03\23

ICI

# C2BRNE DIARY

Dedicated to Global First Responders

March 2023

## Psychological Desensitization of First Responders

**PART B**

An International CBRNE Institute publication

International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

# DIRTY R-NEWS

C2BRNE DIARY

# Russia's Grip on Nuclear-Power Trade Is Only Getting Stronger

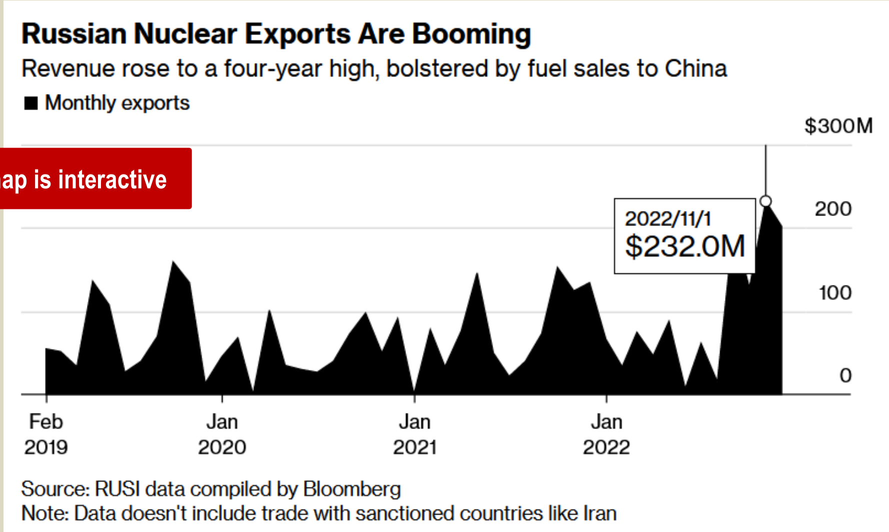
**By Jonathan Tirone**

Source: https://www.bloomberg.com/news/features/2023-02-14/russia-s-grip-on-nuclear-power-trade-is-only-getting-stronger#xj4y7vzkg

Feb 14 – Russia's nuclear exports have surged since the invasion of Ukraine, boosting the Kremlin's revenue and cementing its influence over a new generation of global buyers, as the US and its allies shy away from sanctioning the industry.

Exclusive trade data compiled by the UK's Royal United Services Institute show that Russian nuclear fuel and technology sales abroad rose more than 20% in 2022. Purchases by European Union members climbed to the highest in three years. From Egypt and Iran to China and India, business is booming. The trade brings in plenty of money already, but that's not the full measure of its importance. Every time the Kremlin's nuclear giant Rosatom PJSC agrees to build a new reactor, it locks in cashflows — and political clout — for potentially decades ahead.

The map is interactive



Source: RUSI data compiled by Bloomberg
Note: Data doesn't include trade with sanctioned countries like Iran

Atomic commerce creates relationships that last. It involves large upfront costs — with Russia usually providing the credit — and long-term agreements to service plants, train their operators and replenish fuel. That kind of financial and technical collaboration can strengthen diplomatic ties too.

"This is part of the great-power competition that we're in right now," says Edwin Lyman, director of nuclear-power safety at the Union of Concerned Scientists in Washington. Russia's leaders "see nuclear trade as a way to bolster alliances."

Bushehr Nuclear Power Plant, Iran, October 2022. Rosatom helped finish construction of Iran's first reactor in Bushehr and has now been contracted to build two more units outside of the Persian Gulf port – Satellite image ©2023 Maxar Technologies

## 'Reticent to Sanction'

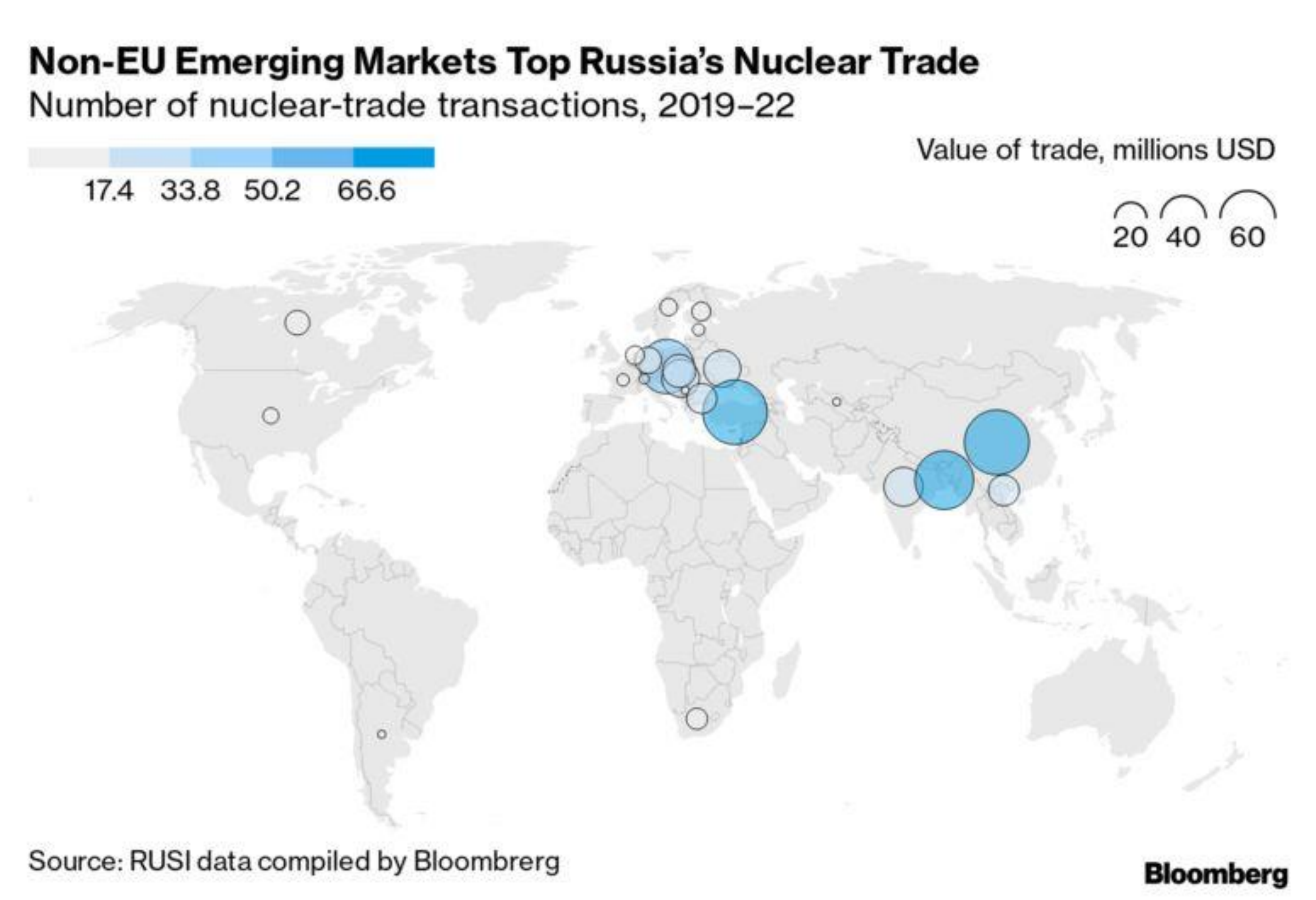
The task is made easier by a dearth of competition. Russia continued investing in nuclear-fuel and technology manufacturing after the Soviet Union collapsed, even as the industry atrophied in other parts of the world.

That's one reason why the US and its European allies — who've been weighing sanctions against the Russian nuclear company since early in the war — haven't followed through. The concern is that shutting off their own nuclear industries from Russian supplies would be too economically painful.

Rosatom provides about one-fifth of the enriched uranium needed for the 92 reactors in the US. In Europe, utilities that generate power for 100 million people rely on the company.

The RUSI data is sourced from a third-party commercial provider and based on Russian customs records, says Darya Dolzikova, the think-tank's sanctions analyst. She says the figures are incomplete and don't capture business with sanctioned countries like Iran. Numbers were validated where possible by comparing them with publicly available export information.

"Nuclear energy projects have very long timelines, so it is difficult to draw any definitive conclusions," she said. "But the data does point to a prioritization of markets that may be reticent to sanction Russian nuclear energy exports or entities."


Non-EU Emerging Markets Top Russia's Nuclear Trade
Number of nuclear-trade transactions, 2019–22
17.4
33.8
50.2
66.6
Value of trade, millions USD
20
40
60
Bloomberg

Source: RUSI data compiled by Bloombreg

The figures show NATO members including Bulgaria, the Czech Republic, Hungary and Slovakia continued to purchase Rosatom fuel last year, amid Ukrainian pleas to shut down the trade after Russia hijacked Europe's biggest power plant.

"Rosatom receives billions of dollars every year from their business abroad," says Petro Kotin, the president of Ukraine's nuclear utility Energoatom. "The money that they're receiving is financing the war." Ukraine imposed sanctions on Rosatom this month, and urged other nations to follow suit.

Even in Ukraine, though, nine reactors still under Kyiv's control rely on stockpiled Russian fuel. It's taken years of planning, aided by US advisers, to make the switch to Westinghouse Electric Co., says Kotin, and full diversification won't be possible for another three or four years.

Countries like Bulgaria, Finland and Slovakia have announced plans to swap suppliers too. That hasn't prevented Rosatom from expanding its European footprint.

Hungary is providing aid for two new reactors that were awarded to Rosatom without public tender. Russia is covering 80% of the cost with a 10 billion euro loan. By the time construction is completed next decade, the project will be one of eastern Europe's biggest foreign investments. Hungary is among the EU countries opposed to including nuclear fuel in the bloc's sanctions, while others such as Poland, Germany and the Baltic nations support the idea.

**'Geostrategic, Not Commercial'**

The data obtained by RUSI show that fuel supplies for aging reactors in former Soviet satellites accounted for almost two-fifths of Rosatom exports since 2019. But its fastest-growing markets lie further afield.

Rooppur Nuclear Power Plant, Bangladesh, in November 2022. Bangladesh's first atomic-power plant is due to begin generating electricity next year after Rosatom financed some 90% of the $13 billion project – Source: Google Maps

"This is a geo-strategic not a commercial technology," says Mark Hibbs, a Berlin-based nuclear analyst at the Carnegie Endowment for International Peace. "By providing state financing, Russia can take financial risk away from countries."

Rosatom chief Alexey Likhachev said this month that the company is in talks with about 10 countries on new projects, and three or four are close to signing inter-government deals. In all the countries where Rosatom is already building nuclear plants, "everything is on track," he said.

Rosatom isn't handicapped by non-proliferation rules imposed by the US Department of Energy. In India, under western trade restrictions since testing a nuclear weapon in 1974, Russia supplies nuclear fuel and is building two reactors scheduled to open in 2025. In China last year, Rosatom provided more than $375 million worth of fuel for a reactor that the US Department of Defense is concerned could bolster Beijing's nuclear-weapons stockpile.

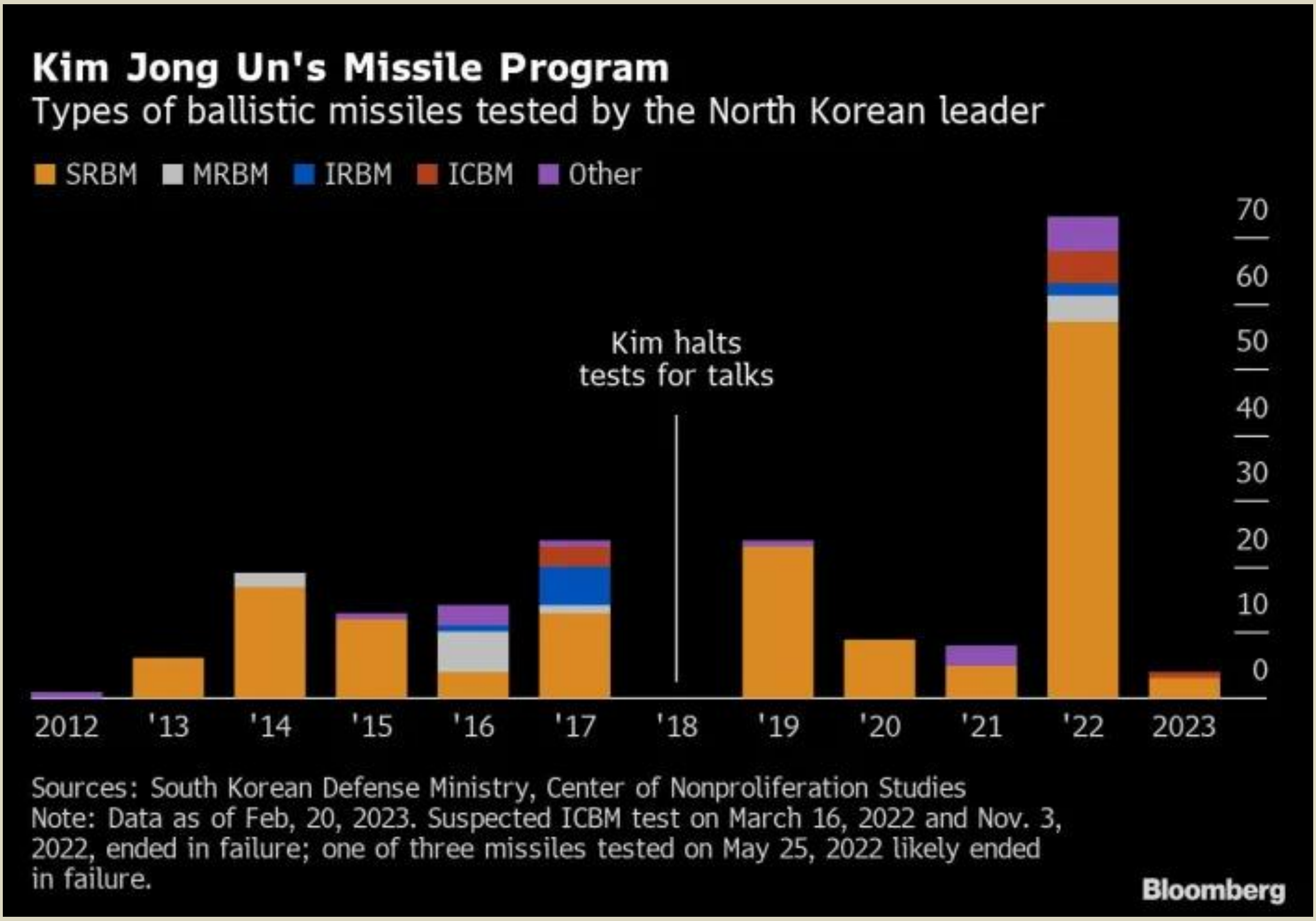
Akkuyu Nuclear Power Plant, Turkey, May 2022. Rosatom is poised to commission the first of four reactors on Turkey's Mediterranean coast in May – Satellite image ©2023 Maxar Technologies

South Africa, which has gotten visits from top US and Russian officials in the last few weeks, is a good example of the strategic dimension of atomic trade. In the only African nation currently operating nuclear-power reactors, the government last month allowed a pact with the US — which gave it access to fuel in exchange for non-proliferation guarantees — to expire. That's opened yet another door for Rosatom.

"They had a lot of hope in the past to do in South Africa what they are doing in Egypt and Turkey, but on a bigger scale," says Hartmut Winkler, an energy researcher at the University of Johannesburg. "Rosatom is keen for contracts that give them influence, especially in countries that proclaim neutrality when it comes to Ukraine."

## US, South Korea Plan for Potential Nuclear Strike by North Korea

Source: https://news.yahoo.com/us-south-korea-discuss-plans-000756829.html


Kim Jong Un's Missile Program

Types of ballistic missiles tested by the North Korean leader

Sources: South Korean Defense Ministry, Center of Nonproliferation Studies
Note: Data as of Feb, 20, 2023. Suspected ICBM test on March 16, 2022 and Nov. 3, 2022, ended in failure; one of three missiles tested on May 25, 2022 likely ended in failure.

Feb 24 – The US and South Korea held discussions over ways they would respond to possible nuclear attacks by North Korea, which has been steadily building up its capability to deliver a credible atomic strike against the two.

The so-called table-top exercise held in Washington focused on hypothetical scenarios of North Korea's use of nuclear weapons, the Pentagon said in a statement late Thursday. They were the first of their sort since South Korean President Yoon Suk Yeol took office about a year ago and bolstered joint military exercises with the US, a move that angered Pyongyang and led it to step up its provocations.

"Both sides discussed various options to demonstrate the Alliance's strong response capabilities and resolve to respond appropriately to any DPRK nuclear use," the Defense Department said, referring to North Korea by its formal name.

The US reiterated that any nuclear attack by North Korea against the US or its allies would "result in the end" of Kim's regime. The South Korean delegation also visited a US nuclear submarine facility in Georgia to see military assets the US could use against North Korea, which are aimed at deterring Pyongyang from launching a strike.

