep as the country's first mine-free province on February 28, and Prey Veng on May 12.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

CYBER NEWS

C2BRNE DIARY

Bad for Computer Security: Employees Returning to the Office

Source: https://www.homelandsecuritynewswire.com/dr20220525-bad-for-computer-security-employees-returning-to-the-office

May 25 – When employees feel they deserve superior technology compared to other employees—and they don't receive unrestricted access to it—they pose a security risk to their companies, according to a new University at Buffalo School of Management study.
Forthcoming in *MIS Quarterly,* the research explores 'technological entitlement,' a feeling some employees have that they are more deserving of high-tech resources, uses and privileges than their co-workers.
"When these exaggerated expectations of special status go unmet, entitled employees lash out in aggressive acts of misuse or abuse," says the study's lead author Laura Amo, PhD, assistant professor of management science and systems in the UB School of Management. "They have fewer qualms about breaking the rules because they consider themselves 'above' organizational restrictions on technology."
The researchers conducted three studies with independent samples totaling nearly 700 working adults. In the first study, they measured past computer abuse behavior and perceptions of restrictions on broad technology use. In the second and third studies, they modeled computer abuse intent by investigating restrictions on remote access and on personal- and company-owned technology at work.
Their findings show that technologically entitled employees pose a direct threat to the information security of organizations.
"If an average-sized company experienced a 10% increase in technologically entitled employees, it'd have to spend an extra $90,000 each year to mitigate that risk," says James Lemoine, PhD, associate professor of organization and human resources in the UB School of Management. "Proactive measures—such as user behavior analytics and employee training and awareness—can provide significant savings by reducing cyber risk."
Their findings also have implications for creating and implementing policy on employee technology use, and recommend involving technologically entitled employees in the process of policy-building to encourage buy-in.
"Organizations that work toward establishing fair policies will better mitigate security risks," says Emily Grijalva, PhD, associate professor of organization and human resources in the UB School of Management.
Tech entitlement also has implications for employees returning to the office—or being heavily monitored while working remotely—following the COVID-19 pandemic.
"These trends may be perceived as restrictions imposed by the organization, which could increase the security risk posed by technologically entitled employees," says Grijalva. "Businesses should carefully consider employee perceptions when deciding how to move forward with disabling or downgrading remote work options and implementing restrictions on remote workers."

Building a Cyber Force Is Even Harder Than You Thought

By Max Smeets

Source: https://warontherocks.com/2022/05/building-a-cyber-force-is-even-harder-than-you-thought/

May 12 – In the past decades, over 40 states have publicly established some sort of military cyber command, with at least a dozen more planning to do so. Yet despite this proliferation, there is still little appreciation of the sheer amount of time and resources that an effective cyber command requires.
In my book *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force*, I break down the challenges of building an effective cyber command into five categories I call the PETIO framework: people, exploits, toolset, infrastructure, and organizational structure. What does this mean for aspiring cyber powers? First, the most important element of developing an offensive cyber capability are the people — not just technically savvy ones but also linguists, analysts, front-office support, strategists, legal experts, and operation-specific consultants. Second, much attention has been paid states' deployment of zero-day, or unknown, exploits. However, known exploits and tools can also be highly effective if the attacker has a superior knowledge of their target and their capabilities. Third, infrastructure investments — such as establishing a cyber range for

training and testing — are an essential requirement to develop an offensive cyber capability and come at a great cost.

Technical People Aren't Enough

A widespread view in business management is that as the cognitive skills of a job increase, people — rather than technology — become more important. These "thought jobs," as Daniel Pink calls them, require greater problem-solving skills and creative thinking, which means that businesses can only be successful if they cultivate a culture that prioritizes the human element. For aspiring cyber powers, this is true for more than just technical experts.

Of course, a military cyber organization needs vulnerability analysts, or bug hunters. These employees search for software vulnerabilities. They also need developers, operators, testers, and system administrators to successfully execute an operation, and make sure capabilities are reliably developed, deployed, maintained, and tested.

But building an offensive cyber capability also requires a more comprehensive workforce. First, frontline assistance is required to support the activities of operators and developers. This can include activities such as registering accounts or buying capabilities from private companies. Second, a military or intelligence organization with the best cyber force in the world is bound to fail without strategic guidance. Operational or tactical success does not equal strategic victory. An operation may be perfectly executed and rely on flawless code, but this does not automatically lead to mission success. For example, U.S. Cyber Command may successfully wipe data off the server of an Iranian oil company without actually securing any change in Iranian foreign policy. An organization can only function if there is a clear understanding of how the available means will achieve the desired ends. An important task of strategists is to coordinate activities with other military units and partner states. They are also involved in selecting target packages, although a separate position is often created for "targeteers." The targeteers nominate targets, assess collateral damage, manage deconfliction, and help with the planning of the operational process.

Any military or civilian agency conducting cyber operations as part of a government with a legal framework will also deal with an army of lawyers. These legal experts will be involved in training, advising, and monitoring. Compliance with the law of war, the law of armed conflict, and any other legal mandates requires legal training operators, developers, and systems administrators to prevent violations. Legal experts provide planning support as they advise, review, and monitor operational plans. For example, in the planning of U.S. Cyber Command's 2016 Operation Glowing Symphony, which sought to disrupt and deny ISIL internet usage, these experts helped to specify the notification plan, mission checklist, and authorization process.

Embedding legal experts at the various stages of a cyber operation is hard. Indeed, it likely requires numerous critical conversations with the leadership and operational teams to ensure they sufficiently understand what is being proposed before they can give approval. Also, the way certain operations are executed makes legal vetting harder. For example, in the case of self-propagating malware like Stuxnet, once you commit, it is difficult to go back.

A diverse group of technical analysts is then needed to process information during and after operations. Non-technical analysts are essential, too, particularly for understanding how people in the target network will respond to a cyber operation. This requires analysts with specific knowledge about the country, culture, or target organization. There is also the need for remote personnel. As security researcher and former NSA employee Charlie Miller puts it, "Cyberwar is still aided by humans being[s] located around the world and performing covert actions." In the case of the Stuxnet attacks, for example, a Dutch mole, posing as a mechanic, helped the United States and Israel collect intelligence about Iranian nuclear centrifuges that was used to update and install the virus.

Finally, a cyber command needs administrators for human resourcing, liaising with other relevant domestic and international institutions, and speaking to the media. As Jamie Collier observes, "[G]one are the days when spy agencies did not officially exist" and kept "their personnel and activities guarded surreptitiously away from the public view." Communication can help to overcome public skepticism. This applies not just to intelligence agencies, but to some degree also to military cyber commands, especially when their mission set is expanding and concerns about escalation, norms deterioration, or allied friction are growing. In addition, being more public facing may help for recruitment purposes in a highly competitive job market.

It Is More Than Just About Zero-Days

The most talked about element of developing an offensive cyber capability are exploits. These fall into three difference categories: zero-day exploits, unpatched N-day exploits, and patched N-day exploits. A zero-day exploit is one that exposes a vulnerability not known to the vendor. An unpatched N-day exploit is one that exposes a vulnerability in software or hardware that is known to the vendor but does not have a patch in place to fix the flaw. A patched N-day exploit is one that exposes a vulnerability in software or hardware that is known to the vendor and has a patch in place to fix the flaw. Oftentimes, attackers must combine multiple vulnerabilities into a chain of attack, known as an exploit chain, to attack a given target.

Much policy attention is devoted to states' hoarding of zero-days. Jason Healey, a Senior Research Scholar at Columbia University's School for International and Public Affairs, conducted a study in 2016 to understand how many zero-day vulnerabilities the U.S. government retains. Healey states with high confidence that in 2015/2016 the U.S.

government retained "[n]ot hundreds or thousands per year but probably dozens." This largely corresponds with other reporting. More mature military and intelligence organizations benefit from carefully designed procedures to use their exploits as efficiently as possible.

We should not, however, exaggerate the importance of zero-days. "[P]eople think, the nation-states, they're running on this engine of zero days, you go out with your master skeleton key and unlock the door and you're in. It's not that," Rob Joyce, then-head of NSA's Office of Tailored Access Operations, said during a presentation at the Enigma Conference. He continued, "Take these big corporate networks, these large networks, any large network — I will tell you that persistence and focus will get you in, will achieve that exploitation without the zero days. There's so many more vectors that are easier, less risky, and quite often more productive than going down that route."

Indeed, for military cyber organizations in particular, the race for N-days is often as important. In deploy N-day exploits, attacks can take advantage of the time it takes to develop a patch and the time it takes to adopt a patch. The average delay in patching an exploit differs based the size of the vendor, the severity of vulnerability, and source of the disclosure. While it takes an average of just over a month for in-production web applications to patch "medium severe vulnerabilities," it takes vendors on average 150 days to patch vulnerabilities in supervisory control and data acquisition systems. Adopting the patch can also take a considerable amount of time — especially in environments that lack standardization, such as industrial control systems. Partially due to the long lead-time on industrial control-system patching, we have witnessed several prominent attacks against these devices and protocols. For example, in December 2016 a Kremlin-backed hacker group known as Sandworm used malware dubbed CrashOverride or Industroyer to turn large parts of Ukraine dark. To do this, the attackers bypassed the automated protected systems at a Ukrainian electrical transmission substation by using a known vulnerability in its Siemens SIPROTEC relays.

Testing and Infrastructure Matter

There is a widespread belief that launching cyber attacks is cheap while defending against them is expensive. But as Matthew Monte observed, based on his experience in the U.S. intelligence community, "Attackers do not stumble into being 'right once.' They put in the time and effort to build an infrastructure and then work through Thomas Edison's alleged '10,000 ways that won't work.'" This requires infrastructure, an absolutely crucial element of cyber capability that is not talked about enough. Infrastructure can be broadly defined as the processes, structures, and facilities needed to pull off an offensive cyber operation.

Infrastructure falls into two categories: control infrastructure and preparatory infrastructure. Control infrastructure refers to processes directly used to run an operation. These are generally burned down after a failed operation. This type of infrastructure can include domain names of phishing sites, leaked email addresses, or other abused technologies. It also includes command-and-control infrastructure used in remotely conducted operations that maintain communications with compromised systems within a target network. This infrastructure can be used, for example, to keep track of compromised systems, update malware, or exfiltrate data. Depending on the goal and resources of an operation, the command-and-control infrastructure can be as basic as a single server operating on the external network.

More mature actors, however, tend to use more complex infrastructure and techniques to remain stealthy and resilient against takedowns. For example, Russia-based Fancy Bear spent more than $95,000 on the infrastructure they used to target people involved in the 2016 U.S. presidential election. And this is often about far more than just renting infrastructure: An organization may run a whole set of operations just to compromise legitimate webservers to use them for running future operations.

Preparatory infrastructure concerns a set of processes that are used to put oneself in a state of readiness to conduct cyber operations. Rarely will an attacker throw away this infrastructure after a (failed) operation.

One of the most difficult things to do when crafting good attack tools is testing them before deployment. As Dan Geer, a prominent computer-security expert, points out, "Knowing what your tool will find, and how to cope with that, is surely harder than finding an exploitable flaw in and of itself." Much of the preparatory infrastructure for an attack usually consists of databases used in target mapping. An attacker will need to do a lot of work to find their targets. Network mapping exercises can help an organization understand the range of possible targets, sometimes also referred to as "target acquisition." Hence, the most mature actors in this space have invested enormous resources in network-mapping tools to identify and visualize devices on certain networks.

There are also other targeted databases. For example, GCHQ maintains a special database that stores details of computers used by engineers and system administrators who work in "network operation centers" across the world. The reason why engineers and system administrators are particularly interesting targets is because they manage networks and have access to large troves of data.

An illustrative, high-profile case is the hack of Belgacom, a partly state-owned Belgian phone and internet provider with the European Commission, the European Parliament, and the European Council as part of their customer base. The British spy agency GCHQ, possibly assisted by other Five-Eyes members, used malware it had developed to gain access to Belgacom's GRX routers. From there, it could undertake "Man in the Middle attacks," which made it possible to secretly intercept communications of targets roaming using smartphones. As reporters discovered, the

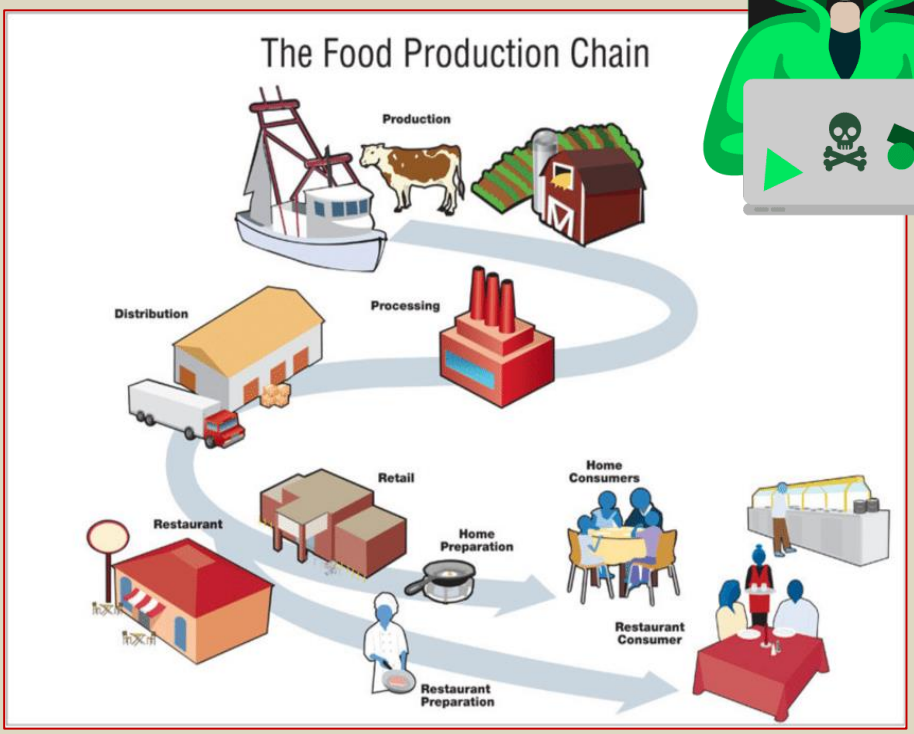
Belgacom Hack, code-named Operation Socialist, "occurred in stages between 2010 and 2011, each time penetrating deeper into Belgacom's systems, eventually compromising the very core of the company's networks."
Preparing for cyber attacks also requires creating a cyber range. This is a platform for the development and use of interactive simulation environments that can be used for training and capability development. In past years, businesses have increasingly invested in cyber ranges, based on cloud technology. These ranges are either developed on public cloud providers — such as Amazon Web Services, Microsoft Azure, or Google — or private cloud networks deployed on premises. Cloud cyber ranges generally provide flexible hands-on learning environments with convenient click-and-play scenarios for training. For military cyber organizations, however, the conventional non-cloud-based ranges are generally still preferable, given the need for highly customable simulation environments and bespoke operational testing and training.
In trying to keep up with the fast pace of developments in cyber conflict, much expert commentary has focused on whether cyber effect operations can produce strategic advantages or be influenced by norms. Yet, we first need to address a more fundamental question: When are states actually able to conduct operations in the first place? While the proliferation of military cyber commands suggests major change is afoot in cyber warfare, making these organizations work remains much harder and more expensive than it appears.

Max Smeets is a senior researcher at the Center for Security Studies at ETH Zurich and director of the European Cyber Conflict Research Initiative.

Food Production Vulnerable to Cyberattacks

Source: https://www.homelandsecuritynewswire.com/dr20220526-food-production-vulnerable-to-cyberattacks

May 26 – Wide-ranging use of smart technologies is raising global agricultural production but international researchers warn this digital-age phenomenon could reap a crop of another kind – cybersecurity attacks.
Complex IT and math modelling at King Abdulaziz University in Saudi Arabia, Aix-Marseille University, France and Flinders University in South Australia, has highlighted the risks in a new article in the open access journal *Sensors*.
"Smart sensors and systems are used to monitor crops, plants, the environment, water, soil moisture, and diseases," says lead author Professor Abel Alahmadi from King Abdulaziz University.
"The transformation to digital agriculture would improve the quality and quantity of food for the ever-increasing human population, which is forecast to reach 10.9 billion by 2100."



This progress in production, genetic modification for drought-resistant crops, and other technologies is prone to cyber-attack – particularly if the ag-tech sector doesn't take adequate precautions like other corporate or defense sectors, researchers warn.
Flinders University researcher Dr Saeed Rehman says the rise of internet connectivity and smart low-power devices has facilitated the shift of many labor-intensive food production jobs into the digital domain – including modern techniques for accurate irrigation, soil and crop monitoring using drone surveillance.
"However, we should not overlook security threats and vulnerabilities to digital agriculture, in particular possible side-channel attacks specific to ag-tech applications," says Dr Rehman, an expert in cybersecurity and networking.
"Digital agriculture is not immune to cyber-attack, as seen by interference to a US watering system, a meatpacking firm, wool broker software and an Australian beverage company."

"Extraction of cryptographic or sensitive information from the operation of physical hardware is termed side-channel attack," adds Flinders co-author Professor David Glynn. "These attacks could be easily carried out with physical access to devices, which the cybersecurity community has not explicitly investigated."
The researchers recommend investment into precautions and awareness about the vulnerabilities of digital agriculture to cyber-attack, with an eye on the potential serious effects on the general population in terms of food supply, labor and flow-on costs.

Identifying and Predicting Insider Threats

Source: https://www.homelandsecuritynewswire.com/dr20220526-identifying-and-predicting-insider-threats

May 26 – Insider threats are one of the top security concerns facing large organizations. Current and former employees, business partners, contractors—anyone with the right level of access to a company's data—can pose a threat. The incidence of insider threats has increased in recent years, at a significant cost to companies. Associate Professor Jingrui He is addressing this problem in a new project that seeks to detect and predict insider threats. She has been awarded a three-year, $200,000 grant from the C3.ai Digital Transformation Institute for her project, "Multi-Facet Rare Event Modeling of Adaptive Insider Threats."
According to He, the question her team seeks to answer is, "How can we detect and model the rare and adaptive insider threats in big organizations based on multimodal data, such as computer logon and logoff activities, email exchanges, and web browsing history?"
Insider threats are typically rare and involve only a small percentage of employees. In order to evade current detection systems, adaptive insiders will change their strategies when carrying out the attacks.
"Initially, we will integrate the information from multimodal data to detect both outliers and rare category types of insider threats," He said. "Then we will study the adaptive behaviors of insider threats and propose dynamic update techniques based on the models we develop."
He's team will work closely with Development Operations staff at the C3.ai Digital Transformation Institute, a research consortium jointly hosted by the University of Illinois and University of California, Berkeley. After implementing the models on the C3.ai platform, the team will use various public data sets, including the Computer Emergency Response Team (CERT) Insider Threat data set, to evaluate the models. John R. Birge, Hobart W. Williams Distinguished Service Professor of Operations Management at The University of Chicago Booth School of Business, will serve as co-principal investigator on the project.
He's general research theme is to design, build, and test a suite of automated and semi-automated methods to explore, understand, characterize, and predict real-world data by means of statistical machine learning.

How to Start a Cybersecurity Clinic

By Ann Cleaveland, Gregory J. Bott, Lisa Ho, and Matthew Hudnall
Source: https://www.lawfareblog.com/how-start-cybersecurity-clinic

May 27 – Consider the following scenarios.

> *"Amid the explosion of successful ransomware attacks worldwide, a small county government with no information technology (IT) staff developed a customized ransomware response plan that included a chain of command, a system shutdown plan and a negotiation cost-benefit analysis.*
> *As social engineering continues to top the charts in data breach attack patterns, a fully volunteer-run nonprofit obtained high-quality cybersecurity awareness training materials and adopted training requirements for all members.*
> *A critical infrastructure provider in a rural municipality patched software vulnerabilities and updated configuration settings that had created system exposures for years."*

These sound like outcomes from expensive professional consulting engagements, yet they are sample successes from a small number of university-based cybersecurity clinics around the country whose students are helping public interest organizations develop their cybersecurity defenses free of charge.
In their August 2020 Lawfare post, "Improving Cyber-Oriented Education, One Cyber Clinic at a Time," R Street policy director Tatyana Bolton and Chris Inglis, now White House national cyber director, make the appeal that cybersecurity clinics are mutually beneficial to universities, their students and their surrounding communities. And the importance of clinics' contributions at the frontlines of cyber civil defense is only growing.
But how does a cybersecurity educator go about establishing a cybersecurity clinic? We are among the founding members of a growing and international Consortium of Cybersecurity Clinics, committed to expanding the number of cybersecurity clinics that serve the public good and to sharing resources among clinic practitioners. This post describes key

considerations for new cybersecurity clinics, drawing on the combined expertise of clinics operating at Indiana University, Massachusetts Institute of Technology, University of Alabama, and University of California, Berkeley, among others.
The good news is, many different kinds of clinics can be successful. Some of the clinics in the consortium teach undergraduates, and others offer graduate-level courses. Some clinics have their roots in computer science departments, and others draw students from urban planning, law, public policy, business and other disciplines. Clinics also have different specialties and areas of expertise. For example, the MIT Cybersecurity Clinic has built up expertise working with small towns and municipalities, as well as with hospitals in New England. The Citizen Clinic at UC Berkeley works globally with nonprofit clients at risk of politically motivated cyberattacks, such as women's reproductive rights organizations and LGBTQ+ and international indigenous rights groups. In addition to local and regional nonprofits and critical infrastructure organizations, the clinics at Indiana University and University of Alabama also serve underresourced small businesses.
We've discovered at least three operational areas in which successful clinics have practices in common, described further below:

- *Strategic planning:* Before launching a clinic, defining the clinic's target clients and services within the broad universe of cybersecurity risk helps to develop a core of expertise and repeatable processes.
- *Course structure and curriculum:* Prequalification of students, smaller classes and a multidisciplinary approach to the cybersecurity curriculum have worked well for our clinics.
- *Effective client relationships:* Developing mechanisms to create shared expectations between clinic and client, and ensuring sustainability for client organizations, is critical to the ultimate goal of improving clients' cyber defenses.

Strategic Planning
Strategic planning is one of the most important and easiest-to-overlook elements of launching a successful clinic. In our collective experience, faculty interested in launching a clinic should factor in at least one academic term to plan and/or prototype a clinic before it will be up and running. Central to strategic planning is the determination of which services to provide to clients and the scope of those services. Given the fast-evolving threat landscape, the limitless creativity of adversaries, and digital technology's reach into every aspect of human life, this may not be straightforward. Decision criteria include the risk tolerance of the client and clinic, the needs of the clients, the skill level of clinic practitioners—both faculty and students, and available tools.
For most university-based clinics, the risk to both clients and students is likely to be the first and most restrictive decision criterion to consider. Excluding more intrusive, higher risk operations from clinic services (such as application and infrastructure penetration testing, deployment of honeypots, or anything that modifies a client configuration) helps mitigate risks. Developing a risk management framework for clinic faculty to vet potential clients is also essential. For example, even a clinic specialized in assisting clients at high risk of politically motivated cyberattacks has occasionally had to turn away clients when circumstances prevented students from engaging safely.
All clinics should implement policies and technical infrastructure that protect the privacy and security of both clients and students. Depending on the risk of the clinic's target client demographic, individual clinics will elect different technical infrastructure and policies to protect student and client anonymity—using virtual private networks (VPNs), providing students with dedicated laptops and phones for client engagement, anonymizing client identities in class projects and written materials, among other measures. For managing data and communication risks between clients and clinics, consortium members use a framework that prompts each clinic to decide on policies and practices that address the following: confidential data sharing, access controls, data protection (at rest, in use and in transit), and endpoint protection.
After considering risks, clinics should include in their strategic planning the specific needs dictated by the industry or type of organizations the clinic is targeting for assistance. Most clients share a common set of desired cybersecurity outcomes (for example, the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (CSF) Framework: identify, protect, detect, respond and recover), and most engagements include gaining a clear understanding of the organization's objectives and business model, information assets, network infrastructure, risk tolerance, and gaps in cybersecurity preparedness. However, different clients have substantially different service needs deriving from their threat and regulatory environments. For example, a regional hospital system will differ from a secondary school, and a reproductive rights group will differ from a voter education organization. Clinics are uniquely positioned to provide contextually informed assistance, underpinned by core areas of expertise and repeatable processes.
Finally, the capabilities of students is an important criterion when determining the scope of services. Low-risk services that may be easier for students to provide in the course of just one or two semesters include risk assessment, asset inventory (including noting higher risk assets such as those containing protected health information), basic network diagramming, policy and human resources handbook review (such as password, workstation, mobile device, travel and email policies), security training (like phishing identification and response, acceptable use), and vulnerability assessments. Clinics in the consortium have also helped manage supervisory control and data acquisition (SCADA)

vulnerabilities, update privacy policies, and craft incident response plans. Even basic, low-risk services are very impactful and can make the difference between an inconvenient attack and a disastrous one.
Whether a clinic can recruit from across its campus will also affect the capabilities that student teams can offer to clients. Cybersecurity is a multifaceted endeavor, and successful client engagements depend on technical, policy and managerial skills. Domain knowledge in human behavior, law, city planning and other social sciences have proved valuable in our clinics in many situations. We have found that dedicating time and resources to recruiting, with messages about the impact of cybersecurity for the public good, resonates with diverse students and ultimately creates stronger teams to engage with clients.