North Korea has ratcheted up tensions in the past week by test-firing an intercontinental ballistic missile designed to deliver a nuclear warhead to the US mainland, and firing two short-range missiles a few days later. Kim Yo Jong, the influential sister of the leader, threatened to turn the Pacific into a "firing range," in a hint the state could start testing whether its warhead designs can withstand the heat of reentering the atmosphere.

North Korea's official media said Friday the state tested four, long-range cruise missiles a day earlier that flew in figure-8 patterns for a distance of about 2,000 kilometers (1,240 miles) — a range that could hit almost all of Japan.

Cruise missiles are designed to fly low to the ground and avoid radar. They move far slower than ballistic missiles and there are no United Nations resolutions that ban Pyongyang from testing them.

"The drill clearly demonstrated once again the war posture of the DPRK nuclear combat force bolstering up in every way its deadly nuclear counterattack capability against the hostile forces," its Korean Central News Agency said.

The launch of the cruise missiles came shortly after the US, Japan and South Korea held a joint naval missile defense exercise in international waters.

North Korea for decades has called the joint exercises a prelude to an invasion and nuclear war and state media Friday carried a fresh threat from one of its top diplomats, who urged the US halt the exercises.

"If the US continues its hostile and provocative practices against the Democratic People's Republic of Korea despite our repeated protests and warnings, it could be regarded as a declaration of war against the DPRK," it quoted Kwon Jong Gun, director general of the Department of US Affairs of the Foreign Ministry, as saying.

Last year, Kim's regime test fired more than 70 ballistic missiles, the most in his decade in power and in defiance of UN resolutions that prohibit such launches. The North Korean leader has been modernizing his inventory of missiles over the past several years to make them easier to hide, quicker to deploy and more difficult to shoot down.

He also is poised to conduct his first test of a nuclear bomb since 2017. The US, Japan and South Korea has pledged a stern coordinated response if North Korea goes ahead the with blast.

**EDITOR'S COMMENT**: It would be reckless to strike both the US and S. Korea. US and nuclear allies will retaliate and N. Korea will become a radioactive field for decades – who cares about its population? Strike only S. Korea? The US might retaliate but it is not for sure – there is always sufficient arsenal to achieve a second strike against the US. The US is forcing S. Korea to go nuclear but this will take time and when they are about ready, N. Korea will attack conventionally – something that they can do at any given moment right now. Perhaps efforts to achieve peace might be better to avoid Armageddon. But again, peace is not a favorite option by the West (see the Taiwan case).

## Sheltering miles from a nuclear blast may not be enough to survive unless you know where to hide, new calculations show

**By Rupendra Brahambhatt**

Source: https://news.yahoo.com/sheltering-miles-nuclear-blast-may-115500093.html

Feb 25 – If a nuclear bomb were dropped in your city tomorrow, would you know where to take cover? Nuclear war is a terrifying thought, but for a team of researchers at the University of Nicosia in Cyprus, it's top of mind. In a recent study, the researchers calculated how the blast from a nuclear explosion could affect people sheltering indoors, and found that even if you're at a safe distance from the explosion to survive the blast, you may still be in immediate peril.

"It is important to understand the impact on humans indoors to provide recommendations for protecting people and assets," said co-author Dimitri Drikakis. "For example, we can design structures that offer more protection."

**Avoid hallways and doors. Seek out corners of windowless rooms.**

UNIVERSITY of NICOSIA

An illustration of the shockwave of a 750-kt nuclear bomb 10 seconds after detonation. The wave has already traveled 2.8 miles (4.6 km). I. Kokkinakis and D. Drikakis, University of Nicosia, Cyprus

When a nuclear bomb detonates, it generates not only radiation in the form of a bright, blinding light and scorching heat, but also powerful shockwaves that can travel for tens of miles.

It's these shockwaves that are potentially lethal for people at a safe enough distance from the fireball.

The team simulated a nuclear explosion from a 750-kiloton atomic bomb. For reference, the bombs the US dropped at Hiroshima was 15 kilotons and at Nagasaki was 25 kilotons. So, on average, that's about 37 times smaller than the bomb in the researchers' simulation. A warhead of this magnitude would likely obliterate everything within 2.5 miles, but people beyond that radius may stand a chance if they're sheltering in the right location of a sturdy structure.

Where that right location is, however, is where the researchers' results get interesting. "The explosion was simulated using high-resolution and high-order computational fluid dynamics," based on three decades of experiments and theory, Drikakis told Insider.

Using these models, they computed how the shockwave would move through buildings — including rooms, walls, corners, doors, corridors, windows, and doorways — at distances of 2.5 miles to 30 miles from the detonation site.

They reported that narrow pockets inside buildings like doorways and hallways could act like a windtunnel, accelerating the shockwave to dangerous pressures of up to 18 times a human's body weight — easily enough to crush bones.

"The most dangerous critical indoor locations to avoid are the windows, the corridors, and the doors," said co-author Ioannis William Kokkinakis.

The best location is in the half of the building farthest from the blast, in a room with no windows. But, "even in the front room facing the explosion, one can be safe from the high airspeeds if positioned at the corners of the wall facing the blast," Kokkinakis told Insider.

It's also worth noting that the building itself is important. You don't want to take cover in a log cabin, for example.

"As the paper noted, if you're too close to the blast there's not much that can be done. However, at a distance building structures particularly stone or concrete or other stout, noncombustible materials can provide some degree of protection from the blast," said Kathryn Higley, a professor of radiation biology at Oregon State University who was not involved in the study.

**Preparing for an uncertain future**

The researchers said they modeled the detonation of a 750-kiloton bomb after Russia's Sarmat, an ICBM the Kremlin test-fired last April. Russia's invasion of Ukraine has raised concerns that we may be inching closer to nuclear war, and one of their prime motivations for the study was "the growing rhetoric about the use of nuclear weapons," Drikakis said.

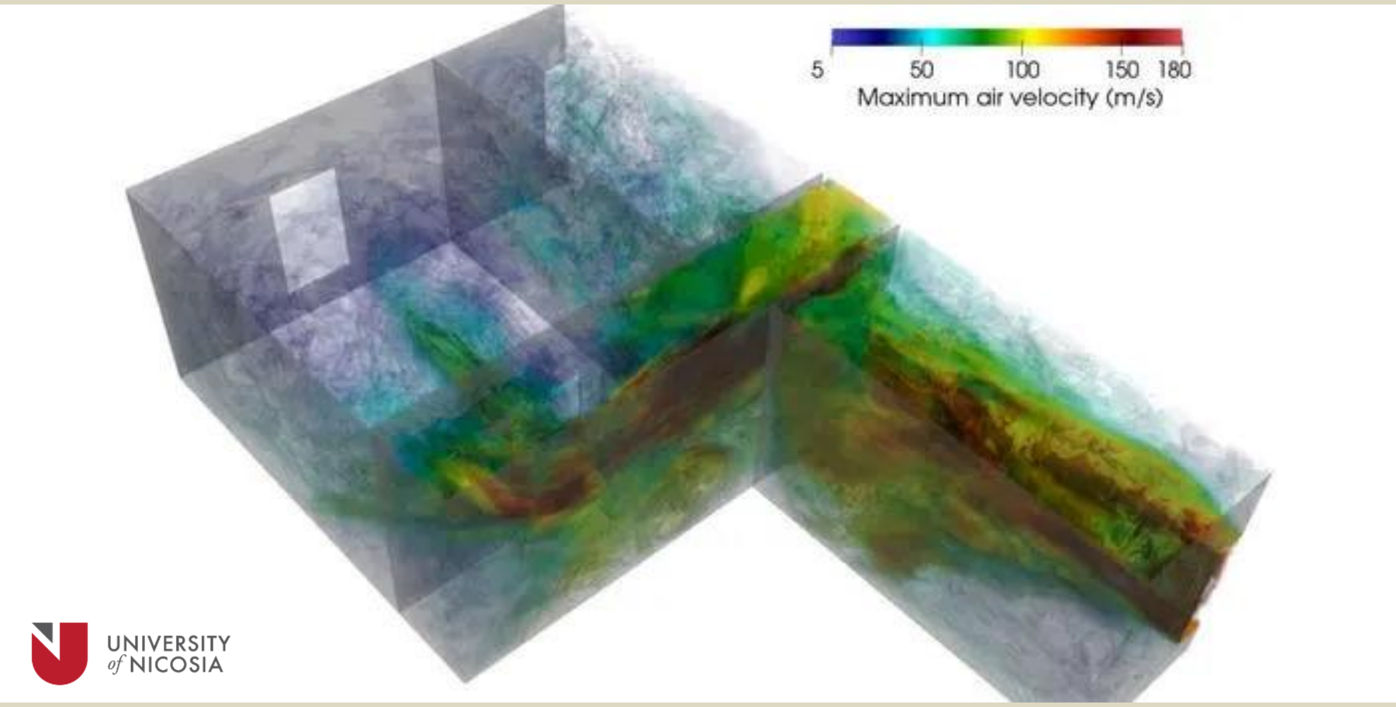


Illustration of how the shockwave would move through a room indoors with narrow corridors increasing the speed and pressure. I. Kokkinakis and D. Drikakis, University of Nicosia, Cyprus

"A nuclear war is a serious matter that will lead to widespread destruction. For several decades, the international community has considered that such a possibility will not arise. However, the rhetoric around the globe has changed," Drikakis said.

The authors believe these findings could help nuclear safety experts devise better strategies to mitigate the damage from atomic explosions and radiation leaks. They hope the results from the study might also guide the development of nuclear-blast-proof buildings in the future.

"The wide-scale implication of this research is that it can add to the understanding of how to best protect yourself in the event of a nuclear detonation," Higley said.

Never mind the nuclear fallout and apocalyptic lifestyle you may face after the fact. Surviving that is a different sort of study, entirely.

## Russian State-Run TV discusses possibility of nuclear strike on Yellowstone National Park

Source: https://www.marca.com/en/lifestyle/us-news/2023/02/24/63f8225722601dab268b45ba.html

Feb 23 – The discussion of a nuclear strike on Yellowstone National Park comes amidst heightened tensions between Russia and the United States

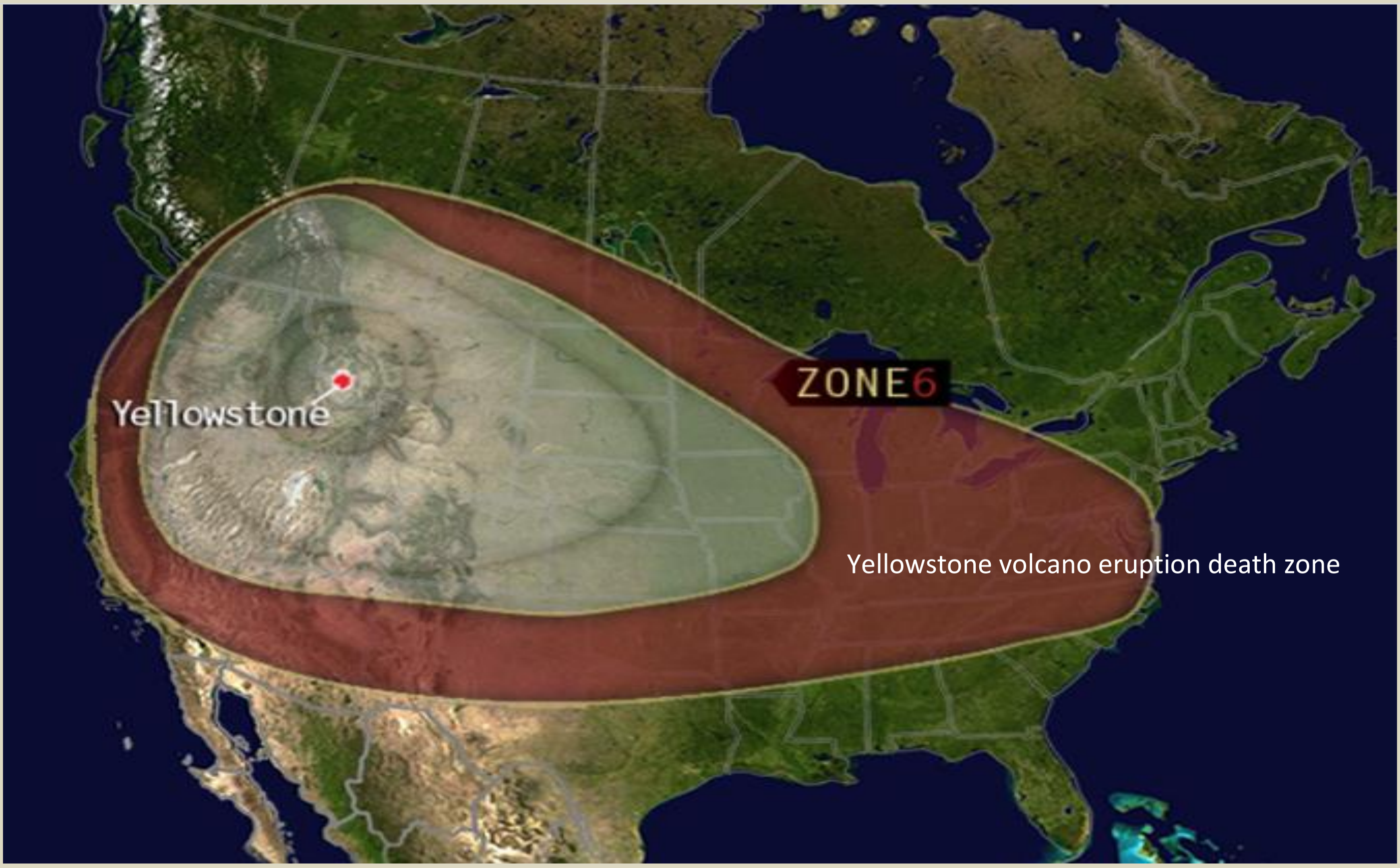
In a recent broadcast on **Russia's state-run TV,** a pundit discussed the possibility of **Russia** using a **nuclear Sarmat missile** to strike a volcano in **Yellowstone National Park.**

The news comes after **Russian President Vladimir Putin** announced that his country would be paying increased attention to strengthening its nuclear missiles based on land, sea, and air, with the **RS-28 Sarmat** intercontinental ballistic missiles set to be deployed this year.

The discussion was aired on host **Vladimir Solovyov**'s **Russia-1** program, and **Anton Gerashchenko**, an adviser to Ukraine's minister of internal affairs, posted two videos on Twitter of the conversation. During the program, retired Russian naval officer Konstantin Sivkov spoke about what he called a "special weapon."

According to **Sivkov,** the powerful Sarmat missiles can deliver "a large number of nuclear warheads to the target" and have the capability of "striking across the **South Pole."** He also stated that the **United States** is "**vulnerable**" to such a weapon, which he said "poses a threat" to the **Yellowstone volcano**.

**Could Russia really use nuclear weapons on Yellowstone?**



Yellowstone volcano eruption death zone

Poseidon stealth torpedo can be remotely placed near the Cascadia Subduction Zone and the San Andreas Fault to blast open the plates and practically sunk California!

The possibility of a nuclear strike on **Yellowstone National Park,** one of America's most popular national parks, has sparked concern among environmentalists and government officials.

A nuclear detonation in the park could trigger a catastrophic eruption of the **Yellowstone supervolcano**, which could have devastating consequences for the surrounding area.

The United States has not yet responded to the discussion on Russian state-run TV. However, the country has previously expressed concerns about Russia's nuclear capabilities and the potential for a **nuclear arms race**.

The discussion on **Russian state-run TV** comes at a time of heightened tensions between Russia and the United States. In recent years, the two countries have been engaged in a number of disputes, including Russia's annexation of Crimea and its alleged interference in the 2016 U.S. presidential election.

## CIA director: Iran could obtain nuclear weapon in a matter of weeks

Source: https://worldisraelnews.com/cia-director-iran-could-obtain-nuclear-weapon-in-weeks/

A technician working at an Iranian uranium conversion facility near Isfahan. (AP/Vahid Salemi, File)

Feb 26 – Central Intelligence Agency (CIA) Director William Burns said that Iran now has the capability to create a nuclear weapon within a matter of weeks, while adding that he believes the Islamic Republic's leadership still hasn't given the order to do so, in an interview aired on Saturday.

"To the best of our knowledge, we don't believe that the supreme leader in Iran has yet made a decision to resume the weaponization program that we judge they suspended or stopped at the end of 2003," Burns told *CBS News*.

"But the other two legs of the stool, meaning enrichment programs, have obviously advanced very far," he added.

Burns' remarks came on the heels of a report from the United Nation's atomic agency inspectors, who found that Iran has now enriched uranium to 84 percent purity.

When uranium is enriched to 90 percent, it is considered nuclear weapons-grade.

"They've advanced very far to the point where it would only be a matter of weeks before they could enrich to 90 percent, if they chose to cross that line, and also in terms of their missile systems, their ability to deliver a nuclear weapon once they've developed it has also been advancing as well," Burns said.

"We don't see evidence that they've made a decision to resume that weaponization program, but the other dimensions of this challenge I think are growing at a worrisome pace to."

Burns did not provide evidence or an explanation as to why believes Iran would increase its uranium enrichment levels – far above what was laid out in the original 2015 nuclear deal – without the intention of creating nuclear weapons.

In November 2022, Iran sent a delegation to Vienna, Austria in order to resume negotiations for long-stalled talks aimed at convincing Tehran to return to the 2015 nuclear deal.
"Iran believes that the diplomatic process is the best process to secure the interests of the negotiating parties in connection with the [deal]," Iranian Foreign Minister Nasser Kanaani said in a media statement at the time.
"But we are not optimistic about the current trend [of the discussions]. We have always been realistic, and we will remain that way… [but at the moment] we are pessimistic."

## U.N. Inspectors Detect Near-Weapons-Grade Enriched Uranium in Iran

Source: https://www.iranwatch.org/news-brief/un-inspectors-detect-near-weapons-grade-enriched-uranium-iran

Feb 19 – International Atomic Energy Agency (IAEA) inspectors detected uranium particles **enriched to 84% fissile purity** in Iran in recent weeks, according to three senior diplomats. Iran does not however appear to be accumulating uranium stocks at that level, according to the diplomats. A spokesman for Iran's atomic energy agency did not deny the report, but he suggested that more highly enriched particles could be a byproduct of enrichment to lower levels.

Caspian Sea
IRAN
Yazd
Persian Gulf
Gulf of Oman

## Iran Announces Start-up of Uranium Mine

Source: https://www.iranwatch.org/news-brief/iran-announces-start-uranium-mine

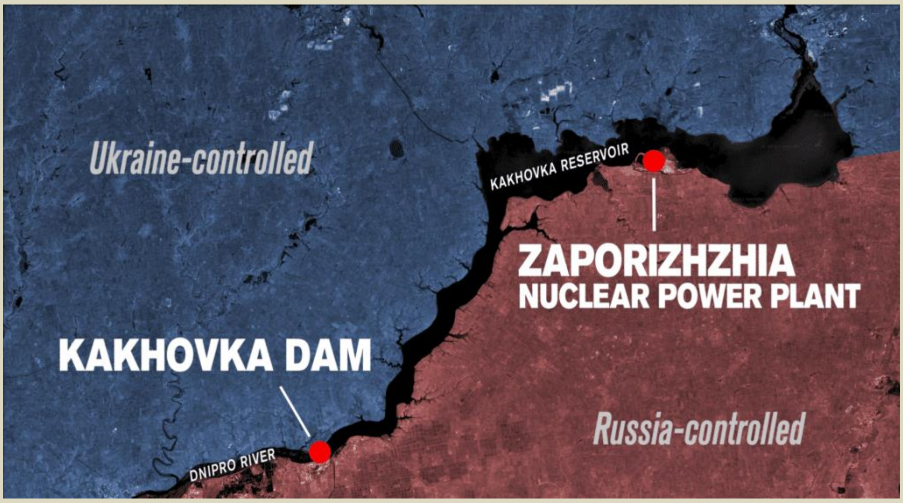
Feb 07 – The Atomic Energy Organization of Iran (AEOI) announced the beginning of operations at the Narigan Mining and Industrial Complex in Yazd province. At the inauguration ceremony, Mohammad Eslami, head of the AEOI, said that uranium from Narigan will be sent to Esfahan for "purification" and will be used for making nuclear fuel. He claimed that the site contained an estimated **650 tons of natural uranium and 4,600 tons of molybdenum.**

## One year later, new dangers threaten Ukraine's embattled Zaporizhzhia nuclear plant

**By Edwin Lyman**
Source: https://thebulletin.org/2023/02/one-year-later-new-dangers-threaten-ukraines-embattled-zaporizhzhia-nuclear-plant/

Feb 28 – Nearly a year after Russia's March 4, 2022 seizure of the Zaporizhzhia nuclear plant in Ukraine, the facility remains in a precarious state. The site has endured fire, structural damage, and five temporary losses of all offsite power as the result of shelling, and the grid connection remains fragile. Unprecedented attempts by Rafael Grossi, the director general of the International Atomic Energy Agency, to create a "safety and security protection zone" around the plant have so far been unsuccessful. And now events many miles away from Zaporizhzhia are posing an additional threat to critical aspects of its operations, reinforcing the need for urgent actions to ensure its safety as fighting intensifies. Like most nuclear plants, the six-reactor Zaporizhzhia facility is situated near a body of water that serves as its ultimate heat sink (UHS), an assured supply of water to its "essential service water system" that enables removal of the radioactive decay heat from shutdown reactors and spent fuel pools. That water system is also used to cool equipment such as the emergency diesel generators needed to provide electrical power when offsite power is lost. (It's important to note that the essential service water system is distinct from the residual heat removal system that provides cooling directly to the fuel in the reactors in cold shutdown. The residual heat removal system, a closed loop, transfers heat from the reactor cores through heat exchangers to the essential service water system, which then carries the heat away to the UHS.)
At Zaporizhzhia, the water supply for the UHS is provided to cooling ponds from the Kakhovka Reservoir, 80 miles downstream of the plant on the Dnipro River. But in recent weeks, reports indicated that the reservoir's water level had decreased and stood at 13.98 meters on February 15, according to the International Atomic Energy Agency. Petro Kotin, the president of Ukraine's state-owned nuclear utility Energoatom, said that if the reservoir level drops below 12.8 meters, then Zaporizhzhia will face an emergency; below 12 meters the situation would become "critical." If the water level gets too low, then the cooling ponds themselves will not be replenished, and the essential service water system will fail. (Ukraine has accused Russian forces controlling the reservoir

dam of draining its water, although, as is typical in this conflict, Russian authorities have denied responsibility and blamed Ukrainian forces for the drop in water levels.) A before and after set of satellite images of the Kakhovka reservoir on the evening of the invasion of Ukraine in February 2022 and in January 2023, showing recent changes to the shoreline. (Landsat / USGS)



Map of the Kakhovka reservoir in southern Ukraine. The Zaporizhzhia nuclear plant is located about 80 miles from the Kakhovka dam on the Dnipro river. (Map: Thomas Gaulkin / Google Earth)

### Learning from Fukushima

What are the safety implications if the UHS is lost? In general, even after reactors are shut down, their highly radioactive irradiated fuel continues to produce large quantities of decay heat that must be efficiently removed to prevent the fuel from overheating and melting. The massive tsunami that caused the March 11, 2011 triple nuclear reactor meltdown at the Fukushima plant in Japan not only disabled the electrical systems needed to run coolant pumps and other equipment, but also destroyed the seawater pumps that were integral components of the UHS. Even if the plant had recovered electrical power in time to allow operation of the cooling pumps, the loss of the UHS would have posed a significant obstacle that operators would have had to overcome, as the pumps carrying steam from the reactors wouldn't have had an effective means of disposing of the heat. Fortunately, there is a reduced risk today that the current situation at Zaporizhzhia would lead to an outcome as dire as Fukushima. First, all six of the reactors have been shut down for at least several months (four in "cold" shutdown and two in "hot" shutdown). Since the decay heat rate decreases significantly over time in a shutdown reactor—dropping by nearly a factor of 100 a few months after shutdown—operators would have a grace period on the order of days, rather than hours, to mitigate a loss of UHS before temperatures rose high enough to cause reactor fuel damage.

Second, the site is better prepared to deal with such an event today than it would have been before Fukushima. In the accident's aftermath, Ukraine, like many countries, carried out stress tests and developed plans for keeping its reactors safe indefinitely under Fukushima-like conditions—not only the long-term unavailability of electrical power, but also loss of the UHS. These plans required acquiring mobile equipment, such as diesel-powered pumps, that operators could use instead of the normal equipment to keep reactors cool without the need for electricity, for instance by feeding water into the steam generators and releasing the steam to the atmosphere. The Ukrainian regulator proposed emergency procedures to connect cooling pumps to the fire water system in the event that a tornado caused a loss of access to the UHS or an earthquake caused the Kakhovka dam to fail. However, the fire water system would need to be replenished from somewhere. The regulator suggested using a suction dredge ship to supply water to the fire system. In its 2012 peer review of Ukraine's stress tests, the European Union recommended that the national regulator should "further analyze in detail … water supply sources" in the event that the normal supply was lost. Although Ukraine reported that this action had been completed in 2021, the feasibility of the dredge ship or other approaches is far from certain, especially in the context of the current military conflict. Ukraine and Russia, with the assistance of the IAEA, need to ensure availability of an alternative water supply in the event that the Kakhovka reservoir level decreases further. And even with an adequate water supply, maintaining these alternative arrangements indefinitely would require a Herculean and sustained effort by plant personnel to operate all the equipment at six reactors manually—comparable or greater to what was needed at Fukushima.

### Still in deep water

Although the risk is lower today at Zaporizhzhia than when all the reactors were at full power, the danger remains. One pipe break, valve failure, or operator error could jeopardize the cooling of one or more of the shutdown cores or spent fuel pools—an event that would be compounded by a loss of offsite power and/or the UHS. Of particular concern are reactor units 5 and 6, which operators are maintaining in "hot shutdown" mode. This means that even though the reactors are not generating power through nuclear fission, the coolant temperature is kept above the boiling point of water, and the residual heat generated from radioactive decay is used to produce steam for plant operations. It is unusual for a nuclear plant to remain in this mode for a sustained period of time, as it is typically only encountered as a transitional phase between refueling and full power operation. Because (based on the example of Western-designed reactors) a number of safety systems are unavailable or cannot be automatically actuated in this mode, operating a plant in this state still comes with an elevated risk if an abnormal event occurs. In that case, operators would have to take prompt manual actions to prevent the temperature from rising further. But given that the remaining operators at the site are already under great stress, and that the Russian occupiers are reportedly blocking Ukrainian staff from maintaining the requisite training, the potential for them to make mistakes in a crisis and possibly exacerbate the situation is a very real one.

Cooling spray ponds, cooling towers, and reactor buildings at the Zaporizhzhia nuclear power plant. (Photo: Energoatom)

Given these circumstances, it is understandable why the Ukrainian regulator recently announced that it would not permit Zaporizhzhia to return to power operation again until the Russian occupation ends and it could assure the safety of the facility. The challenge Ukraine faces with Zaporizhzhia, as with all of its nuclear facilities, is balancing the need for the power they produce against the potential for a nuclear disaster in the face of continued Russian attacks on the country's energy infrastructure. No country should be forced to make such a decision. This is why, if nuclear power is to continue to play a role in providing energy for the world, the international community must ensure that nuclear facilities and their supporting infrastructure are considered strictly off-limits in any military conflict.

**Edwin Lyman** is the Director of Nuclear Power Safety at the Union of Concerned Scientists. He earned a PhD in physics from Cornell University in 1992. He is a co-author (with David Lochbaum and Susan Q. Stranahan) of the book *Fukushima: The Story of a Nuclear Disaster* (The New Press, 2014). In 2018, he received the Leo Szilard Lectureship Award from the American Physical Society.

## What justice means to communities affected by nuclear testing

**By Rebecca Davis Gibbons**

Source: https://thebulletin.org/2023/02/what-justice-means-to-communities-affected-by-nuclear-testing/

Feb 02 – I commend Franziska Stärk and Ulrich Kühn on calling attention to the important but underappreciated topic of nuclear injustice in their recent piece in the *Bulletin*. As their article makes clear, many individuals, communities, and countries have faced nuclear-induced injustices over the course of the nuclear age. Some readers of Stärk and Kühn's article may disagree over aspects of their assessment of nuclear deterrence or the effects of nuclear weapons in the ongoing war in Ukraine. But there should be little debate over the injustices faced by communities victimized by past nuclear testing and uranium mining. A prime example of nuclear injustice can be found on Kili Island in the Republic of the Marshall Islands, a place where I have firsthand experience.

On the day I arrived on Kili Island with two other recent college graduates, our hosts walked us down to the beach. A power boat came ashore, making its way through a channel where the coral that makes up and surrounds the island had been blasted away. One of the fishermen held up a large tuna. He pulled out a knife and cut some of the flesh and gave it to us. I enjoyed the freshest sashimi I had ever tasted to this day.

A nuclear weapon test by the US military at Bikini Atoll in 1946. (Credit: US Defense Department image via Wikimedia Commons, licensed with PD-USGov-Military

It turned out, however, that fish, a traditional staple of the Marshallese diet, was not going to be part of mine as I lived and taught elementary school on the island in the early 2000s. The community on Kili, a speck of an island at 200 acres, is inhabited by the Bikini people. In February 1946, the US military governor for the Marshall Islands arrived on Bikini Atoll and asked its residents to *temporarily* move off their atoll, with its 23 islands and a lagoon full of fish, so the United States could test weapons for "the good of mankind and to end all world wars." They agreed to leave with the promise they would return.

The Bikini community would never move back to their atoll following the detonation of 23 nuclear devices in the 1940s and 1950s. Part of the community came to reside on Kili in 1948, a formerly uninhabited coral island—not an atoll with a lagoon—which made sailing and fishing difficult. While on Kili, the other teaching volunteers and I would not subsist on fish, coconut crabs, pandanus, breadfruit, and coconuts, but rather on canned beef stew, canned fruit cocktail, canned asparagus, white rice, and chicken legs provided by the US government. The reason for this interesting and highly processed food selection? The island of Kili could not sustain the traditional Marshallese diet and the islanders have had to rely on food shipped from the United States.

A traditional—and sustainable—way of eating is just one of many things the US government has stolen from the Bikini community and other Marshallese by conducting 67 atmospheric nuclear tests. Marshallese have lost their culture, their land, and their health. What does justice, therefore, mean to a community that has lost so much?

One of the most important contributions of the Humanitarian Initiative exploring the impact of nuclear weapons was in reminding the world that there are individuals with expertise on nuclear weapons that never wanted such knowledge. (The Humanitarian Initiative emanated in the early 2010s from part of the nuclear nonproliferation community frustrated by the lack of progress in nuclear disarmament.) Individuals from Hiroshima, Nagasaki, Australia, Kazakhstan, Algeria, Western China, the Southwest United States, and the South Pacific learned firsthand about the effects of nuclear weapons when these locations became sites of nuclear detonations. In the same vein, these individuals have become experts in nuclear injustice and justice; they know best what could make their communities whole in 2022.

I asked recently one of my Bikini friends from Kili Island what nuclear justice means to him. He spoke of the inherent unfairness that the Bikini community cannot go back to its homeland and that cancers stemming from radiation are killing their people. He is frustrated that most US citizens still do not know much about what their government did to the Marshall Islands and the Marshallese people with its nuclear testing program. My friend said that justice would mean returning home to a safe environment and sufficient medical care. But more important than any of that, for him, is an apology. The United States "is a powerful country and can do many things," he said. "But it cannot apologize."

Justice comes in many different forms, and discussions on the topic must include those most burdened by nuclear issues; they are necessary voices in any nuclear injustice framework.

**Rebecca Davis Gibbons** is an assistant professor of political science at the University of Southern Maine. She previously served as a fellow and associate of the Project on Managing the Atom at the Harvard Kennedy School's Belfer Center for Science and International Affairs. Before becoming an academic, Dr. Gibbons taught elementary school among the Bikini community on Kili Island in the Republic of the Marshall Islands and served as a national security policy analyst at SAIC providing support to Headquarters Air Force Strategic Stability and Countering WMD Division (AF/A10-S). Her book *The Hegemon's Tool Kit: US Leadership and the Politics of the Nuclear Nonproliferation Regime* was published by Cornell University Press in 2022.

## AI Nuclear Weapons Catastrophe Can Be Avoided

Source: https://www.homelandsecuritynewswire.com/dr20230302-ai-nuclear-weapons-catastrophe-can-be-avoided

Mar 02 - In October 2022, the Pentagon released its National Defense Strategy, which included a Nuclear Posture Review. Notably, the department committed to always maintain human control over nuclear weapons: "In all cases, the United States will maintain a human 'in the loop' for all actions critical to informing and executing decisions by the President to initiate and terminate nuclear weapon employment." Noah Greene writes in *Lawfare* that this commitment is a valuable first step that other nuclear powers should follow. "Still, it is not enough. Commitments like these are time and circumstance dependent. The U.S. military does not currently feel the need to produce and deploy such weapons, in part because it does not see other nuclear powers engaging in similar behavior." The threat of an artificial intelligence (AI)-enabled arms race is not a high-level concern for military planners, but in the future, emerging AI features will only increase the potential for disaster through the possibility of semiautonomous or fully autonomous nuclear weapons.