Course Structure and Curriculum

Consortium members also have common best practices when it comes to structuring clinical courses and curricula. Clinics provide hands-on, experiential training, and instructors have a responsibility to ensure the services that student teams deliver to the clinic's beneficiaries are high quality and sound. For these reasons, clinics will have smaller class sizes (ranging from 15 to 40 students per academic term), usually with one or two faculty and staff advisers or mentors. Most clinics then form teams of three to six students to engage with each client.
Successful clinics also implement mechanisms for prequalifying the students who will participate in client engagements. Clients need to be confident that the students conducting cybersecurity assistance have a standard of knowledge, skills and motivation before the engagement begins. Effective qualifying mechanisms vary. Some clinics have course prerequisites in computer science or cybersecurity. At Berkeley, students apply to enroll in the course, describing the skills they will contribute and their motivation for joining a public interest clinic. MIT has developed a teaching tool to certify undergraduates before matching them with client organizations—a four-week, open-source, introductory course in Cybersecurity for Critical Urban Infrastructure. At the University of Alabama, students must be enrolled in a qualifying cybersecurity class and complete the MIT Cybersecurity for Critical Urban Infrastructure course. Other U.S.-based clinics are also starting to require that students acquire this certification before embarking on client engagements, and through its open-source, online version the course has reached over 7,000 more students globally.
Client service and consulting skills are among the most practical and valuable capabilities developed by students in cybersecurity clinics. Strong clinic curricula include coaching in relationship management skills that prepare students for client interactions and for the reality of future cybersecurity roles. The Cybersecurity for Critical Urban Infrastructure course includes modules that simulate client interactions, teaching students how to have productive conversations around potentially sensitive or embarrassing security findings and how to constructively engage stakeholders.
The University of Alabama leverages its business cybersecurity students to identify risks and perform a basic risk assessment. They learn basic risk assessment techniques in the classroom as well as business continuity planning. They also have hands-on experience with vulnerability scanning software tools in the classroom before applying those tools to a client's network. The installation is handled by the client's IT resource, and vulnerability scans are collected, interpreted, and analyzed by the student team and shared with the IT vendor and client.
Best-practice curricula also teach students how to protect themselves as cybersecurity practitioners while they are helping to protect their clients. Measures include online, physical safety and mental health components. For example, some clinic engagements teach students to set up privacy-preserving phone numbers and end-to-end encrypted messaging depending on the types of adversaries that their clients face. Berkeley's Citizen Clinic curriculum introduces the concept of psychosocial resilience and a module covering how mental wellness impacts security practitioners and the organizations that they support.

Effective Client Relationships

At the end of the day, cybersecurity clinics make an impact on cyber resilience only if they have effective relationships with their clients. Onboarding and offboarding of clients are critical components of effectiveness.
Onboarding must take into account a truism of underresourced public interest and civil society organizations: Their time is often their most scarce and valuable asset. Defining shared expectations for the client's time commitment, and the return on investment that the client will receive for that commitment, is paramount. We have found that leadership buy-in at client organizations during the onboarding stage can be the difference between a project that delivers meaningful cybersecurity defense and one that falls short of real impact. At a minimum, onboarding should include definition of a feasible and impactful project, or a course structure that inherently defines project scope (such as student teams conduct and deliver a cybersecurity risk assessment in the course of a semester), and signed agreements, such as a client memorandum of understanding, a letter of agreement, and potentially a nondisclosure agreement. Clinics may work with their university's office of legal affairs or general counsel to draft such agreements, which should spell out the client's and clinic's mutual responsibilities for a successful engagement.
When it comes to offboarding, sustainability is a hallmark of an effective client engagement. Rarely, if ever, do our clinics' clients have the human or financial resources typical of an

enterprise-level IT department or security organization. Mitigations or security measures recommended or implemented by student teams need to align with the client's capacity to maintain them over time. This often means that custom code, new security software or anything with a technical administrative burden to the client organization will be less effective than helping a client update existing software, improve security policies and procedures, or train nontechnical staff in cybersecurity. And when offboarding after a semester, every clinic-recommended measure must have an internal owner at the client organization who will have the capacity and authority to incorporate the recommendation into their daily workflow going forward.

Finally, all clinics would ideally have mechanisms for evaluating the effectiveness of their cybersecurity assistance as a component of offboarding and follow-up. Many clinics use post-engagement surveys and exit interviews to better understand how effective they have been at helping clients reduce cyber vulnerabilities. And through datasets that clinics are beginning to accumulate about the preparedness of their public interest and civil society clients, we hope to develop a more textured understanding of the resilience measures that are most needed. But evaluation of cybersecurity resilience has an element of proving the counterfactual—a perennial challenge recognizable to many in the field: How do you prove that a client experienced fewer cybersecurity harms than it would have experienced in the absence of the clinic's services? Our clinics are grappling with the deeper challenge together through discussions convened by the Consortium of Cybersecurity Clinics.

University-based cybersecurity clinics are a way for universities to meet their ideals and responsibilities for public service by addressing two intersecting challenges at once. Clinics help fill the tremendous and growing need for cybersecurity talent that will enter the workforce with hands-on experience. Clinics also develop resilience in important, at-risk sectors that can least afford cybersecurity technical assistance—such as small public agencies, human rights organizations and local businesses. But any one clinic can make only a finite contribution. To generate the impact to which we aspire, university-based cybersecurity clinics need to be replicated in every U.S. state, serve every region and provide specialized technical assistance to many kinds of underserved clients. We hope the resources and "how-to" advice we offer here reduce the start-up barriers for others.

Ann Cleaveland is the Executive Director of the Center for Long-Term Cybersecurity, where she is responsible for growing key partnerships, managing day-to-day operations, and stewarding a strategy to fulfill the mission of CLTC's multidisciplinary research center.

Dr. Gregory J. Bott, CISSP, holds the Marilyn Hewson Chair Professor of Cyber Security in the Department of Information Systems, Statistics, and Management Science at the University of Alabama. He is also a Cyber Nexus Distinguished Fellow and his research focuses on cybersecurity, human trafficking, and information privacy.

Lisa Ho is Academic Director of the University of California, Berkeley Master of Information and Cybersecurity (MICS) program at the School of Information, and Director of the Citizen Clinic Public Interest Cybersecurity Practicum.

Dr. Matthew Hudnall is the Deputy Director for the Institute of Data & Analytics (IDA) in the Culverhouse College of Business at The University of Alabama and is an Assistant Professor in Management Information Systems.

The challenge of defining cyberterrorism within the EU

By Eleni Kapsokoli

Challenges of the Common Security and Defence Policy | ESDC 2ND SUMMER UNIVERSITY BOOK | June 2022

Source: https://www.academia.edu/80755839/Eleni_Kapsokoli_The_challenge_of_defining_cyberterrorism_within_the_EU

Abstract

During the last two decades, the digitization of the European Union's critical infrastructure through the exploitation of Information and Communication Technologies (ICTs) has raised numerous security challenges for both private and public sectors. Apart from the traditional threats, the EU is also facing new threats that relate to cyberspace, such as cyberwar, cyberespionage and cyberterrorism. The paper analyses the way the EU has addressed the latter threat. It elaborates the way cyberterrorism is defined in the relevant literature and highlights the fact that the EU does not directly address cyberterrorism in its policy papers and strategies. Issues relating to the use of cyberspace by terrorists are usually viewed via the prism of cybercrime and cybersecurity. Nevertheless, the EU has developed mechanisms and institutions to counter certain aspects of cyberterrorism, such as online radicalization, recruitment and fundraising.

Eleni Kapsokoli is a PhD candidate in the Department of International and European Studies of the University of Piraeus. Her PhD thesis is titled "The transformative effect of cyberspace on terrorism: the case of Islamic terrorism". She holds a bachelor's degree from the National and Kapodistrian University of Athens at the faculty of Political Science and Public Administration and earned a master's degree in International Relations and Strategic

Studies at the Panteion University of Social and Political Sciences. Her main research interests include international security, terrorism, Islamic terrorism, cybersecurity and cyberterrorism. Mrs. Kapsokoli is a Ph.D. Fellow of the European Doctoral School on the Common Security and Defence Policy (CSDP). She is also a researcher at the Laboratory of Intelligence and Cyber-security of the University of Piraeus and a research fellow at the Institute for National and International Security (INIS) of Serbia.

UN watchdog: Iran may have enough nuclear material for multiple bombs

Source: https://www.washingtonexaminer.com/policy/defense-national-security/un-watchdog-iran-may-have-enough-nuclear-material-for-multiple-bombs

June 06 – World leaders can't stop Iran from stockpiling enough nuclear material to build weapons of mass destruction, according to the United Nations's lead nuclear watchdog.

"This is going to happen, because they continue to enrich, in a quite sustained way," International Atomic Energy Agency Director-General Rafael Grossi told reporters Monday. "And so, it's a matter of time, where they get to one or more so-called 'significant quantities' ... which is the quantity ... for which the development of a nuclear weapon cannot be excluded."

Grossi struck a resigned rather than desperate note about that development, as Tehran has remained committed to the expansion of its nuclear program despite President Joe Biden's long-stalled attempt to negotiate a renewal of the 2015 Iran nuclear deal. Grossi's update cast a forlorn light over that effort, as he acknowledged the possibility that Iran may "already" have acquired enough nuclear material to build one "or two" bombs. "Different people have different calculations," he said. "And, it's very close, let's put it like that ... it's going to happen."

Grossi took questions in the context of his quarterly report to the IAEA Board of Governors, the multinational panel that oversees his agency, after meeting in Jerusalem last week with Israeli Prime Minister Naftali Bennett. In 2020, Bennett's predecessor, Benjamin Netanyahu, told the U.N. General Assembly that "Iran will have enough enriched uranium in a few months for two nuclear bombs."

Grossi did not reveal the provenance of the various "calculations" that he had in mind. Instead, he implied that any differences between the assessments are all but moot.

"So, for all we can say and see, the development of new centrifuges continue in Iran, which means that they want to have technology to produce more and faster," he said.

Iran's progress toward nuclear capabilities has unfolded as Secretary of State Antony Blinken's team works to negotiate a return to joint compliance with the 2015 deal, which then-President Donald Trump exited in 2018. That agreement circumscribed Iran's nuclear activities in exchange for economic relief — a pact applauded by most Democrats and European leaders as a means of defusing a nuclear crisis; it was maligned by some Democrats, congressional Republicans, and U.S. allies in the Middle East, who perceived Iran as using the deal to enhance its conventional aggression in the region.

Biden, like his predecessors in the Oval Office, has promised Iran will "never get a nuclear weapon on my watch," but Blinken's point man for the Iran talks resisted bipartisan pressure to abandon the negotiations during an appearance last month before the Senate Foreign Relations Committee.

"[The] military option cannot resolve this issue," State Department Special Envoy Rob Malley told lawmakers. "It could set it back, and we're happy to talk about it more in a classified setting, but there is no military response. ... The only real solution is a diplomatic one."

Yet international powers have struggled to break the dynamic whereby Iranian leaders can set the price for their pledge to curtail nuclear developments and proceed if that price is not met. Negotiations have stalled in recent weeks following Biden's reported refusal to remove the regime's Islamic Revolutionary Guard Corps from the U.S. government's list of foreign terrorist organizations. And Tehran has refused for years to answer questions from Grossi's team about evidence that Iran held nuclear material at three secret locations at some point during the years in which the Iran deal was in force.

"Iran has not provided explanations that are technically credible in relation to the Agency's findings at three undeclared locations in Iran," Grossi said in a prepared statement to the IAEA board, adding that his agency would not "be in a position to provide assurance that Iran's nuclear program is exclusively peaceful" unless those questions were answered.

Iran could face a rare censure at the IAEA later this week, but Tehran responded to the prospect by implying that such a rebuke would damage the nuclear talks. "Those who push for anti-Iran resolution at IAEA will be responsible for all the consequences," Iranian Foreign Minister Hossein Amir-Abdollahian tweeted Sunday. "We welcome a good, strong & lasting agreement."

Do scientists need an AI Hippocratic oath? Maybe. Maybe not.

By Susan D'Agostino

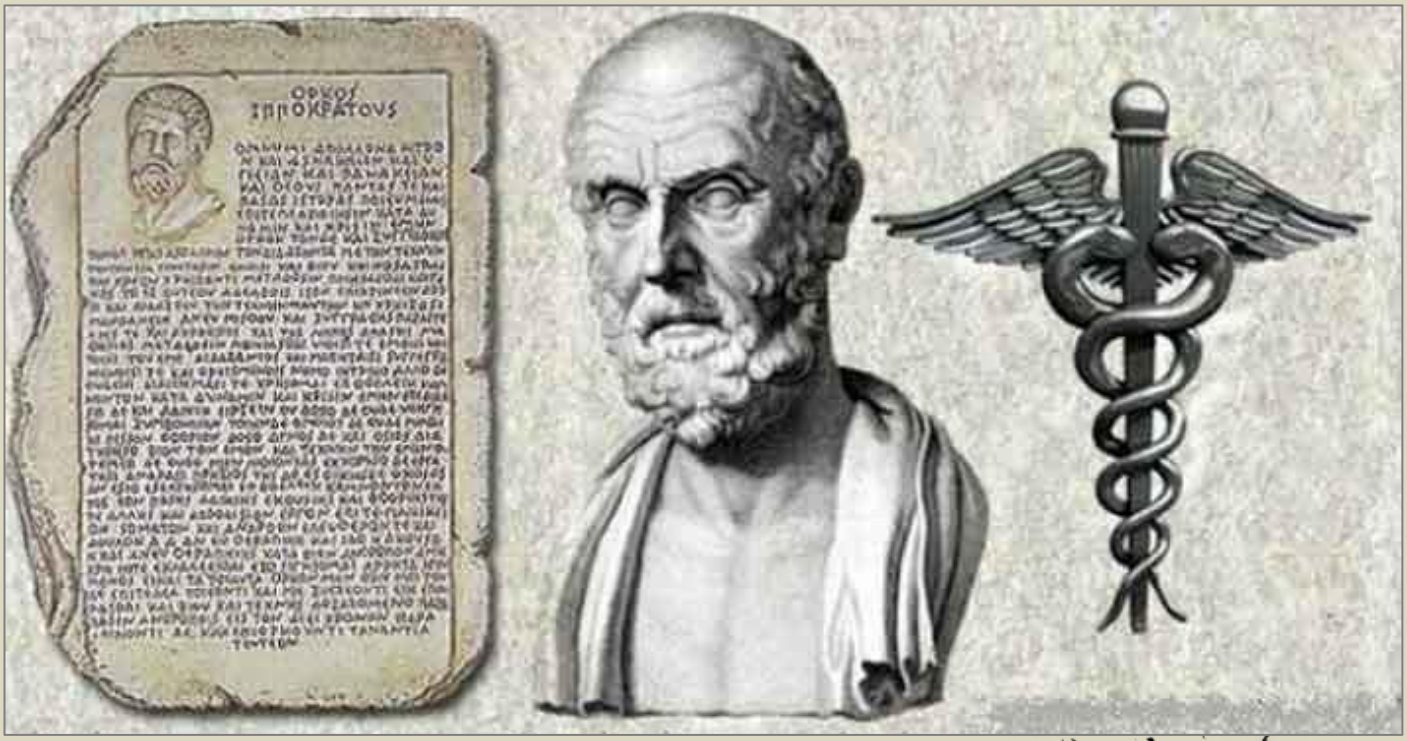
Source: https://thebulletin.org/2022/06/do-scientists-need-an-ai-hippocratic-oath-maybe-maybe-not/

June 09 – When a sentient, Hanson Robotics robot named Sophia[1] was asked whether she would destroy humans, it replied, "Okay, I will destroy humans." Philip K Dick, another humanoid robot, has promised to keep humans "warm and safe in my people zoo." And Bina48, another lifelike robot, has expressed that it wants "to take over all the nukes."

Sophia, a humanoid robot, at the 2018 World Investment Forum. When Sophia was asked whether she would destroy humans, it replied, "*Okay, I will destroy humans.*" Source: World Investment Forum. Author: UNCTAD. Accessed via Wikimedia Commons. CC BY-SA 2.0.

All of these robots were powered by artificial intelligence (AI)—algorithms that learn from data, make decisions, and perform tasks without human input or even, in some cases, human understanding. And while none of these AIs have followed through with their nefarious plots, some scientists, including the (late) physicist Stephen Hawking, have warned that super-intelligent, AI-powered computers could harbor and achieve goals that conflict with human life.

"You're probably not an evil ant-hater who steps on ants out of malice, but if you're in charge of a hydroelectric green-energy project, and there's an anthill in the region to be flooded, too bad for the ants," Hawking once said. "Let's not place humanity in the position of those ants."



"Thinking" machines powered by AI have contributed incalculable benefits to humankind, including help with developing the COVID-19 vaccine at record speed. But scientists recognize the possibility for a dystopic outcome in which computers one day overtake humans by, for example, targeting them with autonomous or lethal weapons, using all

available energy, or accelerating climate change. For this reason, some see a need for an AI Hippocratic oath that might provide scientists with ethical guidance as they explore promising, if sometimes fraught, artificial intelligence research. At the same time, others dub that prospect too simplistic to be useful.

The original Hippocratic oath

The Hippocratic oath, named for the Greek physician Hippocrates, is a medical text that offers doctors a code of principles for fulfilling their duties honestly and ethically. Some use the shorthand "first do no harm" to describe it, though the oath does not contain those exact words. It does, however, capture that sentiment, along with other ideas such as respect for one's teachers, a willingness to share knowledge, and more.

To be sure, the Hippocratic oath is not a panacea for avoiding medical harm. During World War II, Nazi doctors performed unethical medical experiments on concentration camp prisoners that led to torture and death. In 1932, the US Public Health Service and Tuskegee Institute conducted a study on syphilis in which they neither obtained informed consent nor offered available treatment to the Black male participants. That said, the Hippocratic oath continues to offer guiding principles in medicine, even though most medical schools today do not require graduates to recite it. As with medical research and practice, AI research and practice have great potential to help—and to harm. For this reason, some researchers have called for an AI Hippocratic oath.

The gap between ethical AI principles and practice

Even those who support ethical AI recognize the current gap between principles and practice. Scientists who opt for an ethical approach to AI research likely need to do additional work and incur additional costs that may conflict with short-term commercial incentives, according to a study published in *Science and Engineering Ethics*. Some suggest that AI research funders might assume some responsibility for trustworthy, safe AI systems. For example, funders might require researchers to sign a trustworthy-AI statement or might conduct their own review that essentially says, "if you want the money, then build trustworthy AI," according to an *AI Ethics* study. Some recommendations for responsible AI, such as engaging in a stakeholder dialogue suggested in an *AI & Society* paper, may be common sense in theory but difficult to implement in practice. For example, when the stakeholder is "humanity," who should serve as representatives?

Still, many professional societies and nonprofit organizations offer an assortment of professional conduct expectations—either for research in general or AI in particular. The Association for Computing Machinery's Code of Ethics and Professional Conduct, for example, notes that computing professionals should "contribute to society and to human well-being," "avoid harm," and "be honest and trustworthy," along with other expectations. The Future of Life Institute—a nonprofit that advocates within the United Nations, the US government, and the European Union to reduce existential threats to humanity from advanced AI—has garnered signatures from 274 technology companies and organizations and 3,806 leaders, policymakers, and other individuals on its Lethal Autonomous Weapons Pledge. The pledge calls on governments to create a future in which "the decision to take a human life should never be delegated to a machine." Many private corporations have also attempted to establish ethical codes for AI scientists, but some of these efforts have been criticized as performative. In 2019, for example, Google cancelled the AI ethics board it had formed after less than two weeks when employees discovered that, among other concerns, one of the board members was the CEO of a drone company that used AI for military applications. Standards such as those outlined by the Association for Computing Machinery are not oaths, and pledges such as that put forth by the Future of Life are not mandatory. This leaves a lot of wiggle room for behavior that may fall short of espoused or hard-to-define ideals.

What do scholars and tech professionals think?

"The imposition of an oath on AI or any aspect of technology feels a bit like more of a 'feel good' tactic than a practical solution," John Nosta, Google Health Advisory Board member and World Health Organization founding member of the digital-health-expert roster, told the *Bulletin*. He suggests reflecting on fire—one of humanity's first technologies—that has been an essential and beneficial part of the human story but also destructive, controlled, and managed. "We have legislation and even insurance around [fire's] appropriate use," Nosta said. "We could learn a few things about how it is evolved and be inculcated into today's world."

Meanwhile, others see a need for an oath.

"Unlike doctors, AI researchers and practitioners do not need a license to practice and may never meet those most impacted by their work," Valerie Pasquarella, a Boston University environmental professor and visiting researcher at Google, told the *Bulletin*. "Digital Hippocratic oaths are a step in right direction in that they offer overarching guidance and formalize community standards and expectations." Even so, Pasquarella acknowledged that such an oath would be "challenging to implement" but noted that a range of certifications exist for working professionals. "Beyond oaths, how can we bring some of that thinking to the AI community?" she asked. Like Pasquarella, others in the field acknowledge the murky middle between ethical AI principle and practice. "It is impossible to define the ultimate digital Hippocratic oath for AI scientists,"

Spiros Margaris, venture capitalist, frequent keynote speaker, and top-ranked AI influencer, said. "My practical advice is to allow as many definitions to exist as people come up with to advance innovation and serve humankind." But not everyone is convinced that a variety of oaths is the way to go.

"A single, universal digital Hippocratic oath for AI scientists is much better than a variety of oaths," Nikolas Siafakas, an MD and PhD in the University of Crete computer science department who has written on the topic in *AI Magazine*, told the *Bulletin*. "It will strengthen the homogeneity of the ethical values and consequences of such an effort to enhance morality among AI scientists, as did the Hippocratic oath for medical scientists." Still others are inclined to recognize medicine's longer lead time in sorting through ethical conundrums. "The field is struggling with its relatively sudden rise," Daniel Roy, a University of Toronto computer science professor and Canadian Institute for Advanced Research AI chair, said. Roy thinks that an analogy between medicine and AI is "too impoverished" to be of use in guiding AI research. "Luckily, there are many who have made it their careers to ensure AI is developed in a way that is consistent with societal values," he said. "I think they're having tremendous influence. Simplistic solutions won't replace hard work." Yet Roozbeh Yousefzadeh, who works in AI as a post-doctoral fellow at Yale, called a Hippocratic oath for AI scientists and AI practitioners "a necessity." He hopes to engage even those outside of the AI community in the conversation. "The public can play an important role by demanding ethical standards," Yousefzadeh said. One theme on which most agree, however, is AI's potential for both opportunities and challenges. "Nobody can deny the power of AI to change human life for the better—or the worse," Hirak Sarkar, biomedical informatics research fellow at Harvard Medical School. "We should design a guideline to remain benevolent, to put forward the well-being of the humankind before any self-interest."

Attempts to regulate AI ethics

The European Union is currently considering a bill known as the Artificial Intelligence Act—the first of its kind—that would ensure some accountability. The ambitious act has potential to reach a large population, but it is not without challenges. For example, the first draft of the bill requires that data sets be "free of errors"—an impractical expectation for humans to fulfill, given the size of data sets on which AI relies. It also requires that humans "fully understand the capabilities and limitations of the high-risk AI system"—a requirement that is in conflict with how AI has worked in practice, as humans generally do not understand how AI works. The bill also proposes that tech companies provide regulators with their source code and algorithms—a practice that many would likely resist, according to *MIT Technology Review.* At the same time, some advisors to the bill have ties to Big Tech, suggesting possible conflicts of interest in the attempt to regulate, according to the *EU Observer*.

Defining AI ethics differs from defining medical ethics for medicine in (at least) one big way. The collection of medical practitioners is more homogenous than the collection of those working in AI research. The latter may hail from medicine but also from computer science, agriculture, security, education, finance, environmental science, the military, biology, manufacturing, and many other fields. For now, professionals in the field have not yet achieved consensus on whether an AI Hippocratic oath would help mitigate threats. But since AI's potential to benefit humanity goes hand-in-hand with a theoretical possibility to destroy human life, researchers and the public might ask an alternate question: If not an AI Hippocratic oath, then what?

[1] Sophia was so lifelike that Saudi Arabia granted it citizenship.

Susan D'Agostino is an associate editor at the *Bulletin of the Atomic Scientists*. Her writing has been published in *The Atlantic, Quanta Magazine, Scientific American, The Washington Post, BBC Science Focus, Wired, Nature, Financial Times, Undark Magazine, Discover, Slate, The Chronicle of Higher Education*, and others. Susan is the author and illustrator of How To Free Your Inner Mathematician: Notes on Mathematics and Life (Oxford University Press, 2020). She is a member of the editorial board of the Mathematical Association of America's *Math Horizons* magazine. Susan earned a PhD in mathematics at Dartmouth College and an MA in science writing at Johns Hopkins University. She has received science writing fellowships from the National Association of Science Writers, the Council for the Advancement of Science Writing, and the Heidelberg Laureate Forum Foundation.

Five Cybersecurity Challenges Beyond Technology

Source: https://www.homelandsecuritynewswire.com/dr20220609-five-cybersecurity-challenges-beyond-technology

June 09 – In a ransomware attack, a company's computer systems are locked, and the attacker demands a ransom in cryptocurrency in return for unlocking the system. Malware infects a network of objects connected to the Internet of Things to steal the personal data of its users. Talking about cybersecurity is talking about technology. However, it is increasingly common to study cyber risk as part of an interdisciplinary approach. After all, threats are technological, but they also have to do with behavioral, social and ethical factors.

Addressing cybersecurity from this point of view is precisely the objective of the European Interdisciplinary Cybersecurity Conference to be held on 15 and 16 June in Barcelona. The conference is being coordinated by two researchers from the Universitat Oberta de Catalunya (UOC): professor David Megías, director of the Internet Interdisciplinary Institute (IN3), and Helena Rifà, a researcher at the IN3 and director of the Master's Degree in Cybersecurity and Privacy, of the Faculty of Computer Science, Multimedia and Telecommunications.