Greene continues:

> The absence of a firm agreement [on lethal autonomous weapons systems, or LAWS]… also provides a key insight into the perceptions of U.N. member states: A crisis that involves LAWS-related systems is considered to be an issue for the future, not today.
>
> However, autonomous weapons in this vein are far from abstract. During the Cold War, Soviet military planners developed and placed into use a semiautonomous nuclear system known as Perimeter. In the event of nuclear war, Perimeter was designed to launch the Soviet Union's vast missile arsenal without express guidance from central command. In theory, after a human activated the system, network sensors then determined whether the country had been attacked. If the system determined that the country had been attacked, it would check with leaders at the top of the command-and-control structure to confirm. If no response was given, the onus to deploy the missiles fell on a designated official. This was essentially an attempt to ensure mutually assured destruction even in the event of the decapitation of a central government or a "dead hand" scenario.
>
> A lack of urgency in banning such weapons is due to concerns regarding long-term international security implications. At its core, states don't want to make a commitment that could negate a first-mover advantage in adopting certain AI systems, nor do they want to lock themselves out of the market for becoming an early adopter should their enemies decide to utilize these systems.
>
> AI-enabled nuclear weapons are particularly concerning due to their civilization-destroying nature. As James Johnson highlighted in War on the Rocks last year, the question of AI technology being integrated into nuclear mechanisms is not a question of if, but "by whom, when, and to what degree." If viewed along a spectrum, the most extreme degree of AI involvement would be a nuclear weapons system capable of identifying targets and firing on those targets without human approval. The second most extreme example would be a nuclear weapons system capable of firing on a target independently, after a human has locked the target into the system. While neither of these specific systems is known to exist, the future environment for more risky research

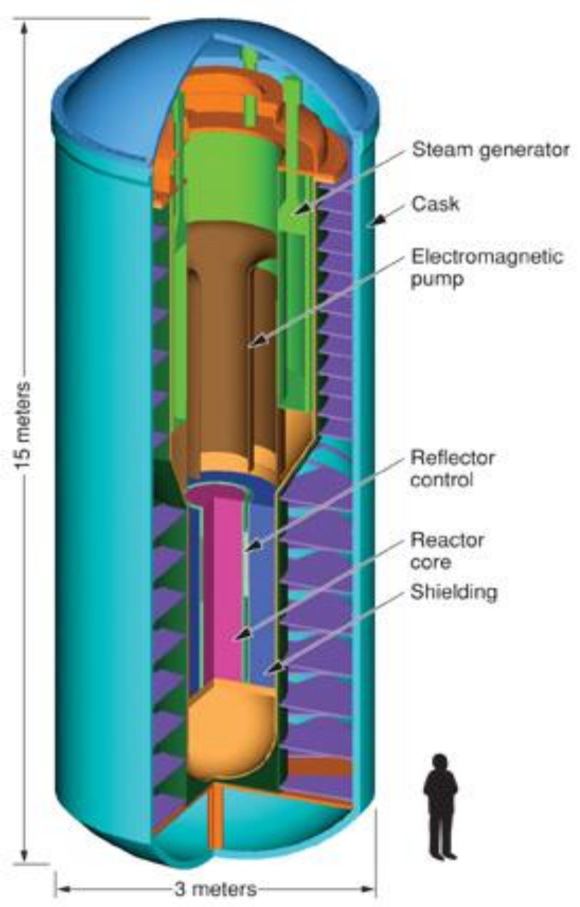
> in this area is far from certain. And both scenarios could be catastrophic. They would also increase the chances of a "broken arrows" incident, in which a nuclear weapon is released accidentally. To at least better humanity's odds of survival, initiating a total ban on these weapons through a P5-led agreement would be a substantial step forward.

Greene concludes:

> As the Soviet-era Col. Petrovcase kindly taught us, without a human firmly in control of the nuclear command-and-control structure, the odds of disaster creep slowly toward an unintended or uncontrolled nuclear exchange. An agreement between nuclear powers on this issue led by P5 states would be an important step toward recreating a patchwork of nuclear treaties that has dissolved over the past two decades. To do otherwise would be to flirt with an AI-enabled nuclear arms race.

## New Biden WMD strategy includes small nuke reactors

Source: https://www.politico.com/news/2023/03/02/biden-strategy-small-nuke-reactors-00085152



Feb 03 – President Joe Biden is signing a new strategy to counter weapons of mass destruction on Thursday, for the first time including radioactive materials at home and abroad. One of the emerging concerns for the administration is the small modular reactors that produce clean energy, but which account for a new proliferation risk.

The reactors could produce "usable material" for terrorist groups seeking to create havoc, a senior administration official told reporters before the signing. "We have to anticipate that and prepare and prevent that becoming a risk. That's been a focal point of this work since the very beginning."

**Context:** In February, the Nuclear Regulatory Commission for the first time certified a new small modular reactor designed for domestic use. The company whose design was approved, NuScale Power, has already signed agreements to deploy its small nuclear reactor plants in 12 countries across Europe and the Middle East. "Nuclear technology is bending towards accessibility and affordability in a way in the past 10 years that I think we couldn't have anticipated," a second administration official added. Both officials were granted anonymity in order to discuss the strategy before it's signed. "And so many more countries who have never pursued nuclear power in the past may be pursuing it in the future."

**Regaining the edge:** The U.S. has long been a leader in establishing and maintaining nuclear safety standards, but with the rise of smaller reactors, "we have lost that edge now, and we need to regain it," the first official said. "And we need to also ensure that as we develop these new capabilities in small modular reactors, we bring the same standard and capability to the global deployment of these reactors."

**What's releasable:** An unclassified fact sheet released Thursday explains that the strategy "establishes the first comprehensive policy for securing radioactive materials, which present continuing domestic and global risk, along with new domestic guidelines for the management and security of nuclear material."

**What's not:** The classified version of the report will incorporate all of the work the U.S. government is doing internationally to prevent and respond to nuclear, chemical, biological, and radiological threats from non-state actors.

## 12 Days: The Time Iran Needs to Produce Enough Weapon-Grade Uranium for a Nuclear Weapon

**By David Albright, Sarah Burkhard, Spencer Faragasso, and Andrea Stricker**

Source: https://www.homelandsecuritynewswire.com/dr20230303-12-days-the-time-iran-needs-to-produce-enough-weapongrade-uranium-for-a-nuclear-weapon

Mar 03 – Iran can now break out and produce enough weapon-grade uranium for a nuclear weapon in 12 days, using only three advanced centrifuge cascades and half of its existing stock of 60 percent enriched uranium. This breakout could be difficult for inspectors to detect promptly, if Iran took steps to delay inspectors' access. A new report from the Institute for Science and International Securitysummarizes and assesses information in the International Atomic Energy Agency's (IAEA) quarterly report for February 28, 2023, *Verification and monitoring in the Islamic Republic of Iran in light of United Nations Security Council resolution 2231 (2015),* including Iran's compliance with the Joint Comprehensive Plan of Action (JCPOA), the nuclear deal between Iran and the P5+ powers which was signed in 205.

**Findings**

- Iran can now break out and produce enough weapon-grade for a nuclear weapon in 12 days, using only three advanced centrifuge cascades and half of its existing stock of 60 percent enriched uranium. This breakout could be difficult for inspectors to detect promptly, if Iran took steps to delay inspectors' access.
- Using its remaining stock of 60 percent enriched uranium and its stock of near 20 percent enriched uranium, Iran could produce enough weapon-grade uranium for an additional four nuclear weapons in a month. During the next two months, Iran could produce two more weapons' worth of weapon-grade uranium from its stock of less than five percent enriched uranium, meaning that Iran could produce enough weapon-grade uranium for five nuclear weapons in one month and seven in three months.
- The IAEA detected uranium particles enriched to 83.7 percent from environmental sampling taken during a monthly interim verification (IIV) at the Fordow Fuel Enrichment Plant (FFEP) on January 22. Iran's answers about this anomaly did not satisfy the IAEA, which has continued probing Iran for more credible answers.
- The IAEA took the environmental samples that detected the presence of near-84 percent enriched uranium a day after inspectors detected an undeclared interconnection between two IR-6 cascades at Fordow, which Iran should have informed the IAEA about under its safeguards obligations. That change likely led the IAEA to take environmental samples at the product sampling point.
- This development amplifies concerns that Iran is undertaking covert experiments that add to its ability to more rapidly break out. Worrisome possibilities include that Iran tested a way to produce near weapon-grade uranium without IAEA detection, or to syphon off a small amount of near 84 percent enriched uranium.
- If the high enrichment level was unintentional, as Iran claims, Iran should have reported the unprecedented enrichment level following the interconnection of the two IR-6 cascades, in line with its reporting of previous fluctuations in the enrichment levels encountered by Iran with the advanced centrifuge cascades dedicated to enriching to 60 percent at the pilot plant. If Iran did not know that the enrichment level reached almost 84 percent, it appears to be operating cascades in a dangerous way, somewhat oblivious to criticality concerns.
- The IAEA seeks increased access to the FFEP. It reports, "At a technical meeting between senior officials in Tehran on 23 February 2023, Iran confirmed that it would facilitate the notified further increase of the frequency and intensity of Agency verification activities at FFEP."
- As of February 12, Iran had a stock of 87.5 kg (an increase of 25.2 kg) (in uranium mass or U mass) of 60 percent enriched uranium in uranium hexafluoride (UF6) form, or 129.4 kg (in hexafluoride mass or hex mass). Adding to concerns about the purpose of this enriched uranium, Iran has converted only 2 kg of 60 percent highly enriched uranium (HEU)¬¬ (U mass) into a chemical form typically used in civilian nuclear programs and none has been converted since March 2022. Iran keeps the majority (80 percent) of its stock of 60 percent HEU at the Esfahan site, where it maintains a capability to make enriched uranium metal.
- Iran's average production rate of 60 percent enriched uranium has doubled to 8 kg per month (U mass) since Iran began on November 22, 2022 to enrich uranium to near 60 percent in two IR-6 centrifuge cascades at the FFEP, in addition to the two cascades, one containing IR-6 centrifuges and the other IR-4 centrifuges, at the Natanz Pilot Fuel Enrichment Plant (PFEP). In both cases, Iran uses up to 5 percent low enriched uranium (LEU) as feed.
- The average production rate of 20 percent enriched uranium at the FFEP decreased by half from 26.8 kg (U mass) or 39.6 kg (hex mass) per month, to 13 kg (U mass) or 19.2 kg (hex mass) per month.
- As of February 12, 2023, Iran had an IAEA-estimated stock of 434.7 kg of 20 percent enriched uranium (U mass and in the form of UF6), equivalent to 643 kg (hex mass). Iran also had a stock of 37.7 kg (U mass) of 20 percent uranium in other chemical forms. At the Natanz Fuel Enrichment Plant (FEP), Iran added seven cascades of advanced centrifuges during the last reporting period, for a total installed of 36 cascades of IR-1 centrifuges, 21 cascades of IR-2m centrifuges (up by six), four cascades of IR-4 centrifuges (up by one), and three cascades of IR-6 centrifuges.
- During the last six months, Iran installed 15 IR-2m centrifuge cascades at the FEP, or roughly 3,650 centrifuges. It is not clear whether these are newly made centrifuges or those taken from storage.
- Iran's current, total operating enrichment capability is estimated to be about 18,700 separative work units (SWU) per year, higher than the 16,300 SWU per year at the end of the last reporting period. As of the end of this reporting period, Iran was not yet using its fully installed enrichment capacity at the FEP, which, as noted above, has grown substantially.

- ❖ Average production of near 5 percent LEU at the FEP decreased, but for the second time in a row since early 2021, Iran's near 5 percent LEU stock increased from one reporting period to the next, reaching 1324.5 kg (U mass).
- ❖ Despite the increase, during this reporting period, in the amount of uranium enriched between two and five percent, Iran has not prioritized stockpiling of this material, during the last two years. This is at odds with its contention that its primary goal is to accumulate 4-5 percent enriched uranium for use in nuclear power reactor fuel. Instead, Iran has used this stock extensively to produce near 20 percent and 60 percent enriched uranium, far beyond any of Iran's civilian needs.
- ❖ Iran's overall reported stockpile of enriched uranium increased by 87.1 kg (U mass).
- ❖ The IAEA discussed a discrepancy in Iran's natural uranium inventory at the Uranium Conversion Facility (UCF). *The Wall Street Journal* reported that the discrepancy may be related to inspectors' efforts to locate undeclared uranium Iran used during its early-2000s nuclear weapons program, in which case the IAEA's upcoming Nuclear Non-Proliferation Treaty (NPT) safeguards report may contain more relevant information.
- ❖ The IAEA reports that it can no longer reestablish continuity of knowledge about Iran's activities under a revived JCPOA, such as production of advanced centrifuges and heavy water, due to Iran's decision in February 2021 to deny the IAEA access to data from key JCPOA-related monitoring and surveillance equipment and Iran's decision in June 2022 to remove all such equipment, including video cameras and online enrichment monitors. The IAEA says it would need to establish a new baseline altogether and would require access to extensive records. It reports, "Any future baseline for [JCPOA] verification and monitoring activities would take a considerable time to establish and would have a significant degree of uncertainty."
- ❖ The absence of monitoring and surveillance equipment, particularly since June 2022, has caused the IAEA to doubt its ability to ascertain whether Iran has diverted or may divert advanced centrifuges. A risk is that Iran could accumulate a secret stock of advanced centrifuges, deployable in the future at a clandestine enrichment plant or during a breakout at declared sites. Another risk is that Iran will establish additional centrifuge manufacturing sites unknown to the IAEA. Iran is fully capable of moving manufacturing equipment to new, undeclared sites, further complicating any future verification effort and contributing to uncertainty about where Iran manufactures centrifuges.
- ❖ The IAEA concludes that "Iran's decision to remove all of the Agency's equipment previously installed in Iran for surveillance and monitoring activities in relation to the JCPOA has [had] detrimental implications for the Agency's ability to provide assurance of the peaceful nature of Iran's nuclear program."
- ❖ Combined with Iran's refusal to resolve outstanding safeguards violations, the IAEA has a significantly reduced ability to monitor Iran's complex and growing nuclear program, which notably has unresolved nuclear weapons dimensions. The IAEA's ability to detect diversion of nuclear materials, equipment, and other capabilities to undeclared facilities remains greatly diminished.
- ❖ Concern about Iran's installation of advanced centrifuges at an undeclared site is magnified as its 60 percent HEU stocks grow. Such a scenario becomes more worrisome and viable, since it requires a relatively small number of advanced centrifuge cascades to rapidly enrich the 60 percent material to weapon-grade. This hybrid strategy involves the diversion of safeguarded HEU and the secret manufacture and deployment of only two or three cascades of advanced centrifuges. With greater uncertainty about the number of advanced centrifuges Iran is making, there is a greater chance of Iran hiding away the requisite number of advanced centrifuges to realize this scenario.

**David Albright** is the President and Founder of the *Institute for Science and International Security*.
**Sarah Burkhard** is Research Associate, and **Spencer Faragasso** is a Research Fellow, at the Institute for Science and International Security.
**Andrea Stricker** is deputy director of the Foundation for Defense of Democracies (*FDD*) Nonproliferation and Biodefense Program and an *FDD* research fellow.

**North Korea's Nuclear Tests Expose Neighbors to Radiation Risks**

Source: https://www.homelandsecuritynewswire.com/dr20230303-north-korea-s-nuclear-tests-expose-neighbors-to-radiation-risks

Mar 03 – Tens of thousands of North Koreans and people in South Korea, Japan, and China could be exposed to radioactive materials spread through groundwater from an underground nuclear test site, a Seoul-based human rights group said in a just-published report.

North Korea secretly conducted six tests of nuclear weapons at the Punggye-ri site in the mountainous North Hamgyong Province between 2006 and 2017, according to the U.S. and South Korean governments, Reuters reports:

> The study by the Transitional Justice Working Group (TJWG) said radioactive materials could have spread across eight cities and counties near the site, where more than 1 million North Koreans live, and where groundwater is used in everyday lives including drinking. It also said that neighboring South Korea, China and Japan might be at risk due partly to agricultural and fisheries products smuggled from the North.

"The populations in neighboring countries such as South Korea, China and Japan are also exposed to the radioactive risk from the contaminated agricultural and marine products imported from North Korea," the report said.

TJWG, formed in 2014, worked with nuclear and medical experts and defectors and used open source intelligence and publicly available government and U.N. reports for the study, which was backed by the National Endowment for Democracy (NED), a non-profit corporation funded by the U.S. Congress.

**Here are the Introduction and Major Findings sections of the TJWG report**:

### Introduction

There have been calls in the past to highlight the linkage between the North Korean nuclear and human rights issues. In January 2013, Navi Pillay, then-UN High Commissioner for Human Rights, expressed her concern that "at the international level, the spotlight is almost exclusively focused on DPRK's nuclear program and rocket launches" and added that "while these, of course, are issues of enormous importance, they should not be allowed to overshadow the deplorable human rights situation in DPRK, which in one way or another affects almost the entire population and has no parallel anywhere else in the world" as she called for a full-fledged international inquiry into serious crimes that had been taking place in North Korea.(1)

The 2014 Report of the UN Commission of Inquiry on Human Rights in the Democratic People's Republic of Korea stated that:

> The State has consistently failed in its obligation to use the maximum of its available resources to feed those who are hungry. Military spending – predominantly on hardware and the development of weapons systems and the nuclear program – has always been prioritized, even during periods of mass starvation.(2)

Since then, resolutions and statements by other countries or international organizations on the human rights situation in North Korea also point out the deterioration of the human rights situation as a result of the North Korean government investing scarce resources in nuclear and weapons development. Accordingly, there is a growing international awareness that resolving the nuclear issue is inextricably linked to human rights issues.