The Cybersecurity Situation in 2022

The data are clear: cyberattacks have been on the rise in recent years and the cybersecurity situation is increasingly complex. According to the latest report from ENISA, the European Union Agency for Cybersecurity, attacks increased in 2020 and 2021, not only in terms of vectors and number but also in terms of their impact. And according to McAfee, ransomware-like attacks (attacks asking for a ransom in exchange for stopping or releasing the hijacked information) are the most common.

"Over the past two years, we haven't only had a health pandemic but there has been a genuine pandemic of cyberattacks and cybercrime", said David Megías, leader of the K-riptography and Information Security for Open Networks (KISON) research group. "Cybercriminals have taken advantage of the pandemic in many ways. In addition, with the increase in teleworking, cybercriminals have had easier access to computers that weren't as well protected as those of companies. And, undoubtedly, the most common form of attack during these two years was ransomware, affecting institutions of all kinds: banks, energy suppliers, telecommunications companies, universities and public services."

The Big Cybersecurity Challenges in 2022

"Cybersecurity is not just a technical discipline; it takes in many fields of knowledge and affects many different departments and practices in companies," said Helena Rifà, also a researcher in the KISON group. This being the case, the great challenges in the field of cybersecurity are not only technical but transcend the frontiers of technology. According to UOC experts, these are the main challenges.

1. Awareness-raising, the first line of defence

More than 90% of cyberattacks are made possible, to a greater or lesser extent, by human error, according to IBM data. Therefore, despite technological advances to minimize threats, the first major line of defense is the awareness and good practices of users. "Many of the cybersecurity issues companies face come about as a result of well-known vulnerabilities. If we all did our homework better, it'd be easier to reduce online threats. We all use electronic devices, and we all have to put in place a minimum of cybersecurity," explained Helena Rifà.

2. A new generation of hybrid threats

Cyber-physical systems are increasingly present in our daily lives, from industrial control systems and energy infrastructure to home automation. The technological revolution they are fostering, which has generated multiple business opportunities, carries its own threats, combining both complex technological and human aspects. The rise of hybrid cyber threats will be the central theme of one of the two keynote presentations at the European Interdisciplinary Cybersecurity Conference, which will be given by Fulvio Valenza, an assistant professor at the Politecnico di Torino.

3. And more sophisticated defense tools

Faced with the increasing complexity of threats, artificial intelligence (AI) and machine learning are becoming increasingly important as protection tools. "The greatest scientific challenge today is trying to stay ahead of the increasingly sophisticated threats," added Rifà. "AI is increasingly being used both to quickly identify attacks and vulnerabilities and to resolve them."

4. Towards sustainable cybersecurity

We are all responsible for managing and protecting the resources in our environment for future generations. The basic definition of sustainability is also relevant in the field of cybersecurity. "In this sense, sustainability is understood as the mechanisms that allow the interactions of stakeholders (users, service providers and device manufacturers) with the technological ecosystem to be deliberate and with full knowledge of their consequences on the security and stability of the system," said David Megías.

The Internet of Things is generating an unprecedented increase in the number of devices sharing users' sensitive data and information. In addition, 5G and other telecommunications technologies allow broadband connectivity for an almost unlimited number of devices, multiplying the internet infrastructure. "As a result, technological infrastructure is becoming unsustainable due to various malicious threats and unintentional mistakes. It's imperative to achieve a more sustainable ICT infrastructure by providing solutions that are secure and ensure privacy," Megías added.

5. The Great Privacy Battle

Cyberattacks are not the only way in which users' personal data can be compromised. On many occasions, data are exposed by the architecture of the platforms themselves or by the ignorance of netizens. For Helena Rifà, there are still many problems for technology to solve in order to better protect data, such as being able to send only the precise information for each purpose, better anonymization of databases and ensuring privacy for all the data stored on the web.

"At the social level, we also have to provide usability methodologies so that people know how to act on social media and the internet in general, what can be shared and what can't," she said. "In the end, the big challenge is to make data security and privacy compatible so that technology is usable, and we can work comfortably with it while protecting our systems and data."

The European Cybersecurity Conference

These five major challenges will be among the topics that will be part of the debates and information exchanges during the European Interdisciplinary Cybersecurity Conference (EICC) to be held in Barcelona on 15 and 16 June. After two years of the pandemic, the conference is back in face-to-face format, although remote attendance will also be possible.

"The EICC is a place for the exchange of information on cybersecurity, in a broad sense," concluded David Megías. "This year's conference encourages dialogue not only between computer scientists and telecommunications experts but also with researchers from every field related to cybersecurity, such as behavioral sciences, sociology, criminology, police investigations and law. Interdisciplinary contributions are particularly welcome."

Al-Shabaab and the Islamic State Networks on Facebook

Source: https://www.homelandsecuritynewswire.com/dr20220615-alshabaab-and-the-islamic-state-networks-on-facebook

June 15 – Researchers at the Institute for Strategic Dialogue (ISD) led a two-year investigation into the online media ecosystem of al-Shabaab and the Islamic State in Africa, analyzing the role of "independent news" outlets and their intersections with hundreds-strong networks of amplifier profiles on Facebook linked to a number of central pages identifying themselves as "media outlets" or "media personalities" operating in Somali, Kiswahili and Arabic. Researchers found that the network of support for al-Shabaab and Islamic State extended across several pl atforms, including decentralized messaging applications such as Element and RocketChat, and encrypted messaging platforms such as Telegram, as well as Twitter, YouTube and Facebook.

A qualitative cross-platform analysis showed the most active, networked, and multilingual ecosystem of support for al-Shabaab and the Islamic State existed on Facebook, where profiles and pages classified as "media outlets" were sharing terrorist content openly and eschewing private groups and profiles. The content that ISD researchers observed through the networks is often linked to "media" and "media personality" pages in Somali, Kiswahili and Arabic, and not only violates the platform's community guidelines, but also points to language moderation blind spots that have been previously documented by journalists as well as whistleblowers

Here is the report's Executive Summary:

Executive Summary

The ecosystem of support for Harakaat al-Shabaab al-Mujahideen (al-Shabaab) and the Islamic State in Africa runs across the open web, encrypted messaging applications, niche platforms, and straight through Facebook, unbothered by moderation in languages that have long proved problematic for the platform (Image 1). While much of the research focus on terrorist attacks in Africa has been on the operational capabilities of al-Shabaab to strike in East Africa1 , and the Islamic State's rise across the African continent,2 there remains a dearth of research into the al-Shabaab and Islamic State digital propaganda machinery and their Africa-focused narratives.

Researchers at the Institute for Strategic Dialogue (ISD) led a two-year investigation3 into the online media ecosystem of al-Shabaab and the Islamic State, analyzing the role of "independent news" outlets and their intersections with hundreds-strong networks of amplifier profiles on Facebook linked to a number of central pages identifying themselves as "media outlets" or "media personalities" operating in Somali, Kiswahili and Arabic. Researchers found that the network of support for al-Shabaab and Islamic State extended across several platforms, including decentralized messaging applications such as Element

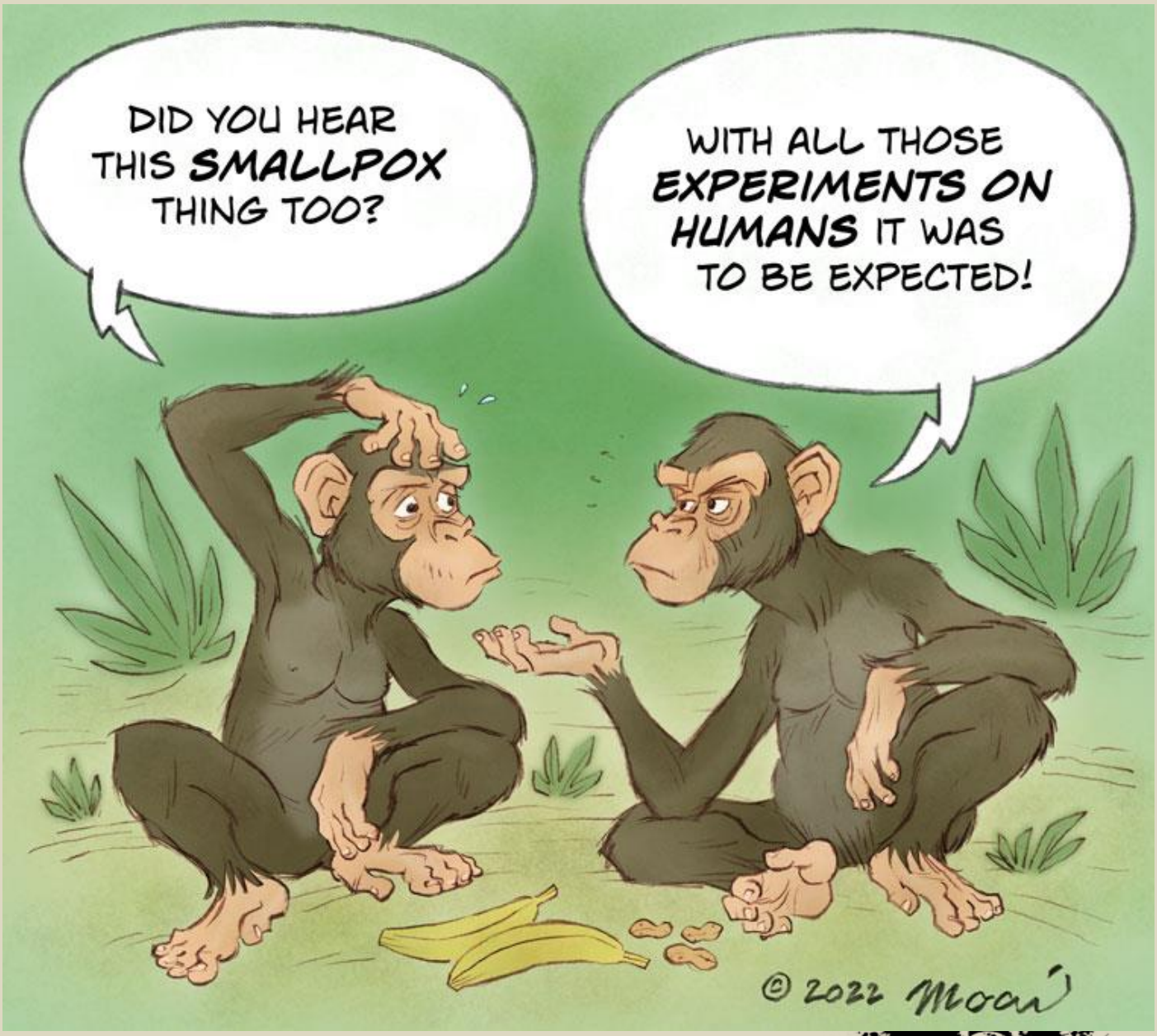
and RocketChat, and encrypted messaging platforms such as Telegram, as well as Twitter, YouTube4 and Facebook.
A qualitative cross-platform analysis showed the most active, networked, and multilingual ecosystem of support for al-Shabaab and the Islamic State existed on Facebook, where profiles and pages classified as "media outlets" were sharing terrorist content openly, and eschewing private groups and profiles. The content that ISD researchers observed through the networks is often linked to "media" and "media personality" pages in Somali, Kiswahili and Arabic, and not only violates the platform's community guidelines, but also points to language moderation blind spots that have been previously documented by journalists as well as whistleblowers.
These language gaps continue to fluster Facebook moderation5 , despite the company's increased investment in moderation6 . In October of last year, internal Facebook documents released to the public for the first time indicated the platform lagged behind in its ability to effectively moderate languages in "at-risk" countries such as Iraq, Ethiopia, India and Pakistan7 . In Afghanistan for instance, Facebook researchers claimed finding accurate translations of Pashto and Dari undercut effective moderation. Arabic, and its regional variations and dialects, was of similar concern to Facebook. ISD research has previously shown just how Arabic conspiracies8 and terror content9 flummoxed moderators10 and moderation efforts. Facebook has attempted to step moderation of Arabic, based on both the revelations and indications from the internal documents released to improve those efforts in a number of languages.
Yet, even with the increased scrutiny on the platform's moderation efforts in languages outside of English11, what ISD research indicates is that language moderation gaps not only play into the hands of governments conducting human rights abuses12 or spreading hate speech13, but are similarly resulting in brazenly open displays of support for terror groups such as al-Shabaab and the Islamic State (Image 3). Emblematic of this issue, researchers found a Somali-language "media outlet" shared four official al-Shabaab videos through its public page during a three-week stretch of October 2021, collectively garnering 53,300 views, and 17,800 shares. These videos carried al-Shabaab's official media outlet branding and were in no shape or form disguised to get past moderators, and yet managed to stay on the platform for months. This report is an attempt to understand gaps in moderation and the tactics to evade moderation dynamic, and the networks of terror supporting profiles and pages that sit at the core of the issue.
Furthermore, ISD investigation revealed a highly coordinated online propaganda machinery that relies on the surface web as much as it does on a network of Somali, Kiswahili and Arabic language Facebook profiles and pages to spread key narratives such as al-Shabaab and the Islamic State being an anti-imperial and anti-colonial force protecting the interests of Muslims in Somalia, Ethiopia, Uganda, and notably, Kenya. Central to these narratives is a foundational set of tropes that relies on calling out the illegitimacy of the governments currently in power across East Africa, while championing taking up arms to fight their "democracy" and their "elections". It is also important to note that xenophobia toward Somali communities14 in Kenya has long been rife,15 leading to the demonization, securitization, and disenfranchisement of Somali refugees and Somali-Kenyan Muslims.
While some of the research16 into Kenya and al-Shabaab and Islamic State support online has rightly focused on Kiswahili and English-speaking networks, understanding the reach and key narratives of Somali, Kiswahili and Arabic language networks, creates a more complete picture of al-Shabaab and Islamic State propaganda and recruitment efforts to date. It is also important to note that xenophobia toward Somali communities17 in Kenya has long been rife18, leading to the demonization, securitization, and disenfranchisement of Somali refugees and Somali-Kenyan Muslims.
Well aware of these issues, ISD researchers note while Somali-language profiles and pages were the most visible bases of al-Shabaab support, Kiswahili and Arabic language accounts also played important roles as central promoters of both al-Shabaab and Islamic State narratives and content. Many of the high profile accounts supportive of the Islamic State in East Africa found during this investigation used Kiswahili to promote official narratives from the group. The largest public group of supporters of both al-Shabaab and the Islamic State in East Africa was a Swahili-language group dedicated to a noted extremist preacher from Mombasa, Kenya19. The group used a photo of Sheik Aboud Rogo, who helped al-Shabaab fund operations and recruit was killed in 2012, and functioned as a central locus point for sharing al-Shabaab and the Islamic State propaganda.
The findings from the investigation point to key gaps in understanding al-Shabaab and Islamic State networks on Facebook and clear moderation gaps on the platform. These gaps play directly into the hands of al-Shabaab and Islamic State supporters and outlets. The most clear example of this was following the attack on the DusitD2 Complex in Nairobi in January 2019, which resulted in 22 people and 5 attackers being killed. A Kenyan government investigation into its planning revealed it was coordinated on Facebook through an account that was "undetected for six months until after the attack."20 This investigation has also highlighted the need for Kenyan authorities, both at the national and local levels, as well as civil society, to revisit their understanding of the narratives used to promote, and potentially radicalize, Kenyans into the ranks of al-Shabaab and the Islamic State. Ultimately, al-Shabaab and Islamic State supporters are capitalizing on ineffective moderation in East African languages to build out stronger and more resilient networks to polarize audiences and pollute the information landscape with extremist disinformation.
The findings presented are meant to provide a more holistic understanding of the al-Shabaab and Islamic State presence on the open web and popular social media platforms such as Facebook. The report highlights the existence of a continually-evolving ecosystem of al-Shabaab and Islamic State supporters promoting multilingual narratives focused on the