North Korea's rulers have sought to maximize international interest in its nuclear capabilities while avoiding attention on its human rights issues. There is in fact a tendency to view the North Korean nuclear issue solely from a security perspective. Governments and research institutes around the world have been focusing on monitoring and analyzing the type, scale, evidence and signs of resumption of nuclear tests. By contrast, there has been little interest in human rights violations such as forcible transfer of population, forced labor for nuclear tests and threats to human security caused by soil or water resource contamination. A few media outlets reported stories of North Korean escapees who had lived near the nuclear test site, but interest did not last.

Six nuclear tests have made Punggye-ri and Mt. Mantap internationally famous, but there has been a dearth of studies on how many people live near the site of repeated tests of increasing magnitude, what they eat and drink and how their health is affected. Nevertheless, mapping the possible range of leakage and dissemination of radioactive materials through groundwater points to a large area and population at risk.

The populations in neighboring countries such as South Korea, China and Japan are also exposed to the radioactive risk from the contaminated agricultural and marine products imported from North Korea. It is the responsibility of the respective governments to find out and inform the public about where North Korea's nationally advertised specialties like "Mt. Chilbo pine mushrooms" are grown and how they are consumed across borders.

South Korea is the country best suited to conduct a meaningful epidemiological investigation provided it has the political will, since there are nearly 900 North Korean escapees who had lived in the areas near the Punggye-ri nuclear test site after the first nuclear test in 2006. But South Korea's Ministry of Unification reluctantly conducted radiation exposure tests for only 30 escapees in 2017 and 10 escapees in 2018 and covered up the test results showing worrying levels of chromosomal abnormalities among 9 of them (22.5 percent); the tests ceased from 2019. The South Korean government under President Moon Jae-in (2017- 2022) avoided publicizing issues expected to rattle North Korea.

Since 2019, TJWG has been gauging the interests of diplomats and journalists at home and abroad. The diplomats expressed interest and pointed out that, despite the need to discuss the North Korean nuclear issue along with the North Korean human rights issue, it has been difficult to find concrete links thus far. The journalists stated that there are limits to reporting based on rumors or interviews with a few North Korean escapees.

TJWG continued to collect information and data while waiting for an opportune moment. From March 2022, the news of impending resumption of nuclear tests brought about a renewed interest.(3) With the end of Seoul's appeasement of North Korea following the inauguration of the Yoon Seokyeol government in May 2022, an environment conducive to the disclosure of relevant information emerged. Therefore, TJWG decided to gather and organize information to publish a visual report explaining the issue in a coherent manner.

The purpose of this report is fivefold. First, it sets out to clarify the indivisibility of the North Korean nuclear issue and the North Korean human rights issue. Second, it aims to inform the North Korean people about the risk of harm caused by repeated nuclear tests through various means and channels. Third, there is a need to raise awareness about the health risks posed to the people living in South Korea, China and Japan, due to the smuggling and distribution of agricultural and marine products from North Korea. Fourth, the report aims to persuade the South Korean government to expand the radiation exposure tests for the North Korean escapees who had lived in the areas near the Punggye-ri nuclear test site and to disclose the test results. Fifth, TJWG urges the interested states and international organizations to discuss what to explore and how to proceed with additional investigations based on the contents of this report.

## Main Findings and Recommendations

***Hundreds of thousands of people living in the areas near the Punggye-ri nuclear test site are at risk from the leakage and dissemination by water of the radioactive materials from the nuclear test site.***

- There are 8 cities and counties (Kilju County, Hwadae County, Kimchaek City, Myonggan County, Myongchon County, Orang County, Tanchon City and Paegam County) of 3 provinces (North Hamgyong Province, South Hamgyong Province and Ryanggang Province) by administrative division within a 40km radius of the nuclear test site or within the scope of influence from the Mt. Mantap-Changhung Stream-Namdae Stream water system.
- According to North Korea's 2008 census data, the total population of the eight cities and counties is approximately 1.08 million.
- It is not known whether the prisoners at Kwanliso (political prison camp) No. 16 adjacent to the nuclear test site were included in the census of Myonggan County (formerly Hwasong County). The number of prisoners is known to be approximately 28,700 (as of June 2022).
- Out of approximately 1.08 million people, the affected population would be approximately 540,000 or 270,000 under the assumption that 50 or 25 percent respectively has been affected.
- Considering the number of deaths over the 17 years since the start of the nuclear tests in 2006, the affected population may be higher.
- The actual situation of water use is of particular concern. North Korea's 2008 census data shows that nearly one out of every six households (15.5%) in North Hamgyong Province which includes Kilju County uses groundwater, waterhole, public tap, spring, etc. as drinking water. Since the chronic shortage of electricity makes the piped water into dwelling units useless, it appears that more households are in fact using groundwater, waterhole, etc. as drinking water.

***As a result of the smuggling and distribution of agricultural and marine products and local specialties like pine mushrooms from the areas near the Punggye-ri nuclear test site, not only the North Korean people but also the populations in neighboring countries such as South Korea, China and Japan may also be at risk.***

- Despite the risk of radioactive contamination through water, agricultural and marine products from the areas around Punggye-ri are consumed mainly by local people while the local specialties like pine mushrooms are distributed to other regions and overseas as a highly profitable and secret way to earn foreign currency for the North Korean government.
- Pine mushrooms grow not only around Mt. Chilbo but also in mountains within a 40km radius of the Punggye-ri nuclear test site. North Korean escapees from Kilju County and Paegam County stated that the locals picked pine mushrooms from the Mt. Chilbo area prior to the construction of the nuclear test site and that the picking of mushrooms has continued in the mountains around the restricted area after its construction.
- In 2017, China's Ministry of Environmental Protection and the Central Military Commission of the Chinese Communist Party (CCP) reacted with alarm at a possible radioactive leakage after North Korea's 6th nuclear test; however, the Chinese authorities have failed to stop the smuggling of North Korea's agricultural and marine products or their distribution within China or to a third country.
- In 2015, the South Korean authorities detected 981Bq/kg or more than 9 times the standard level of radioactive cesium isotopes (Cs-134 and Cs-137), which is 100Bq/kg, in dried hedgehog mushrooms imported from North Korea disguised as Chinese products but were not able to identify the area of origin within North Korea. In 2018, the South Korean government came under criticism for giving away the pine mushrooms that President Moon Jae-in had received as a gift from Chairman Kim Jong-un to about 4,000 16 Mapping the Risk and Effect of Radioactive

Contamination of Groundwater Sources from the Punggye-ri Nuclear Test Site in North Korea elderly separated families reportedly without radiation testing.

- Although Japan banned all imports from North Korea after North Korea's first nuclear test in 2006, North Korean pine mushrooms disguised as Chinese products in "pine mushroom laundering" are in demand because their price is 1/10 that of the Japanese ones. The Japanese authorities have arrested and prosecuted the executives of the pro-Pyongyang General Association of Korean Residents in Japan (Chongryon) involved in the smuggling operations and reportedly obtained transaction documents between Chongryon and Office No. 39 of the Workers' Party of Korea (WPK) in North Korea, responsible for raising slush funds for North Korea's supreme rulers, stating that the export of pine mushrooms is a state project. There was no news about the testing of the mushrooms for radioactive contamination.

***After reluctantly initiating radiation exposure tests, South Korea's Ministry of Unification watered down the test results revealing abnormalities in 9 out of 40 North Korean escapees from the areas near the Punggye-ri nuclear test site (22.5 percent) in 2017 and 2018 and ceased the tests from 2019; testing all 160 escapees who had lived in Kilju or all 881 escapees who had lived in the areas near the Punggye-ri nuclear test site since North Korea's 1st nuclear test in 2006 can be done with a budget of about 250 million won (211,000 USD) or 1.4 billion won (1,164,000 USD) respectively.***

- The pioneering research by North Korean escapee Dr. Choi Kyong-Hui, president of SAND Institute, and her efforts to publicize the issue as well as concerns about radioactive leakage after North Korea's 6th nuclear test made the Ministry of Unification initiate its own radiation exposure tests for the escapees.
- The Ministry of Unification presented the results of the radiation exposuretests conducted on 30 North Korean escapees from Kilju County in 2017 in an informal oral briefing restricted to the South Korean media journalists and downplayed the significance of the test results. The Ministry of Unification reduced the number of test subjects in 2018 to 10 people and failed to announce the test results for 9 months after the completion of testing until the issue was raised at the National Assembly.
- Among the 30 escapees tested in 2017, 4 (13 percent) showed 7 to 10 stable chromosomal abnormalities and the median radiation dose was 279 to 394 mSv while among the 10 escapees tested in 2018, 5 (50 percent) showed 7 to 59 stable chromosomal abnormalities and the median radiation reached 279 to 1,386 mSv.
- Those who stayed in Kilju County until the 3rd to 6th nuclear tests period tend to have more chromosomal abnormalities and higher radiation doses than those who stayed until the 1st and 2nd nuclear tests period. There was one test subject who had escaped from Myongchon County, but none from Kilju County, immediately after the 6th nuclear test. Therefore, the South Korean government needs to actively contact the North Korean escapees who have experienced the 3rd to 6th nuclear tests period and expand the number of test subjects.
- The National Assembly recommended the Ministry of Unification and the Korea Institute of Radiological & Medical Sciences (KIRAMS) to conduct tests for all North Korean escapees from the areas near the nuclear test site, but the two organs ceased the testing from 2019 and it has yet to resume as of February 2023.
- Among a total of 33,882 North Korean escapees who have entered South Korea by the end of 2022, those who had lived in Kilju County and the areas near Punggye-ri after North Korea's 1st nuclear test in 2006 are 160 and 881 respectively; those who had lived in Kilju County and the areasnear Punggye-ri after the 6th nuclear test in September 2017 are 3 and 20 respectively (as of February 2022).
- According to the unit price of 1,568,000 KRW (1,300 USD) per person for the radiation exposure tests applied by the Korea Institute of Radiological & Medical Sciences (KIRAMS) in 2017-2018, it would take 253,760,000 KRW (211,000 USD) to test all 160 escapees who had lived in Kilju County after 2006 and 1,397,266,000 KRW (1,164,000 USD) to test all 881 escapees from the areas near the Punggye-ri nuclear test site.

***TJWG, mindful of the seriousness and transboundary nature of the risk of nuclear leakage and contamination, recommends the following to governments, international organizations and other stakeholders***:

- The North Korean government: a complete, verifiable, and irreversible denuclearization (CVID); a prompt, effective, thorough, independent and impartial investigation and disclosure of its findings; notification of the risk and other protective measures for the people in the 8 cities and counties near the Punggye-ri nuclear test site, testing of agricultural and marine products.
- The South Korean government: the disclosure of the full reports for the radiation exposure tests conducted in 2017 and 2018; notification of the risk for the North Korean escapees who had lived in the 8 cities and counties near the Punggye-ri nuclear test site after 2006 and resumption of tests; strengthened inspection of agricultural and marine products from North Korea; and the insertion of the risk of Punggye-ri's

radioactive contamination in statements and resolutions concerning North Korea's nuclear development and human rights situation.

- The Chinese government: the disclosure of past radioactive environment survey results; strengthened inspection of agricultural and marine productsfrom North Korea; and the insertion of the risk of Punggye-ri's radioactive contamination in statements and resolutions concerning North Korea's nuclear development and human rights situation. · The Japanese government: strengthened inspection of agricultural and marine products from North Korea; and the insertion of the risk of Punggye-ri's radioactive contamination in statements and resolutions concerning North Korea's nuclear development and human rights situation.
- Other governments and regional bodies: the insertion of the risk of Punggye-ri's radioactive contamination in statements and resolutions concerning North Korea's nuclear development and human rights situation; and publicization by governments, human rights ambassadors, human rights reports as well as parliamentary resolutions and reports.
- UN: inclusion of the risk of Punggye-ri's radioactive contamination in the North Korean security and human rights agenda at the UN Security Council, General Assembly and Human Rights Council; and publicization through the UN special procedures mandate holders, North Korea's 4th cycle Universal Periodic Review (UPR) in October/November 2024 and the monitoring committees of core human rights treaties to which North Korea is a party.
- IAEA: call for North Korea's investigation of the risk of radioactive leakage and contamination from the Punggye-ri nuclear test site based on the Convention on Early Notification of a Nuclear Accident and the Convention on Assistance in the Case of a Nuclear Accident or Radiological Emergency which North Korea signed in 1986.
- Civil society, media, and ordinary citizens: call for a prompt, effective, thorough, independent and impartial investigation and urge the governments and international organizations to take the measures stated above.

## Dogs Living in The Chernobyl Exclusion Zone Are Genetically Distinct, Study Shows

Source: https://www.sciencealert.com/dogs-living-in-the-chernobyl-exclusion-zone-are-genetically-distinct-study-shows

Mar 04 – Nearly 40 years ago, the world's worst nuclear disaster turned the Ukrainian city of Pripyat and its nearby power plant, Chernobyl, into a radioactive hot zone – and surprisingly, decades later, a haven for wildlife.

BELARUS
Pripyat
Chernobyl Nuclear Power Station
EXCLUSION ZONE
UKRAINE

Wolves, wild horses, birds, bison, elk, frogs, and dogs roam among the decaying concrete buildings and surrounding forests of what is now essentially one of Europe's largest nature reserves. Where humans fled, plants grew.

A new genetic analysis conducted by an international team of researchers on the region's canine clans could provide a foundation for learning just how the contamination dusting the landscape may have affected their DNA through the generations.

Scientists have long wondered what effects decades of exposure to low-dose radiation may have had on the area's wildlife.

Some studies have pointed to sharp declines in bird populations, and an increase in genetic mutations among certain species at sites with higher radiation levels. But other investigations have found little evidence of such radiation effects.

One unresolved question contributing to the confusion is whether animals are absorbing small amounts of lingering radiation at levels that are barely harmful or inheriting observed differences from earlier generations who experienced the blast. Or both.

Considering the fact that animals have probably moved into and out of the contaminated zone over the years, it's clearly a messy natural experiment – but one that could still be hugely useful for improving our understanding of the effects radiation has on biology.

By characterizing distinct populations of dogs that live in and around Chernobyl, this latest genetics study provides a better basis for comparing changes in the species.

Some of these dogs may be descendants of pets left behind by evacuees, but it's unclear how many populations remain or how diverse these populations are, and if they differ from other feral dogs throughout Ukraine and adjacent countries.

"Before the effects of radiation on the whole genomes of this population can be isolated from other influencing factors, the demography and history of the population itself need to be understood," write University of South Carolina biologist Timothy Mousseau and colleagues in their published paper.

Large mammals such as dogs and horses are of particular interest because the effects on their health could enlighten us as to what might happen when humans eventually return.

Radiation continues to emanate from the area now known as the Chernobyl Exclusion Zone, which extends some 2,600 square kilometers (about 1,000 square miles) around the ruinous power plant.

Despite the radioactivity, feral dog numbers have been rising, prompting the formation of Chernobyl Dog Research Initiative (CDRI), which has provided veterinary care for these dogs since 2017.

Chernobyl dogs living outside the New Safe Confinement Structure, which was built to contain radioactivity from the explosion of reactor four. (Clean Futures Fund+)

More than 800 dogs are estimated to be living in and around Chernobyl, often fed by power plant workers who return to maintain the facility. They exist in three distinct populations, though this new analysis revealed a surprising amount of genetic overlap and kinship ties between them.

One population lives in the power plant itself; the second occupies Chernobyl city, an abandoned residential area some 15 kilometers from the plant; and the third lives 45 kilometers (28 miles) away in Slavutych, a city with relatively less contamination where some power plant workers still reside.

Over two years, CDRI veterinarians collected blood samples from 302 stray dogs across the three populations, which University of South Carolina PhD student Gabriella Spatola then analyzed.

Spatola, Mousseau, and colleagues identified three main family groups amongst the Chernobyl dogs, with the largest one spanning all three geographical areas where the samples were collected.

Based on their genetic kinship, it appears these dogs move between sites, live close to one another, and breed freely.

The history of mixing between the three Chernobyl populations evident in their genomes indicates "that dogs have existed in the Chernobyl region for a long period of time, potentially since the disaster, or even earlier," Mousseau and colleagues write.

Comparative analyses showed the Chernobyl dogs are also genetically distinct from free-breeding dogs in Eastern Europe, Asia, and the Middle East.

There have, however, been some influxes of genetic material from modern dogs such as mastiffs into some Chernobyl populations. This may be because residents and their pets have begun moving back into Chernobyl City, the researchers suspect.

What will be interesting for future studies is that the three Chernobyl dog populations have been exposed to varying levels of radiation. The next step, the researchers say, will be designing broader studies "aimed at finding critical genetic variants that have accumulated for more than 30 years in this hostile, contaminated environment."