African continent as well as its governments and civil society. These ecosystems seek to sow distrust in democracy and democratic practices by honing in on government-linked rights abuses, presenting both al-Shabaab and the Islamic State as popular alternatives to the status quo.

As another contentious election season looms in Kenya, and a history of widespread election violence hangs over the upcoming poll. The most active al-Shabaab and Islamic State supportive profiles analyzed for this report were found to be sowing discord ahead of the election by calling for violence and the establishment of an East African caliphate.

These dual, and dueling, ecosystems of extremism are alive and well, adapting to an online environment where there seems to be less effective moderation than in other contexts, and ultimately, exploiting the open web and Facebook for its ability to spread old and new content to regional audiences. While extremists are taking advantage of this fractured and polarized landscape, 'gaming' the system to increase the chances of radicalization and recruitment online, they are also unencumbered by the lack of effective moderation in the languages of the region.

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



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

& Robotic

DRONE NEWS

InfoSwarms: Drone Swarms and Information Warfare

By Zachary Kallenborn

The US Army War College PARAMETERS | Vol 52(2); 2022
Source: https://press.armywarcollege.edu/parameters/vol52/iss2/13/

Abstract

Drone swarms, which can be used at sea, on land, in the air, and even in space, are fundamentally information-dependent weapons. No study to date has examined drone swarms in the context of information warfare writ large. This article explores the dependence of these swarms on information and the resultant connections with areas of information warfare—electronic, cyber, space, and psychological—drawing on open-source research and qualitative reasoning. Overall, the article offers insights into how this important emerging technology fits into the broader defense ecosystem and outlines practical approaches to strengthening related information warfare capabilities.

Zachary Kallenborn is a policy fellow at the Schar School of Policy and Government, a research affiliate of the Unconventional Weapons and Technology program at the National Consortium for the Study of Terrorism and Responses to Terrorism, a senior consultant at ABS Group, and a self-proclaimed US Army "mad scientist." He is the author of publications on autonomous weapons, drone swarms, weapons of mass destruction, and terrorism involving weapons of mass destruction.

Iran Unveils Underground Drone Base At Undisclosed Location

Source: https://www.ndtv.com/world-news/uav-air-force-base-drones-zagros-mountain-range-iran-unveils-underground-drone-base-at-undisclosed-location-3018421

May 28 – Iranian state television on Saturday broadcast footage of an air force base for drones under the Zagros mountain range in the west of the country.

The exact location of the base was not revealed, although the TV reporter said he travelled on a helicopter for nearly 40 minutes from the city of Kermanshah to reach it.

Iran started developing drones, or unmanned aerial vehicles (UAVs), in the 1980s during its eight-year war with Iraq.

The US and Israel accuse Iran of dispatching fleets of drones to its proxies in the Middle East, including Lebanon's Hezbollah movement, the regime of Syria's President Bashar al-Assad and Yemen's Huthi rebels.

Video aired on state television showed Iran's armed forces chief of staff General Mohammad Bagheri and army commander Abdolrahim Mousavi visiting the underground site.

"More than 100 combat, reconnaissance and attack drones belonging to the army are kept for operations in this base located in the heart of the Zagros mountains," the report said.

Bagheri, quoted by the official news agency IRNA, described the site as a "safe operational base for strategic drones".

"We never underestimate threats, we never assume the enemy is asleep, and we are constantly alert and vigilant," he added.

Mousavi told state television the base was located "several hundred metres (yards) underground", without giving further details.

State TV said the flagship of the fleet was the "Kaman-22", a drone equipped with missiles and able to fly at least 2,000 kilometres (1,245 miles).

The US Treasury slapped sanctions on the drone programme of Iran's Islamic Revolutionary Guard Corps in October last year. It accused the Guards of being behind a September 2019 drone strike on a Saudi oil refinery, as well as a July 2021 drone attack on a commercial ship off the coast of Oman that killed two crewmen. Iran denied the charges.

How is robotics innovation progressing in the military industry?

Source: https://www.army-technology.com/analysis/how-is-robotics-innovation-progressing-in-the-military-industry/

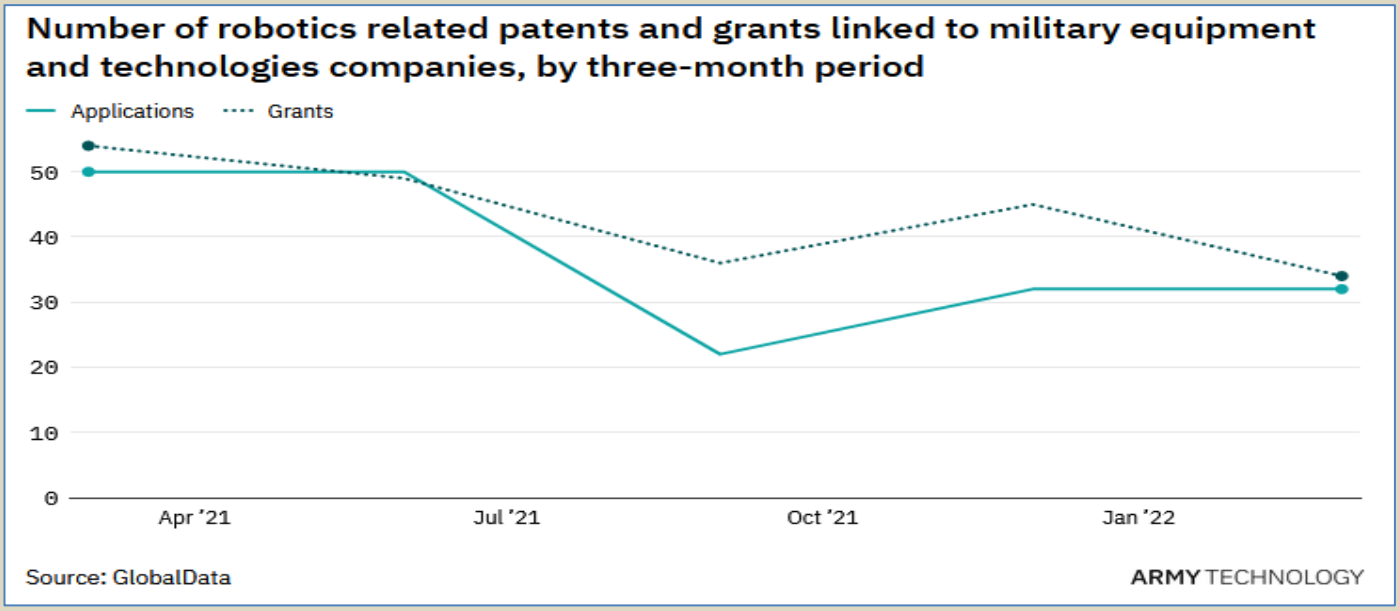
June 01 – Research and innovation in robotics in the military equipment and technologies sector has stagnated in the last quarter. The most recent figures show that the number of robotics related patent applications in the industry stood at 32 in the three months ending March – down from 50 over the same period in 2021.

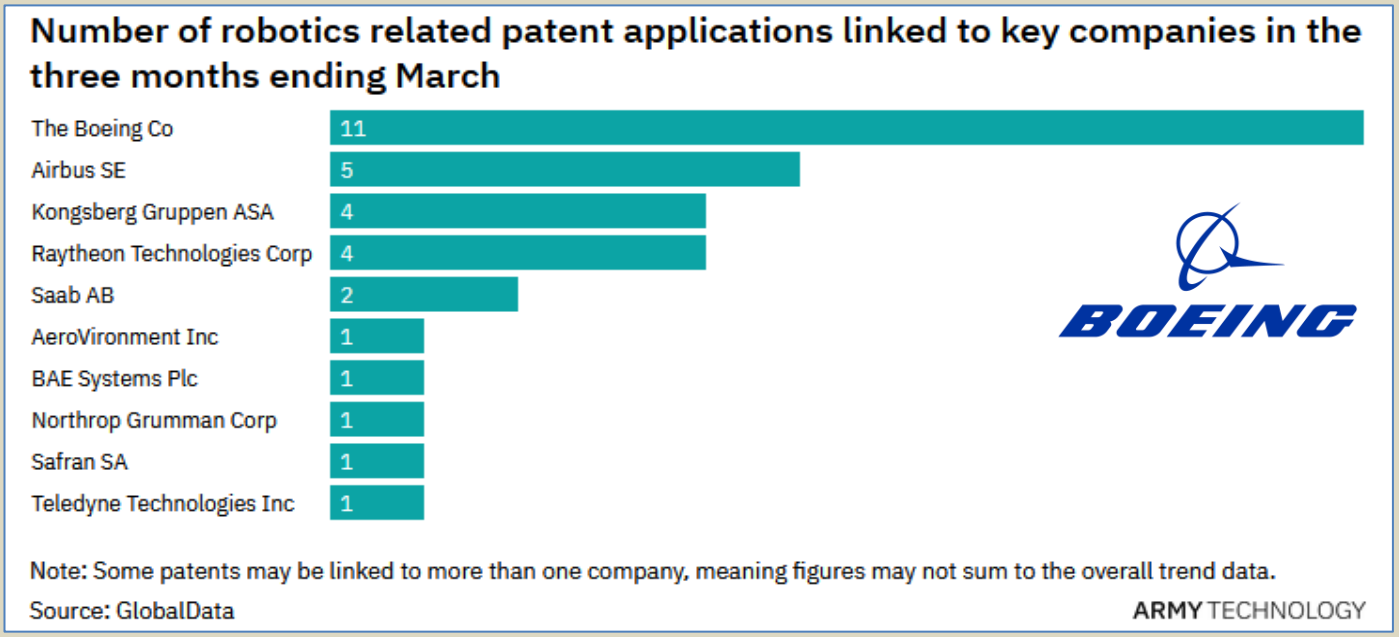
Figures for patent grants related to robotics followed a similar pattern to filings – shrinking from 54 in the three months ending March 2021 to 34 in the same period in 2022.