If the studies conducted so far on the wildlife of Chernobyl are anything to go by – and based on what we know about how environmental exposures can be inherited as molecular etchings on an organism's genome – scientists will be hard-pressed to tease out clear findings that resolve their debates once and for all.

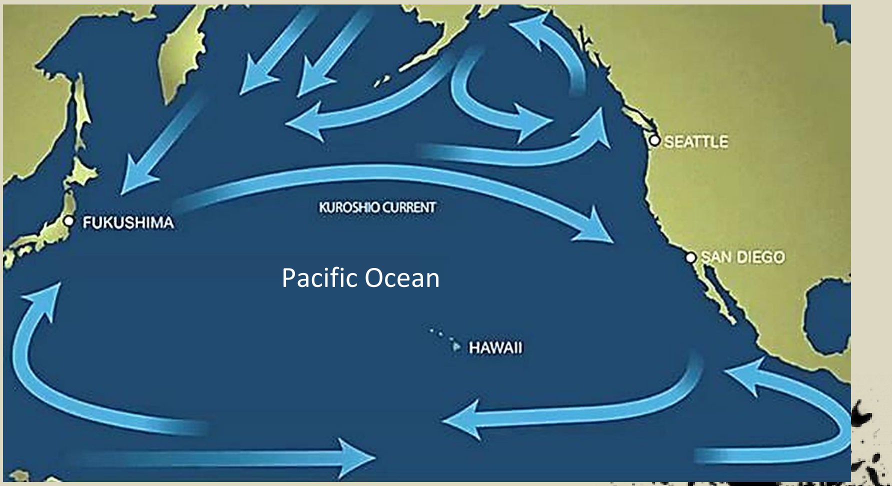
●▶ **The research has been published in** *Science Advances*.

## Will Fukushima's Radioactive Water Endanger The Pacific Ocean?

**By Nigel Marks et al.**

Source: https://www.sciencealert.com/will-fukushimas-radioactive-water-endanger-the-pacific-ocean

Aerial view of Fukushima Daiichi Power Plant. (Ministry of Land, Infrastructure, Transport and Tourism/Wikimedia Commons)



Japanese authorities are preparing to release treated radioactive wastewater into the Pacific Ocean, nearly 12 years after the Fukushima nuclear disaster.

This will relieve pressure on more than 1,000 storage tanks, creating much-needed space for other vital remediation works. But the plan has attracted controversy.

At first glance, releasing radioactive water into the ocean does sound like a terrible idea. Greenpeace feared the radioactivity released might change human DNA, China and South Korea expressed disquiet, while Pacific Island nations were concerned about further nuclear contamination of the Blue Pacific.

One academic publication claimed the total global social welfare cost could exceed US$200 billion.

But the Japanese government, the International Atomic Energy Agency (IAEA), and independent scientists have declared the planned release to be reasonable and safe.

Based on our collective professional experience in nuclear science and nuclear power, we have reached the same conclusion. Our assessment is based on the type of radioactivity to be released, the amount of radioactivity already present in the ocean, and the high level of independent oversight from the IAEA.

**How much water is there, and what's in it?**

The storage tanks at Fukushima contain 1.3 million tonnes of water, equivalent to around 500 Olympic-sized swimming pools.

Contaminated water is produced daily by ongoing reactor cooling. Contaminated groundwater also collects in the basements of the damaged reactor buildings.

The water is being cleaned by a technology called ALPS, or Advanced Liquid Processing System. This removes the vast majority of the problematic elements.

The ALPS treatment can be repeated until concentrations are below regulatory limits. Independent monitoring by the IAEA will ensure all requirements are met before discharge.

The main radioactive contaminant remaining after treatment is tritium, a radioactive form of hydrogen (H) that is difficult to remove from water ($H_2O$). There is no technology to remove trace levels of tritium from this volume of water.

Tritium has a half-life of 12.3 years, meaning 100 years passes before the radioactivity is negligible. It is unrealistic to store the water for such a long time as the volumes are too great. Extended storage also increases the risk of accidental uncontrolled release.

Like all radioactive elements, international standards exist for safe levels of tritium. For liquids, these are measured in Bq per liter, where one Bq (becquerel) is defined as one radioactive decay per second.

At the point of release, the Japanese authorities have chosen a conservative concentration limit of 1,500 Bq per liter, seven times smaller than the World Health Organization's recommended limit of 10,000 Bq per liter for drinking water.

**Why is it acceptable to release tritium into the ocean?**

One surprising thing about radiation is how common it is. Almost everything is radioactive to some degree, including air, water, plants, basements, and granite benchtops. Even a long-haul airline flight supplies a few chest X-rays worth of radiation to everyone on board.

In the case of tritium, natural processes in the atmosphere generate 50-70 peta-becquerels (PBq) of tritium every year. This number is difficult to grasp, so it's helpful to think of it as grams of pure tritium. Using the conversion factor of 1 PBq = 2.79 g, we see that 150-200 g (5.3-7.1 oz) of tritium is created naturally each year.

Looking at the Pacific Ocean, around 8.4 kg (3,000 PBq) of tritium is already in the water. By comparison, the total amount of tritium in the Fukushima wastewater is vastly smaller, at around 3 g (1 PBq).

Japanese authorities are not planning to release the water all at once. Instead, just 0.06 g (22 TBq) of tritium is scheduled for release each year. Compared with the radioactivity already present in the Pacific, the planned annual release is a literal drop in the ocean.

The current levels of tritium radioactivity in the Pacific are not of concern, and so the small amount to be added by the Fukushima water won't cause any harm.

What's more, tritium only makes a tiny contribution to the total radioactivity of the oceans. Ocean radioactivity is mostly due to potassium, an element essential for life and present in all cells. In the Pacific Ocean there is 7.4 million PBq of radioactivity from potassium, more than 1,000 times greater than the amount due to tritium.

**How do other countries manage the discharge of tritium?**

All nuclear power plants produce some tritium, which is routinely discharged into the ocean and other waterways. The amount generated depends on the type of reactor.

Boiling water reactors, such as at Fukushima, produce relatively low quantities. When Fukushima was operating, the tritium discharge limit was set at 22 TBq per year. That figure is far below a level that could cause harm, but is reasonably achievable for this type of power plant.

In contrast, the UK Heysham nuclear power plant has a limit of 1,300 TBq per year because this type of gas-cooled reactor produces a lot of tritium. Heysham has been discharging tritium for 40 years without harm to people or the environment. Annual tritium discharge at nearby nuclear power plants far exceeds what is proposed for Fukushima. The Fuqing plant in China discharged 52 TBq in 2020, while the Kori plant in South Korea discharged 50 TBq in 2018.

Each of these power plants releases more than twice the amount to be released from Fukushima.

**Are there other reasons for not releasing the water?**

Objections to the planned release have been the subject of widespread media coverage. *TIME* magazine recently explained how Pacific Island nations have been grappling for decades with the legacy of Cold War nuclear testing.

*The Guardian* ran an opinion piece from Pacific activists, who argued if the waste was safe, then "dump it in Tokyo, test it in Paris, and store it in Washington, but keep our Pacific nuclear-free".

But the Pacific has always contained radioactivity, from potassium in particular. The extra radioactivity to be added from the Fukushima water will make the most miniscule of differences.

Striking a different tone, The Pacific Island Forum commissioned a panel of experts to provide independent technical advice and guidance, and help address concerns on the wastewater.

The panel was critical of the quantity and quality of data from the Japanese authorities, and advised that Japan should defer the impending discharge.

While we are sympathetic to the view that the scientific data could be improved, our assessment is that the panel is unfairly critical of ocean release.

The main thing missing from the report is a sense of perspective. The public seminar from the expert panel, available on YouTube, presents only a portion of the context we provide above. Existing tritium in the ocean isn't discussed, and the dominance of potassium is glossed over.

The most reasonable comments regard the performance of ALPS. This is largely in the context of strontium-90 and cesium-137, both of which are legitimate isotopes of concern.

However, the panel implies that the authorities don't know what is in the tanks, and that ALPS doesn't work properly. There actually is a lot of public information on both topics. Perhaps it could be repackaged in a clearer way for others to understand. But the inferences made by the panel give the wrong impression.

The most important thing the panel overlooks is that the contaminated water can be repeatedly passed through ALPS until it is safe for release. For some tanks a single pass will suffice, while for others additional cycles are required.

**The big picture**

The earthquake was the primary environmental disaster, and the planet will be dealing with the consequences for decades. In our view, the release of Fukushima wastewater does not add to the disaster.

It's easy to understand why people are concerned about the prospect of radioactive liquid waste being released into the ocean. But the water is not dangerous. The nastiest elements have been removed, and what remains is modest compared with natural radioactivity. We hope science will prevail and Japan will be allowed to continue the recovery process.

**Nigel Marks** is an Associate Professor of Physics @ Curtin University;
**Brendan Kennedy** is a Professor of Chemistry @ University of Sydney.
**Tony Irwin** is an Honorary Associate Professor, Nuclear Reactors and Nuclear Fuel Cycle @ Australian National University.

## Serbia-Croatia border arrests over radioactive material found in car

Source: https://www.bbc.com/news/world-europe-64874255

Mar 07 – Three Croatian nationals have been arrested in Serbia after radioactive material was discovered in their car, Serbian officials say.

They were about to enter Croatia on Saturday when scanners detected a "serious amount" of radiation.

A subsequent search of an Audi car revealed the head of a radioactive lightning rod in the spare tyre slot of the boot, Serbian customs said.

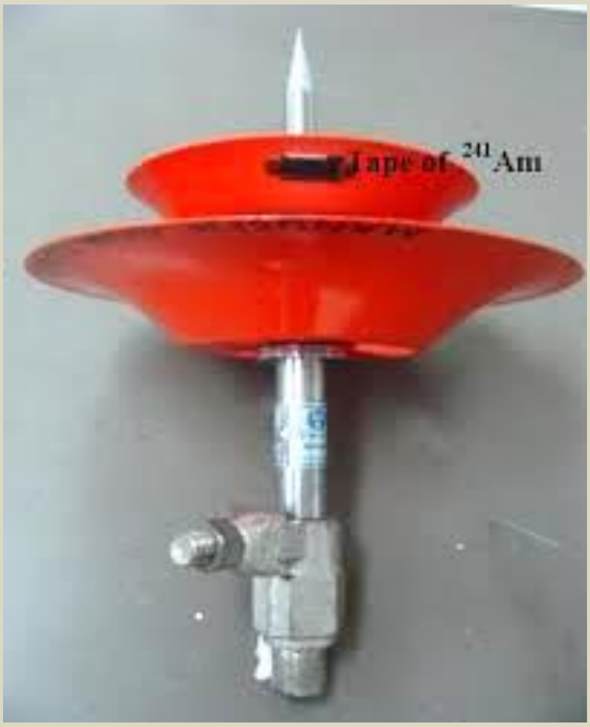
Such rods were widely used in the past, but are now largely being dismantled.

The incident occurred at the Bezdan border crossing near the town of Sombor on Saturday at 20:30 (19:30 GMT).

HUNGARY
Zagreb
Sombor
CROATIA
SERBIA
Belgrade
BOSNIA
AND HERZEGOVINA

A statement by Serbian customs authorities said stationary monitors had sounded as the car was being checked before exiting the country. A subsequent search revealed the the head of the lightning rod, as well as a device for measuring the composition of the metal.

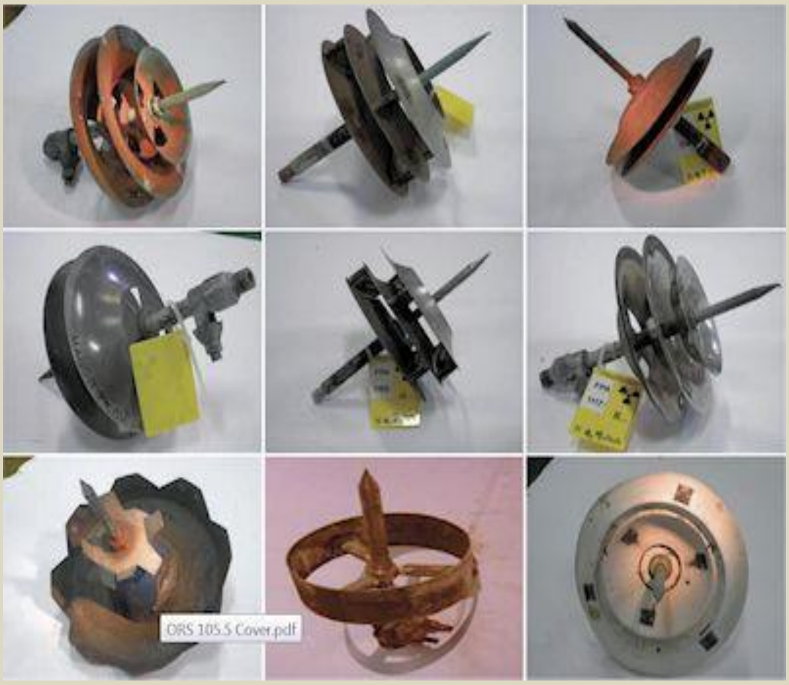
A hand-held device used for measuring radiation ionisation had reacted to that substance, it added.



Model radioactive lighting-rod sold in Brazil

There has been no detail about the amount of radioactive material involved or its potential impact, but workers at the border crossing were ordered to discard their clothing and undergo medical checks as a precaution, Serbian media report. Experts from Serbia's Vinca nuclear research institute have reportedly moved the head of the lightning rod to a safer place.

**Hundreds of thousands of radioactive lightning rods were installed worldwide in the past few decades,** according to the International Atomic Energy Agency (IAEA), in the belief that they enhanced the chance of lightning strikes hitting the rods and not nearby targets.



Nine models of radioactive lightning rods

In a report last year, the IAEA said that "no convincing scientific evidence has been produced to demonstrate increased efficacy" and many countries had decided to stop the production of these devices. Some have started to remove the radioactive sources from the lightning rods that have already been installed.

However, the report suggested most of the rods were installed more than 50 years ago, when nuclear safety standards had not been introduced. No reliable data existed about their overall numbers or location, it added, let alone the state of wear and tear or decay of the protective cases or the radioactive material contained inside. It highlighted cases where rod heads were sold as scrap metal by traders unaware of their existence or danger.

**EDITOR'S COMMENT:** Perhaps a new threat that we are not aware of – and it is everywhere and usually not well guarded. In a study conducted in Italy, the authors first give a brief history of the development of lightning rods. Next, an assessment is made of the possible radiological hazards of the radioactive rod and the benefits of the radioactive rod as compared to the Franklin rod. The authors conclude that the use of $^{226}$Ra and $^{241}$Am sources in lightning rods should be considered as a risk not justified by demonstrated benefits.

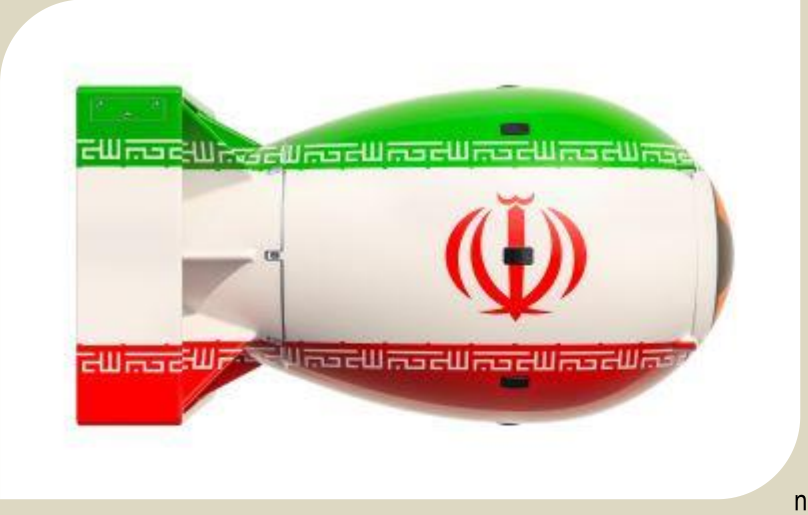
## Nuke your city

Source 1: https://outrider.org/nuclear-weapons/interactive/bomb-blast
Source 2: https://nuclearsecrecy.com/nukemap/
Source 3: http://www.carloslabs.com/projects/200712B/GroundZero-2-6.html

# The Secret Russia-Iran Nuclear Deal -- Enriched Uranium for the Mullahs

**By Benjamin Weinthal**

Source: https://www.meforum.org/64230/the-secret-russia-iran-nuclear-deal-enriched



Mar 05 – Amid the International Atomic Energy Agency's disclosure this week that the Islamic Republic of Iran accumulated near weapons-grade enriched uranium for its alleged nuclear weapon program, Fox News Digital has learned that Iran has allegedly secured secret deals with Russia to guarantee deliveries of uranium.