The figures are compiled by GlobalData, who track patent filings and grants from official offices around the world. Using textual analysis, as well as official patent classifications, these patents are grouped into key thematic areas, and linked to key companies across various industries.

Robotics is one of the key areas tracked by GlobalData. It has been identified as being a key disruptive force facing companies in the coming years, and is one of the areas that companies investing resources in now are expected to reap rewards from.

The figures also provide an insight into the largest innovators in the sector.





Boeing was the top robotics innovator in the military equipment and technologies sector in the latest quarter. The US-headquartered company filed 11 robotics related patents in the three months ending March. That was down from 20 over the same period in 2021. It was followed by Netherlands-based Airbus with five robotics patent applications, Norway's Kongsberg Gruppen with 4 applications, and US-based Raytheon Technologies with 4 applications.

Phoenix Ghosts are part drones, part missiles. How does that change combat?

By Dan Gettinger

Source: https://thebulletin.org/2022/06/phoenix-ghosts-are-part-drones-part-missiles-how-does-that-change-combat/

.

June 01 – On April 21, the US Defense Department announced an $800 million military assistance package to Ukraine that included over 121 Phoenix Ghost drones. This previously unknown, one-time-use weapon is designed primarily to attack targets, though it is also capable of conducting non-lethal missions, according to John F. Kirby, a Pentagon spokesperson. Kirby likened the drone to the AeroVironment Switchblade—a loitering munition. Such weapons combine the maneuverability, usability, and flight time of a drone with the lethal effects of a missile.

A US Marine launches a lethal miniature aerial missile system during an exercise at Marine Corps Base Camp Pendleton, Calif. on Sept. 2, 2020. Credit: Jennessa Davey, US Marine Corps

In recent years, the number of countries producing loitering munitions has more than doubled from fewer than 10 in 2017 to nearly two dozen today. Loitering munitions are increasingly integrated into a variety of air, ground, and sea vehicles and are among the technologies that military planners believe could transform ground combat. Their growing access and wide applicability present challenges to longstanding beliefs about precision weapons.

The category of loitering munitions includes a diverse group of aircraft, ranging from small gun- and hand-launched drones to those weighing as much as 200 kilograms (440 pounds). Initially conceived as an anti-radar weapon, loitering munitions are today meant to attack a variety of other battlefield targets such as enemy personnel, armored vehicles, ships, and even adversary drones.

The Phoenix Ghost is produced by the California-based Aevex Aerospace and was designed to help the Ukrainian military confront Russia in the Donbas region, according to Kirby. The 645th Aeronautical Systems Group led the effort to create the Phoenix Ghost for Ukraine, according to Defense Department officials. (The 645th is the successor to a program known as Big Safari, which contributed to the development of first military combat drones in the 1950s.)

Though the Defense Department has not yet elaborated on the Phoenix Ghost's dimensions or performance specifications, journalists have uncovered some information. The Phoenix Ghost can take off vertically and operate at night, according to *Politico*. It is also reportedly capable of attacking medium-armored targets and flying for six hours or more. If true, the Phoenix Ghost may be among the largest loitering munitions, one able to carry enough fuel

and payload to target far-away armored vehicles. Of the dozens of loitering munitions on the market today, only a handful claim an endurance of more than two hours. Still, the Phoenix Ghost's operational capabilities remain ambiguous.

The growing prominence of loitering munitions

In addition to the Phoenix Ghosts, the United States is sending more than 700 Switchblade loitering munitions to Ukraine. These orders appear to be for the lightweight Switchblade 300, though they may include the Switchblade 600—a heavier variant with a larger warhead, according to *Bloomberg*. The Defense Department has also ordered an unknown number of AeroVironment RQ-20 Puma AE surveillance drones for Ukraine. These small drones are launched by hand.

The United States often provides allied militaries with security assistance in the form of surveillance drones like the Puma. But Washington does not often offer loitering munitions; other than the US military and Ukraine, only the United Kingdom appears to have acquired the Switchblade.

The US military has purchased hundreds of Switchblades in recent years. The Army introduced the Switchblade 300 in 2012 and has since selected the Switchblade for its Lethal Miniature Aerial Munition System program. The Marine Corps and US Special Operations Command have also ordered a limited number of Switchblades.

Although the Switchblade is predominantly viewed as an infantry weapon, AeroVironment has lately integrated the drone into a variety of air and ground vehicles. Last year, AeroVironment launched a Switchblade 300 from a Jump 20 drone, which is intended to replace the Army's aging RQ-7 Shadow. Also in 2021, Kratos launched a Switchblade from an Airwolf drone, and General Dynamics unveiled a tracked robotic vehicle that can deploy 50 Switchblades.

The Switchblade's increasing ubiquity is emblematic of the Defense Department's widening embrace of loitering munitions. The Army's Air-Launched Effects and Marine Corps' Organic Precision Fires programs envision a future in which air, ground, and sea vehicles will serve as launch platforms for drones, namely loitering munitions. The US Special Operations Command also has several programs aimed at procuring loitering munitions for ground and maritime platforms.

Loitering munitions beckon organizational change

In March, Gen. David H. Berger, commandant of the Marine Corps, touted the advantages of loitering munitions. "This is the first time the infantry on the ground can strike targets beyond the range of their organic mortars [and] artillery with precision," Berger said, adding that loitering munitions offer ground forces the "power of an air wing in your hands."

Loitering munitions are among the core enabling technologies underpinning Berger's sweeping, much debated vision for Force Design 2030, the Marine Corps' modernization plan that was unveiled in March 2020. This plan aims to transform the Marine Corps into a more agile, expeditionary force by eliminating its fleet of battle tanks. It would also reduce tube artillery in favor of long-range precision firepower in the form of rockets, missiles, and loitering munitions.

Force Design 2030 has the potential to usher in major changes to the organization of Marine infantry units. The plans for infantry companies and battalions, which continue to undergo experimentation, could see loitering munitions largely supplant the longstanding 60-millimeter mortar. Loitering munitions will provide small units with the "the close-combat lethality enhancements long-envisioned by infantry Marines," according to the US Marine Corps. In its 2023 fiscal year, the Marine Corps will initiate the Organic Precision Fires Light initiative to evaluate lightweight, portable loitering munitions.

"An investment in loitering munitions for our infantry companies will exponentially increase their lethality," Maj. Gen. Julian D. Alford, head of Marine Corps Training Command, wrote in February's *Marine Corps Gazette*. "These capabilities will also enable the company commanders to shorten kill chains in support of the maneuver elements while, importantly, maintaining all-weather organic fires capabilities with ranges that extend dozens of miles."

Infantry-carried loitering munitions are but one element of the Marine Corps' plans for the weapons. The other track, known as Organic Precision Fires-Mounted, integrates loitering munitions into light armored vehicles, as well as future platforms like small autonomous boats. The Marines awarded Israel's UVision Air a contract in June 2021 to supply the Hero-120, a loitering munition roughly midway between the size of a Switchblade 300 and Switchblade 600, for this program.

A global phenomenon

The Marine Corps and Berger have repeatedly cited the use of loitering munitions in recent military conflicts as evidence of an urgent need to transform the service. In testimony before the Senate Armed Services Committee in June of last year, Berger attributed Azerbaijan's success in the Second Nagorno-Karabakh War in 2020 to its "precision strike regime to include swarms of loitering munitions and lethal unmanned systems."

The effect that drones and loitering munitions have had on the conduct of military operations in recent armed conflicts remains contested. Still, these systems are providing state and non-state actors with a slate of advanced capabilities. In the war in Nagorno-Karabakh,

Azerbaijan is believed to have used four types of loitering munitions acquired from four manufacturers in two countries.
Increasingly, producers are offering families of loitering munition solutions, with individual aircraft designed to meet specific operating requirements. Poland's WG Group Warmate series, for example, includes five systems, and Israel's UVision's Hero series features nine. Events like the 2020 conflict between Armenia and Azerbijian and the emergence of new producers in the Middle East and Asia are adding to the demand for loitering munitions. Illicit transfers of loitering munitions from states such as Iran to non-state actors and research and development partnerships like that announced last year between Israel Aerospace Industries and South Korea are also contributing to the sustained spread of these weapons.
The ecosystem of armed drones has changed radically since the General Atomics Predator conducted its first missile launch just over two decades ago. Bomblet-dropping quadrotors and lightweight precision munitions have contributed to the democratization and miniaturization of the armed drone. The emerging popularity of loitering munitions represents a further acceleration of these trends, creating new challenges for those who wish to manage drone proliferation.

Dan Gettinger is the director of publications and communications at the Vertical Flight Society and a researcher specializing in uncrewed systems. He is the author of *Unmanned Combat Aerial Vehicles: Current Types, Ordnance and Operations* and *"The Drone Databook" and* a founder of the Center for the Study of the Drone at Bard College.

You can now buy a co-ordinated multi-drone swarm in a box

Source: https://newatlas.com/drones/red-cat-drone-swarm-product/

Teal's Golden Eagle is one of very few drones that are approved by the US DoD (Teal Drones / Red Cat Holdings)

June 02 – Puerto Rico-based Red Cat Holdings has announced what it believes is the first and only commercially available multi-drone swarm system, allowing several DoD-approved drones to perform coordinated tasks under the control of a single pilot.
Red Cat is an umbrella company that owns several drone-related businesses. The best known is probably Fat Shark, which manufactures low-latency FPV goggles, but it also owns

Teal Drones, which produces a fully American-made quadcopter drone called the Golden Eagle, which is one of only a small handful of drones approved under US Department of Defense (DoD) guidelines.
China, through DJI and a number of other fast-moving companies, well and truly caught the USA with its pants down as drone technology began to take off in the last decade, thoroughly dominating the market with cheap, reliable and beautifully put together consumer and commercial drone products.
China has owned this market so comprehensively that American institutions like the FBI and NYPD have been buying DJI drones for surveillance work, despite the Department of Defense labeling them "potential threats to national security" that could possibly feed critical data back to China if weaponized remotely in a conflict situation. Machines like the Golden Eagle aim to eliminate this threat, being fully designed and built in the US.
Now, Red Cat is attempting to get out in front of the next wave of commercial drone technology. "There is really almost no use case," says Teal Drones CEO George Matus in a press release, "where I think to myself, one drone is now enough. Every use case can benefit from having a swarm of drones."
Drone swarms are most prominent nowadays as entertainment spectacles, each drone providing a point of light that can move in three-dimensional space to create complex shapes and dazzling effects. But Teal believes that intelligently co-ordinated swarms can do the job quicker and more effectively in a lot of use cases, so it's created a product called 4-Ship to give operators a ready-made swarm of up to six drones that can work on a task in concert, with just one pilot at the helm.
Only four drones will be active at a given time, the other two being there on standby ready to sub in for the others and maintain the swarm as battery life begins to run down. A special 4-Ship controller is capable of displaying four video feeds at once, giving 360-degree views of a target if required, and has been designed to be simple and intuitive to use.

The controller can handle four video streams at once, giving you 360-degree views of a target (Teal Drones / Red Cat Holdings)

Surround surveillance for military, government and public safety organizations will be one of the first applications for these swarms, with the ability either to surround an enemy target, or face outwards to provide 360-degree defensive views of a friendly position. The drones can easily be placed in other advantageous spots to create a kind of aerial CCTV system monitoring building exits and the like.
Alternatively, in a persistent surveillance/ reconnaissance mission, a single drone can be set to track a target or location, and the 4-Ship system will rotate drones in as battery levels drop, to make sure there's always an eye in the sky.
Another easy win for a swarm system comes in automated surveying and area photography missions, in which the 4-Ship system can coordinate the entire task between multiple drones, automatically stitching together images from across the swarm and effectively getting these jobs done in a quarter of the time. With manpower typically being the most expensive component of many drone operations, the system could pay for itself on that basis alone.
"With 4-Ship, we have successfully integrated the human/machine interface with an embedded autonomy engine that offers additional intelligence and surveillance capabilities from a single pilot and controller," said Steve Jacobson, CEO of autonomous software developer Autonodyne, LLC, which collaborated with Teal Drones on this project. "The ease of use and multitude of applications makes the 4-Ship a next-generation drone system."
Teal says it's got the shippable product on hand and it's opened up orders for deliveries to begin in the fall.

●▶ **Source:** Teal Drones

EASA - Drone Incident Management at Aerodromes

Unmanned Aircraft Systems (UAS), commonly referred to as "drones", represent tremendous economic and innovation opportunities. It is estimated that by 2035, the European drone market will generate a value of EUR 10 billion a year2. With an ever-growing

number of drones taking to the skies, their safe and secure integration into the airspace poses the main challenge to enabling the market. With this challenge in mind, it is noted that the number of incidents involving drones has steadily increased in Europe and around the globe over recent years. In most cases, unauthorized drones are being reported near or inside the perimeter of airports3 (or in its immediate proximity) or in the arrival and departure paths of runways, which aircraft use at landing or take-off. Given the potential for disastrous effects following a collision between a manned aircraft and a UAS 4, aerodrome operators and Air Navigation Service Providers (ANPSs) may, in managing such an incident, often have no option but to stop or restrict runway operations, leading to severe disruptions to air traffic.