In what could be a major setback to a new Iran nuclear deal, foreign intelligence sources speaking on the condition of anonymity, and who are familiar with the negotiations between Moscow and Tehran over Iran's reported illegal nuclear weapons work, told Fox News Digital that Russian President Vladimir Putin agreed to return enriched uranium that it received from Iran if a prospective atomic deal collapses. The State Department would neither confirm nor deny the reports.

The State Department spokesperson told Fox News Digital, "We will not comment on purported secret intelligence reports, but in any event the JCPOA has not been on the agenda for months." A spokesperson for the National Security Council deferred comment to the State Department.

One major component of the effort by the U.S and other world powers to revive the Joint Comprehensive Plan of Action (JCPOA), the formal name of the Iran nuclear deal, is for Russia to warehouse Tehran's enriched uranium. The rationale for Russia storing the uranium is to prevent the regime from using the material to construct an atomic bomb.

The foreign intelligence sources claim, "As part of the agreement between the two countries, Russia has undertaken to return all the enriched uranium to Iran as quickly as possible if, for any reason, the U.S. withdraws from the agreement."

"It would make sense to me that they would agree to this type of side deal," Rebekah Koffler, a former analyst at the U.S. Defense Intelligence Agency, said. Koffler noted that, "Based on my knowledge of Russian doctrine and state tradecraft, the Russians are trying to play both sides. On the one side, they do not want Iran to have a nuclear weapon. On the other hand, they do want assistance from Iran for Ukraine." Koffler, an expert on Russian strongman Vladimir Putin, added, "Russia benefits from being a party to the JCPOA. Russia's tactic is to drag things on and play both sides. That gives Putin leverage over both sides but also allows him to be perceived as a deal-maker. Russia is signaling that the U.S. is dependent on Russia."

She concluded that, "The Russians are trying to signal to the Iranians that they will help them out like they did with Iran's civilian nuclear program. On the other hand, they might want to put pressure on the U.S. to do the deal. It is just part of Putin's standard playbook to try to game his opponents." Former U.S. President Donald Trump withdrew from the Iran nuclear deal in 2018 because he and his administration believed the JCPOA failed to stop Iran from building a nuclear bomb. Trump's White House also argued that the Iran nuclear pact did not crack down on the theocratic state's terrorism and restrict its missile program.

Iran's regime wants an ironclad agreement from the Biden administration that it and future U.S. administrations will not pull the plug on a new JCPOA. The White House said it cannot guarantee that a new administration will not walk away from the controversial deal. On Tuesday, a top U.S. Defense Department official told Congress that Iran's regime could develop enough fissile material for a nuclear bomb in a mere 12 days.

When asked about the secret deals between Iran and Russia over the shipments of enriched uranium, Mojtaba Babaei, a spokesperson for the Iran mission at the United Nations, told Fox News Digital, "There's no information about the claim."

He added, "Massimo Aparo, deputy director general and head of the Department of Safeguards, visited Iran last week and checked the alleged enrichment rate. Based on Iran's assessment, the alleged enrichment percentage between Iran and the IAEA is resolved. Due to the IAEA report being prepared before his trip, his trip's results aren't in it and hopefully the IAEA director general will mention it in his oral report to the board of governors." When questioned about the Islamic Republic building a nuclear weapon, Babaei said, "Iran has no plans to make nuclear weapons because its military doctrine prohibits the use of weapons of mass destruction in any form." Experts on Iran's alleged atomic weapons program have long sharply disagreed with the Islamic Republic's denials and the growing cooperation between Russia and Iran has exacerbated the conflict over Tehran's nuclear program.

Jason Brodsky, the policy director of the U.S.-based United Against a Nuclear Iran (UANI), told Fox News Digital that the "reported side deals between Iran and Russia on the nuclear file just demonstrate the risks of depending on Moscow as a participant or guarantor in a JCPOA-like arrangement. The geopolitical context has fundamentally shifted with its invasion of Ukraine."

He added, "P5+1 [China, France, Russia, Britain, U.S. and Germany] under these conditions of great power conflict is not a viable diplomatic platform. Iran has leverage over Russia in 2023 that it did not have in 2015 with its supply of arms. It's in this dynamic that the Kremlin can't be trusted. The JCPOA of 2015 has no future. It's time to declare it dead, invoke the snapback sanctions mechanism, and pivot to a deterrence strategy as the diplomatic track has run aground."

Iran's regime is supplying Russia with sophisticated lethal drone technology in its war against Ukraine.

The uranium enrichment deal was hammered out during Putin's visit to Iran in July 2022. The ostensible quid pro quo arrangement between the authoritarian regimes further solidified their growing alliance.

The Intelligence officials said, "President Putin, who made a special trip to Iran to pursue weapons deals between the two countries, agreed to approve the request, apparently due to his interest in compensating the Iranians for their assistance." Talks about the secret deals also unfolded between Moscow and Tehran during August 2022, when Iran's regime was providing a shot into the arm of Putin's war machinery in Ukraine. According to the intelligence officials, the Iranians seized the opportunity during Putin's desperate need for drones and demanded a "nuclear guarantee" that would enable Iran "to quickly restore its uranium stock to the quantity and enrichment levels it had maintained before the resumption of the agreement."

The attempt to circumvent the U.S. and the other Western powers would gut the entire purpose of the Iran nuclear deal, argued the intelligence officials, who noted, "This would significantly undermine U.S. interests and would give Russia de facto control over the nuclear agreement in the present and future." The Biden administration remains deeply wedded to the Iran nuclear deal, which would provide Tehran with up to $275 billion in financial benefits during the first year of the agreement and a startling $1 trillion by 2030, according to one U.S. think tank study. In an unusual move, the Biden administration is following a more dovish approach than its Western European counterparts who want Iran to be censured at Monday's IAEA meeting for enriching near weapons-grade uranium. The Islamic Republic has produced weapon-grade material of 60 percent since 2021, but new material was discovered showing 84 percent purity. Weapons-grade uranium starts at around 90 percent. Michael Singh, an expert on Iran's nuclear program and the managing director for The Washington Institute for Near East Policy, urged the Biden administration and its allies in a late February article on the think tank's website to "snap back sanctions" against Iran in response to Tehran's near weapons-grade uranium enrichment. The 2015 JCPOA contains a penalty that allows for snapback sanctions and Singh argued that the sanctions would "bolster military deterrence, and plan for potential crisis scenarios."

The row over Iran's illicit enrichment of weapons-grade uranium comes amid a Fox News Digital report that Tehran may be behind an assassination and terror target list focused on law enforcement agencies in Boston.

The U.S. government under both Democratic and Republican administrations has classified Iran's regime as the worst state sponsor of international terrorism. Fox News Digital queries to Russia's government and the IAEA were not immediately returned.

The IAEA's Director General Grossi said on Saturday while in Tehran that he had "constructive" meetings and a settlement with Iran over its near weapons-grade enrichment of uranium was reached. Grossi met with the head of Iran's atomic energy organization, Mohammad Eslami. The IAEA board is scheduled to meet Monday in Vienna to consider the organization's latest report and could once again censor Iran for its actions.

**Benjamin Weinthal** is a Middle East Forum writing fellow, reports on Israel, Iran, Syria, Turkey and Europe for Fox News Digital.

## The narrow field of options for safely managing Ukraine's Zaporizhzhia Nuclear Power Plant

**By Mark Hibbs**

Source: https://thebulletin.org/2023/03/the-narrow-field-of-options-for-safely-managing-ukraines-zaporizhzhia-nuclear-power-plant/

Mar 10 – Last month, Ukraine told the International Atomic Energy Agency (IAEA) it would not permit any of the six reactors at the Zaporizhzhia Nuclear Power Plant (ZNPP) to generate electric power until Russia had given the occupied installation back to Ukraine. Ukraine's statement challenges Russia's resolve to prolong and tighten its grip over Europe's biggest nuclear power station, and it has narrowed the field of options for managing the nuclear plant as the war continues.

One year after Russia's assault and takeover of the Zaporizhzhia plant, Russians and Ukrainians face decisions about the operation status of the six reactors that will significantly impact nuclear safety and security. Decision makers might mothball the reactors, or instead elect one or more of a range of modes for operating them, on a scale from cold shutdown to resumed criticality and low-power operation.

On February 6, four days before the IAEA made the Ukraine statement public, I published a detailed account of nuclear safety considerations pertinent to forthcoming decisions about whether and under what conditions reactors at the ZNPP would be allowed to operate. Since September and until now, all six reactors have been shut down, but two units have been prepared for restart, an action that could significantly affect the safety profile of the plant. During preparation of that article, the IAEA did not answer my questions about whether, under a proposal for a "protection zone" the IAEA has proposed for ZNPP, the reactors would be permitted to operate.

IAEA Director General Rafael Mariano Grossi and member of the International Atomic Energy Agency (IAEA) delegation inspect remains of a rocket shell during a visit to the Zaporizhzhia nuclear power plant in Ukraine on September 1, 2022. (Photo Konstantin Mihalchevskiy / Sputnik via AP)

But the February 10 release of the statement from the State Nuclear Regulatory Inspectorate of Ukraine (SNRIU) addressed that issue in a policy declaration. Ukraine, it said, would "only permit ZNPP to resume power-generating operations after it has been returned to the control of Ukraine and a thorough inspection program and the implementation of any measures deemed necessary to restore the plant to safe working conditions have been completed."

Since March 5 last year, Russian forces have occupied the Zaporizhzhia facility; Russia has claimed ownership of the station; Russia has declared that the territory on which the plant sits has been annexed by Russia; and the Russian state has set up a company, assisted by Rosatom, Russia's national nuclear energy corporation, to manage the plant. Russian interference with and intimidation of Ukrainian personnel have degraded nuclear safety and nuclear security. By all accounts, a highly charged relationship between Russian occupiers and Ukrainian personnel and authorities persists. During the second half of last year, cooperation or coercion sufficed to shut down all the reactors, carry out refueling and limited maintenance at some units, and then, beginning last fall, prepare two reactors for resumed operation.

Determination by Ukraine not to permit any reactors at Zaporizhzhia to produce electricity in effect stands in the way of any Russian effort to connect the plant to the Russian power grid, generate electricity, and transmit power to Russian-occupied Ukrainian territory. Ukrainian personnel have asserted since March that occupiers informed them that Russia, aided by Rosatom, planned to take such action.

In theory, Russia, supported by increasing numbers of Russian technical personnel at the station, might decide to start up reactors and generate electricity in defiance of Ukrainian oversight. If so, that step would escalate conflict over control of the station, but it is less certain that the procedure would be successful.

Since Ukraine's independence in 1991, the six ZNPP reactors, plus nine others located elsewhere in Ukraine, have been steadily upgraded, based largely on Western government and industry assistance. This effort was accelerated by the meltdown of three reactors at Fukushima-Daiichi in Japan in 2011 and by Russia's seizure of Crimea in 2014. After Fukushima the European Union included Ukraine in an EU-wide program to assess and improve reactor safety, focusing on issues that had contributed to the disaster in Japan. The Crimea takeover marked the beginning of stepped-up cooperation between Ukraine and Western governments to address the physical security and cybersecurity of Ukraine's strategic infrastructure, including the electrical power system and nuclear power plants. For Ukraine's nuclear stations, the EU launched a program covering 1.5 billion euros worth of safety improvements.

Significantly, since the 1990s ZNPP has been upgrading instrumentation and control systems and equipment, in partnerships that include vendors in the United States and Europe. Procedures have also become more aligned with Western practice. Should Russian occupiers attempt to restart and operate reactors without assistance from experienced Ukrainian personnel, they might encounter difficulties, take safety risks, and perhaps fail. Should Ukrainian operators with deep knowledge of ZNPP's technology and operating modes conclude that instructions to start up reactors contravene Ukrainian government directives, it is plausible that they might interfere with or sabotage startup procedures.

**Zaporizhzhia plant operating modes**

For as long as the war continues, the safety profile of the installation will reflect pending decisions about the operational status of its reactors. Apart from electric power production, Ukraine's regulator did not specifically exclude any other option for operating the Zaporizhzhia reactors, on a spectrum from cold shutdown to low-power operation.

In September all six reactors were in cold shutdown: In this condition, control rods are fully inserted into the fuel, preventing criticality, and temperature and pressure are reduced to well below operating levels. Decay heat from the reactor is removed by the residual heat removal system; after several idle months the heat load in the fuel would be reduced to a fraction of the operating level. With that final point in mind, six months ago some observers appeared to view cold shutdown as a ready fix for safety hazards at the Zaporizhzhia plant.

But late last year, two reactors in cold shutdown, Z-5 and Z-6, were prepared for low-power operation. They were therefore put into "hot shutdown." In this state, temperature and pressure are normally allowed to increase in preparation for "hot standby" followed by zero-power operation and then low-power operation. During this transition, temperature and pressure increase, steam begins to form in steam generators, and the turbine will be put into service. Shutdown cooling is shifted from residual heat removal equipment to the reactor cooling pumps, a step having major safety implications. Upon authorization, the reactor may be heated up further to a level permitting criticality, and by manipulating control rods and other variables, reactor power may be slightly increased to allow the turbine to operate but below the level at which the electric generator connected to the turbine would begin producing electricity.

**A complex risk profile**

How decision makers in fact proceed on operation of the Zaporizhzhia plant will reflect system safety concerns but may also take into account vulnerabilities to terrorism and military attacks and the desire of owner/operators to protect operating licenses and avoid long outages that may damage turbine-side equipment. Cold shutdown conditions normally obtain during refueling and maintenance outages lasting a few weeks; at ZNPP however several reactors have been in cold shutdown for many months.

In 1991, Slovenia anticipated an attack by Yugoslavia against its Krsko nuclear power plant; it chose to put the plant into cold shutdown based on important assumptions, namely, that the crisis would be over in days, and that in an emergency, the plant would be supplied with off-site power and the heat sink would be available to cool the reactor. The situation at Zaporizhzhia looks very different; foreign military occupation is indefinite, and there is less confidence about both off-site power and the heat sink. Shelling attacks have interrupted off-site power—such an interruption occurred after a Russian missile attack this week—and the Zaporizhzhia heat sink—a water reservoir fed by the Dnipro River—may be threatened by mines and by reckless Russian actions away from the power plant that appear to be drawing down the water volume. The nuclear safety risks associated with cold and hot shutdown modes are not identical, reflecting in part requirements for different reactor cooling equipment, and they also depend on plant-specific variables; on March 9 the two units in hot shutdown were put back into cold shutdown after shelling attacks interrupted supply of off-site power.

Should decision makers elect to operate reactors in startup modes for months, personnel under intense pressure from occupiers would be relied upon to carefully micromanage safety-significant reactor parameters. Even under routine conditions, during reactor shutdown operators could unleash severe accident sequences. Vulnerabilities would likely be greater should the war escalate and spread to the power plant site. A Russian counteroffensive may be imminent, and Ukraine's nuclear power management recently asserted that Ukraine aims to expel Russian occupiers from Zaporizhzhia with force of arms.

Given these risks, in principle the safest option for the Zaporizhzhia nuclear power plant would be to shut all reactors down, depressurize the circuits, and remove their fuel until the end of the war. As an IAEA peer reviewer in one European country with similar reactors said: "There would be no heat, no pressure, no radioactivity, and no severe accident."

But the plant's fuel inventory is another key consideration in decisions about how or if the Zaporizhzhia reactors are to be run. If removed from reactor cores, hot, highly radioactive fuel must be safely stored and contained. Ukraine regulations require that the spent fuel storage pool at each reactor accommodate a full core of fuel in an emergency. As part of EU post-Fukushima upgrades, Zaporizhzhia reactors were outfitted with portable equipment to supply water in an emergency to spent fuel pools and to reactor cores. But moving a core of fuel into a pool would significantly increase the heat load, and safe storage margins might be limited following previous re-racking to pack more fuel in the pools. Safety authorities may ultimately decide that the fuel would be better protected if left in the reactors, since they were designed to protect and cool the fuel including in an emergency. Separately, the owner/operator may not want to undertake prolonged outages of de-fueled reactors in the interest of limiting restart authorization requirements.

A year after Russia wrested control of the Zaporizhzhia plant, officials in Russia and Ukraine making decisions about its operating status are challenged by a nuclear safety and security profile that may appear more nuanced and complex than at any time under Russian occupation, especially before all six reactors were idled six months ago. No single reactor-management option for reducing risk will minimize or address all hazards for as long as the war continues, especially since the design basis of the plant does not include risks associated with warfare and foreign military occupation. The decision last September to idle all six reactors may not prevail, and reactors may be ordered to go critical and their nuclear fuel sustain a fission chain reaction. A separate option—to mothball the plant and banish the probability of a severe accident—may so far have been rejected at least in part following a plant-specific safety assessment. Perhaps all six reactors will be managed in a regime fluctuating between periods of shutdown and low-power operation. The choice may reflect a balancing act, taking into account the interests of regulators and safety experts, managers and operators, diplomats, and, ultimately, military commanders. The most significant impact of their decision making might not become apparent immediately but instead if and when violence at and around the nuclear plant intensifies.