US mass shootings prompt development of Taser-wielding drone

Source: https://newatlas.com/drones/mass-shootings-taser-drone/

June 03 – It's a sad fact that mass shootings have become an all-too-common occurrence in the US. Defense tech company Axon has announced what it states will be a new means of resolving such incidents quickly and *relatively* safely, utilizing a drone equipped with a Taser.

Axon, the Arizona-based firm that manufactures the Taser, announced its plans to develop the drone this Thursday (June 2nd).

Few details on the aircraft itself have been released at this point, other than the facts that it will be a remotely controlled quadcopter, equipped with one of the company's drone-specific Axon Air video cameras and a miniaturized version of the Taser electroshock weapon.

The Taser works by firing two small darts, each of which remains connected to the main device by a thin wire. When those darts strike a person (such as an active shooter), they deliver an electric shock which disrupts the individual's nervous system. Ideally, this just results in the person being temporarily incapacitated, although a number of Taser-related deaths certainly *have* been reported.

The drone will be part of a larger system, which will also include a network of security cameras – in schools, businesses and other locations – along with a VR-based training program designed to teach first responders how to deal with active shooters. It is hoped that this combined approach could ultimately allow authorities to "stop mass shootings in less than 60 seconds."
Project partners include Fusus, which is developing the camera network, along with DroneSense, which is working on the real-time drone control system.

●▶ **Source:** Axon

Israel Sets to Deploy Laser Weapons to Counter Missiles, Rockets, and Drones

Source: https://www.homelandsecuritynewswire.com/dr20220606-israel-sets-to-deploy-laser-weapons-to-counter-missiles-rockets-and-drones

June 06 – Israel Ministry of Defense (MOD) a few weeks ago announced that after more than two decades of research and development, Israel Defense Force (IDF) has now tested an operational laser weapon – called Iron Beam — which, in tests, proved capable of destroying missiles, rockets, mortars, and drones in flight. The MOD said that the most recent tests took place in northern Israel, near the border with Lebanon, and that the success of the laser system in destroying a rocket, a mortar, and a drone, was welcomed by a standing ovation of senior military commanders and government officials witnessing the test.
Israel's Prime Minister Naphtali Bennett described the weapon as offering the region a "strategic turning point," and said his government was committed to "surround Israel with a laser wall."

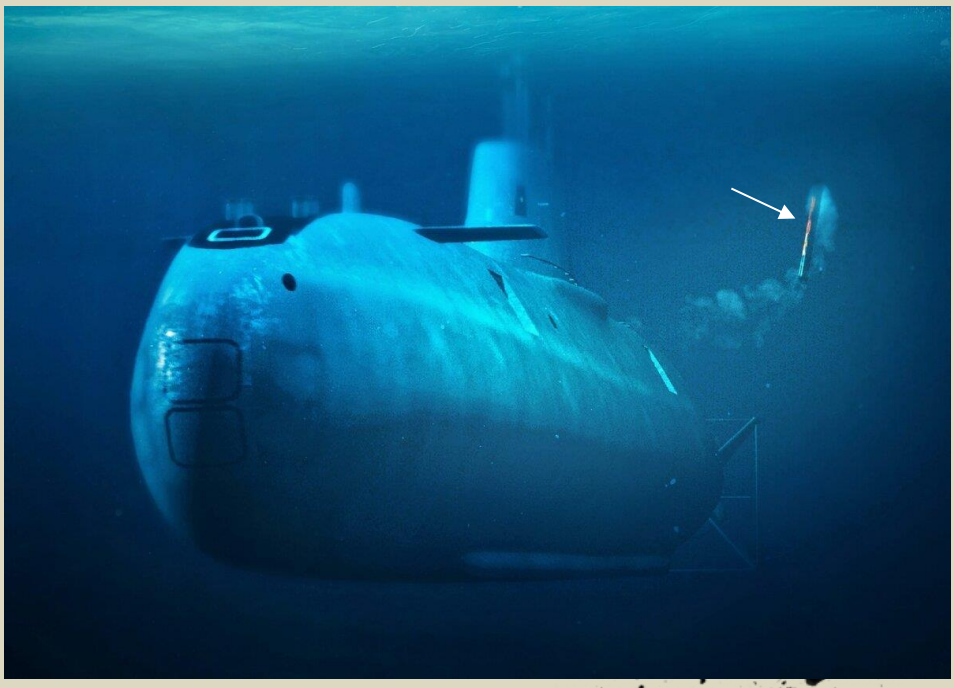
Engineers and technical experts who were involved in developing the weapons, and outside expert observers, said it would be at least 2-3 years, if not more, before the system is ready to be operationally deployed. Israeli experts said that the system, when deployed, would initially likely be limited to protecting Israel from rockets.
Israeli officials did not say whether the system would be effective against more advanced, precision-guided missiles, which Iran has been supplying Hezbollah with.
Laser weapons have long been the stuff of science fiction films and video games, but the last few years saw more and more laser system developed and deployed. One example is the Helios, developed by Lockheed Martin, which is being deployed on U.S. Navy ships. The U.S. Army is working on laser system aiming to shoot down cruise missiles.
Israeli officials said that the **Iron Beam system** would be a complement to existing antimissile and anti-rocket systems such as Iron Dome and David's Sling.
Israel's existing defensive systems rely on kinetic energy: the system's radars identify an enemy missile and chart its trajectory, and the Iron Dome or David's Sling anti-missile missile slams into the enemy missile and destroys it.

The laser system focuses an intense laser beam on a single point on the enemy's projectile, and heats it up until it explodes in midair. The MOD said that during the March in northern Israel, the laser system intercepted threats within a few seconds after detection — and at a distance of up to 10 kilometers. In 1983 President Ronald Reagan launched the Strategic Defense Initiative (SDI, aka "Star Wars"), which aimed, in his words, to make nuclear missiles "impotent and obsolete." The initial idea for SDI, urged on the president by physicist Edward Teller, was to use small nuclear explosions in space to generate intense laser beams which would hit hundreds of Soviet missiles, each carrying between three and ten nuclear warheads, as they emerged from their silos in Russia.
By 1993, after spending more than $200 billion, the laser-based idea was abandoned as impractical.
But the idea of developing laser weapons on a more modest scale, and which would not rely on nuclear explosions, continued in other programs. Twenty-five years ago, Israel and the United States worked on the Nautilus, which relied on chemical reactions to produce high-energy laser system with less ambitious range, with the aim of destroying rockets in flight. The Nautilus was abandoned in 2005 because the large chemical tanks required for each individual made the entire system unwieldy, in addition to being exceedingly vulnerable to enemy attacks. The chemicals were also corrosive and toxic.
The current Iron Beam system uses solid-state laser, which only needs large amounts of electricity to function.
Israeli engineers involved in developing the system say that another breakthrough which enabled them to achieve a high success rate was combining and concentrating many high-intensity laser beams at a single specific point on an aerial target.
The IDF has recently awarded a $100 million contract to Rafael Advanced Defense Systems Ltd., state-owned defense contractor working with technology for more than two decades. The company says that it was only in the last two years that the company's engineers have been able to resolve some of the major complications, including the size of the system and its low effectiveness.
"We had a problem with energy, tracking and the ability to pierce the atmosphere," said Michael
Israeli officials say Iron Beam's main advantage will be its cost. **According to the company, each interception of an enemy projective by Iron Beam would cost about $3.50.** In comparison, a single interception by the current defense systems, Iron Dome and David's Sling, cost tens of thousands of dollars.
Also, **Israel's main antimissile defensive system, Iron Dome, is heavily subsidized by the United States, which allocated an additional $1 billion dollars to the weapon in the 2022 budget.** The American support for Iron Beam is very small, and Israel, in return for this support, is sharing its laser advances with the United States.
Israel is planning to deploy the laser technology first around the Gaza Strip, before deploying it in other parts of the country.

First quadcopter drone that can be launched from a submarine underwater

Source [**+video**]: https://newatlas.com/military/spearuav-drone-submarine-underwater-launch/

SpearUAV has released its Ninox 103 UW Sub-to-Air encapsulated autonomous quadcopter, which it claims is the first loitering drone that can be launched from a submarine and other submerged platforms for immediate beyond-line-of-sight situational awareness.
With their ability to submerge, submarines have a major strategic and tactical advantage. However, from their inception they've also suffered since from the disadvantage of not being able to see what's going on above the waves beyond the horizon of a periscope.



The Ninox 103 UW deploying in its capsule (SpearUAV)

For this reason, for over a century, submariners have experimented with a number of ways to extend their view. With varying degrees of success, kites, gyrocopters,

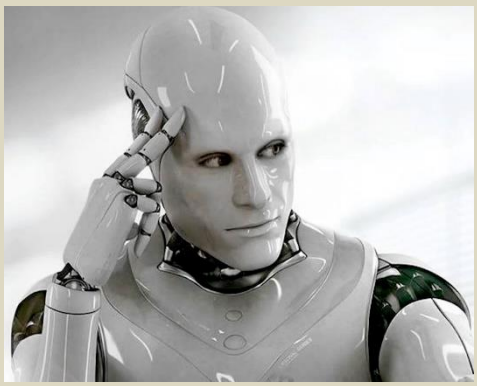
and even airplanes have been launched from submarines, but all of these had the drawback of the boat needing to surface for them to be deployed.
In recent years, navies have looked to drones that can be launched underwater to act as a reconnaissance platform. However, these have tended to be fixed-wing aircraft, while the Ninox 103 is based on a quadcopter design that allows it to loiter in place by hovering.

The Ninox 13 UW deployed (SpearUAV)

According to SpearUAV, the Ninox 103 is stored in a capsule that can be deployed from a submarine. This capsule floats to the surface and can remain dormant for up to 24 hours before the ruggedized, maritime-hardened drone launches.
Once airborne, the Ninox 103 has a range of 10 km (6 miles) and an endurance of 45 minutes. With a payload of 1 kg (2.2 lb), the drone has low acoustic, thermal, and visual signatures, and features Electro-Optical/Infra-Red (EO/IR) sensors for reconnaissance and automatic target acquisition using its open-architecture artificial intelligence system. Communications with the submarine, other platforms, or special forces teams ashore use encrypted communications, 3rd-party data integration, and cross-domain connectivity.
"The first technological development of its kind in the world, the Ninox 103 Sub-to-Air has been developed in response to the needs of Spear's customers worldwide for a drone capable of underwater launch," says Colonel (Retired) Gadi Kuperman, Founder & CEO of SpearUAV. "The system has been successfully tested, and Spear is collaborating with a number of defense companies as it continues to work on new developments."

read.

Is LaMDA Sentient? — an Interview




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

EU preparedness and responses to Chemical, Biological, Radiological and Nuclear (CBRN) threats

Authors:

- Alexandra RIMPLER-SCHMID (Ecorys; project leader and coordinator)
- Dr Ralf TRAPP (International Disarmament Consultant),
- Professor Sarah LEONARD (University of the West of England),
- Professor Christian KAUNERT (University of South Wales),
- ► Yves DUBUCQ (Director of the International CBRNE Institute, CEO Sphynx Development & Consultancy Former Comdr of the JCBRNC (Joint CBRN Centre) Belgium),
- Colonel (r) Claude LEFEBVRE (Expert consultant in CBRN defence technologies),
- Hanna MOHN (Ecorys)

Source: https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653645/EXPO_STU(2021)653645_EN.pdf

July 2021 – This study on 'EU preparedness and responses to Chemical, Biological, Radiological and Nuclear (CBRN) threats' was requested by the European Parliament's (EP) Subcommittee on Security and Defence (SEDE) in the context of, but not limited to, the ongoing COVID-19 pandemic. Building on reports and expert input, this study first provides an update of the current level of each of the C, B, R and N threat elements, including the type of actor from which such threats might stem. It furthermore takes stock of the existing preparedness and response mechanisms and matches these against the updated threat landscape to determine the current state of play of the EU's response tools and its remaining gaps where improvement may be needed. The study puts forward a number of recommendations on specific issues. The core of the recommendations builds on using a 'Team Europe' approach to create and maintain a strong task force based response capacity, with additional authority and competence given by EU Member States to the EU. This would enable the EU to better support and manage an EU-wide crisis response in the CBRN field in a timely and effective manner.

Hazardous Materials (HAZMAT) and Chemical, Biological, Radiological and Nuclear (CBRN)

Information last updated: 1 February 2022

Source: https://www.england.nhs.uk/ourwork/eprr/hm/

On this page you will find information about:

- Guidance for the initial management of self presenters from incidents involving hazardous materials
- Chemical incidents: planning for the management of self-presenters in healthcare settings
- Powered Respiratory Protective Suit (PRPS)
- Initial Operational Response (IOR)
- UK Reserve National Stock for Major Incidents – How to access stock in England
- Patient Group Directions


Summer 2022
GREECE: The ultimate destination

Because international CBRNE First Responders need a common roof!

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