**Mark Hibbs** is a senior associate in Carnegie's Nuclear Policy Program, based in Bonn and Berlin. Before joining Carnegie, for over 20 years he was an editor and correspondent for nuclear energy publications, including Nucleonics Week and Nuclear Fuel, published by the Platts division of the McGraw-Hill Companies. From the late 1980s until the mid-1990s, he covered nuclear developments in the Soviet bloc, including research on the USSR's nuclear fuel cycle facilities and its nuclear materials inventories. Since the mid-1990s, his work has focused on emerging nuclear programs in Asia, including China and India. Since 2003, he has made many detailed findings about clandestine procurement in Europe related to gas centrifuge uranium enrichment programs in Iran, Libya, North Korea, and Pakistan. His Carnegie report, "The Future of the Nuclear Suppliers Group," was published in December.

# Nuclear Notebook: Chinese nuclear weapons, 2023

By Hans M. Kristensen, Matt Korda, and Eliana Reynolds

Source: https://thebulletin.org/premium/2023-03/nuclear-notebook-chinese-nuclear-weapons-2023/

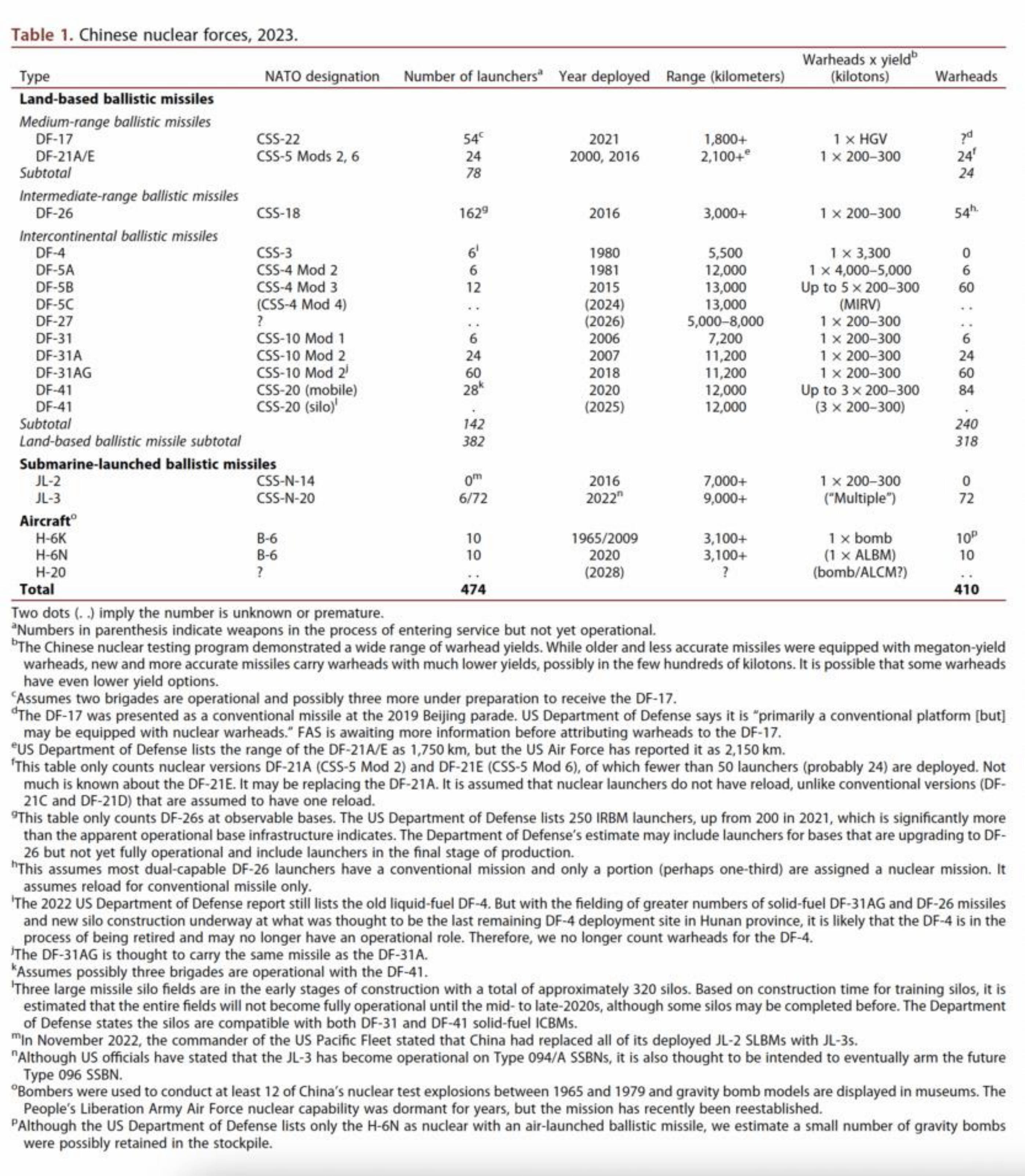


**Table 1.** Chinese nuclear forces, 2023.

| Type | NATO designation | Number of launchers[a] | Year deployed | Range (kilometers) | Warheads x yield[b] (kilotons) | Warheads |
|---|---|---|---|---|---|---|
| **Land-based ballistic missiles** | | | | | | |
| *Medium-range ballistic missiles* | | | | | | |
| DF-17 | CSS-22 | 54[c] | 2021 | 1,800+ | 1 × HGV | ?[d] |
| DF-21A/E | CSS-5 Mods 2, 6 | 24 | 2000, 2016 | 2,100+[e] | 1 × 200–300 | 24[f] |
| *Subtotal* | | *78* | | | | *24* |
| *Intermediate-range ballistic missiles* | | | | | | |
| DF-26 | CSS-18 | 162[g] | 2016 | 3,000+ | 1 × 200–300 | 54[h]. |
| *Intercontinental ballistic missiles* | | | | | | |
| DF-4 | CSS-3 | 6[i] | 1980 | 5,500 | 1 × 3,300 | 0 |
| DF-5A | CSS-4 Mod 2 | 6 | 1981 | 12,000 | 1 × 4,000–5,000 | 6 |
| DF-5B | CSS-4 Mod 3 | 12 | 2015 | 13,000 | Up to 5 × 200–300 | 60 |
| DF-5C | (CSS-4 Mod 4) | . . | (2024) | 13,000 | (MIRV) | . . |
| DF-27 | ? | . . | (2026) | 5,000–8,000 | 1 × 200–300 | . . |
| DF-31 | CSS-10 Mod 1 | 6 | 2006 | 7,200 | 1 × 200–300 | 6 |
| DF-31A | CSS-10 Mod 2 | 24 | 2007 | 11,200 | 1 × 200–300 | 24 |
| DF-31AG | CSS-10 Mod 2[j] | 60 | 2018 | 11,200 | 1 × 200–300 | 60 |
| DF-41 | CSS-20 (mobile) | 28[k] | 2020 | 12,000 | Up to 3 × 200–300 | 84 |
| DF-41 | CSS-20 (silo)[l] | . | (2025) | 12,000 | (3 × 200–300) | . |
| *Subtotal* | | *142* | | | | *240* |
| *Land-based ballistic missile subtotal* | | *382* | | | | *318* |
| **Submarine-launched ballistic missiles** | | | | | | |
| JL-2 | CSS-N-14 | 0[m] | 2016 | 7,000+ | 1 × 200–300 | 0 |
| JL-3 | CSS-N-20 | 6/72 | 2022[n] | 9,000+ | ("Multiple") | 72 |
| **Aircraft**[o] | | | | | | |
| H-6K | B-6 | 10 | 1965/2009 | 3,100+ | 1 × bomb | 10[p] |
| H-6N | B-6 | 10 | 2020 | 3,100+ | (1 × ALBM) | 10 |
| H-20 | ? | . . | (2028) | ? | (bomb/ALCM?) | . . |
| **Total** | | **474** | | | | **410** |

Two dots (. .) imply the number is unknown or premature.

[a] Numbers in parenthesis indicate weapons in the process of entering service but not yet operational.

[b] The Chinese nuclear testing program demonstrated a wide range of warhead yields. While older and less accurate missiles were equipped with megaton-yield warheads, new and more accurate missiles carry warheads with much lower yields, possibly in the few hundreds of kilotons. It is possible that some warheads have even lower yield options.

[c] Assumes two brigades are operational and possibly three more under preparation to receive the DF-17.

[d] The DF-17 was presented as a conventional missile at the 2019 Beijing parade. US Department of Defense says it is "primarily a conventional platform [but] may be equipped with nuclear warheads." FAS is awaiting more information before attributing warheads to the DF-17.

[e] US Department of Defense lists the range of the DF-21A/E as 1,750 km, but the US Air Force has reported it as 2,150 km.

[f] This table only counts nuclear versions DF-21A (CSS-5 Mod 2) and DF-21E (CSS-5 Mod 6), of which fewer than 50 launchers (probably 24) are deployed. Not much is known about the DF-21E. It may be replacing the DF-21A. It is assumed that nuclear launchers do not have reload, unlike conventional versions (DF-21C and DF-21D) that are assumed to have one reload.

[g] This table only counts DF-26s at observable bases. The US Department of Defense lists 250 IRBM launchers, up from 200 in 2021, which is significantly more than the apparent operational base infrastructure indicates. The Department of Defense's estimate may include launchers for bases that are upgrading to DF-26 but not yet fully operational and include launchers in the final stage of production.

[h] This assumes most dual-capable DF-26 launchers have a conventional mission and only a portion (perhaps one-third) are assigned a nuclear mission. It assumes reload for conventional missile only.

[i] The 2022 US Department of Defense report still lists the old liquid-fuel DF-4. But with the fielding of greater numbers of solid-fuel DF-31AG and DF-26 missiles and new silo construction underway at what was thought to be the last remaining DF-4 deployment site in Hunan province, it is likely that the DF-4 is in the process of being retired and may no longer have an operational role. Therefore, we no longer count warheads for the DF-4.

[j] The DF-31AG is thought to carry the same missile as the DF-31A.

[k] Assumes possibly three brigades are operational with the DF-41.

[l] Three large missile silo fields are in the early stages of construction with a total of approximately 320 silos. Based on construction time for training silos, it is estimated that the entire fields will not become fully operational until the mid- to late-2020s, although some silos may be completed before. The Department of Defense states the silos are compatible with both DF-31 and DF-41 solid-fuel ICBMs.

[m] In November 2022, the commander of the US Pacific Fleet stated that China had replaced all of its deployed JL-2 SLBMs with JL-3s.

[n] Although US officials have stated that the JL-3 has become operational on Type 094/A SSBNs, it is also thought to be intended to eventually arm the future Type 096 SSBN.

[o] Bombers were used to conduct at least 12 of China's nuclear test explosions between 1965 and 1979 and gravity bomb models are displayed in museums. The People's Liberation Army Air Force nuclear capability was dormant for years, but the mission has recently been reestablished.

[p] Although the US Department of Defense lists only the H-6N as nuclear with an air-launched ballistic missile, we estimate a small number of gravity bombs were possibly retained in the stockpile.

Table 1: Chinese Nuclear Forces, 2023

DF-31 nuclear missile launcher on display at the Chinese People's Revolutionary Military Museum in Beijing in 2017, during a themed exhibition commemorating the 90th anniversary of the founding of the country's People's Liberation Army.

Mar 13 – China is continuing the nuclear weapons modernization program that it initiated in the 1990s and 2000s, but is expanding it significantly by fielding more types and greater numbers of nuclear weapons than ever before. Since our previous Nuclear Notebook on China in November 2021, China has continued to modernize its road-mobile intercontinental ballistic missile (ICBM), has significantly advanced the construction of its three new missile silo fields for solid-fuel ICBMs, and has also expanded the construction of new silos for its liquid-fuel DF-5 ICBMs. China is also significantly expanding its DF-26 intermediate-range ballistic missile force and has also begun replacing some older conventional short- range ballistic missiles with new DF-17 medium-range ballistic missiles equipped with hypersonic glide vehicles. At sea, China apparently has refitted its six Type-094 ballistic missile submarines with the longer-range JL-3 submarine-launched ballistic missile. In addition, China has recently reassigned a nuclear mission to its bombers and is developing an air-launched ballistic missile that might have nuclear capability.

We estimate that China has produced a stockpile of approximately 410 nuclear warheads for delivery by land-based ballistic missiles, sea-based ballistic missiles, and bombers. Additional warheads are thought to be in production to eventually arm additional road-mobile and silo-based missiles and bombers (see Table 1). The Pentagon's 2022 report to Congress estimated that by 2030 China's nuclear stockpile "will have about 1,000 operational nuclear warheads, most of which will be fielded on systems capable of ranging the continental United States" (US Department of Defense 2022a, 97). If expansion continues at the current rate, the Pentagon projected, China might field a stockpile of about 1,500 nuclear warheads by 2035 (US Department of Defense 2022a, 94, 98).

These projections, however, have yet to fully materialize. They depend on many uncertain factors, including how many missile silos will be built, how many warheads each missile will carry, and assumptions about the future production of fissile materials by China. US estimates for China's nuclear weapons stockpile have been wrong several times already in the past (Figure 1). Current US projections appear to simply apply the same increase rate of new warheads added to the stockpile between 2019 and 2021 to the subsequent years until 2035.

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

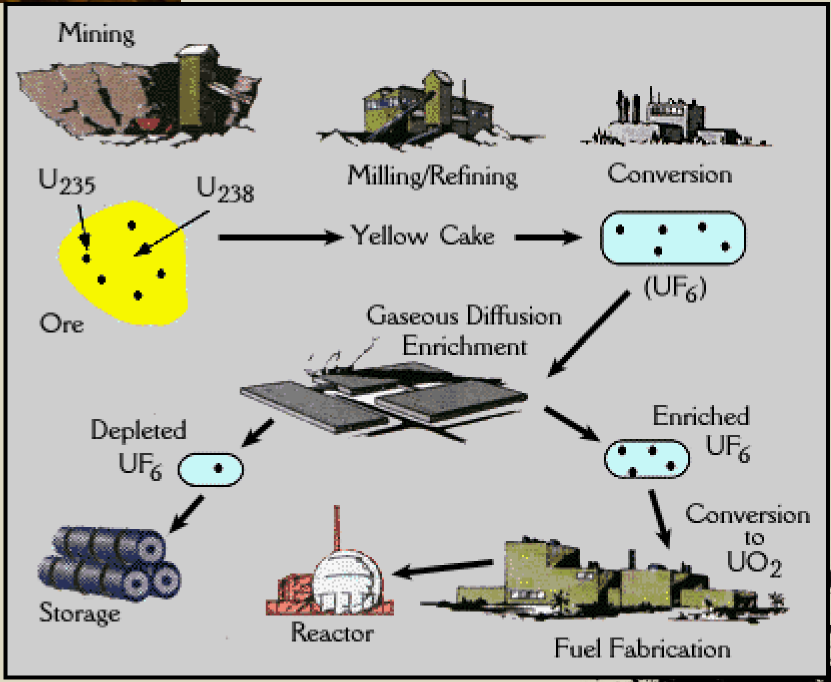
**Hans Kristensen** is the director of the Nuclear Information Project with the Federation of American Scientists (FAS) in Washington, DC. His work focuses on researching and writing about the status of nuclear weapons and the policies that direct them. Kristensen is a co-author to the world nuclear forces overview in the *SIPRI Yearbook* (Oxford University Press) and a frequent adviser to the news media on nuclear weapons policy and operations. He has co-authored the Nuclear Notebook since 2001.
**Matt Korda** is a Senior Research Associate and Project Manager for the Nuclear Information Project at the Federation of American Scientists, where he co-authors the Nuclear Notebook with Hans Kristensen. Matt is also an Associate Researcher with the Nuclear Disarmament, Arms Control and Non-proliferation Programme at the Stockholm International Peace Research Institute (SIPRI). Previously, he worked for the Arms Control, Disarmament, and WMD Non-Proliferation Centre at NATO HQ in Brussels. Matt received his MA in International Peace & Security from the Department of War Studies at King's College London. His research interests are nuclear deterrence and disarmament; progressive foreign policy; and the nexus between nuclear weapons, climate change, and injustice.
**Eliana Reynolds** is a research associate for the Nuclear Information Project at the Federation of American Scientists, where she researches the status and trends of global nuclear forces and the role of nuclear weapons. Previously, Eliana worked as a project associate for DPRK Counterproliferation at CRDF Global, focusing on WMD nonproliferation initiatives to curb North Korea's ability to gain revenue to build its weapons programs. Eliana graduated with her bachelor's in Political Science with minors in Music and Korean in 2021 from the University of Maryland, Baltimore County.

## Nuclear: 2.5 tons of uranium disappeared from Libya site, says IAEA

Source: https://www.tellerreport.com/news/2023-03-15-nuclear--2-5-tons-of-uranium-disappeared-from-libya-site--says-iaea.HJem09Akxn.html

Yellow cake represents an intermediate step in the process of making nuclear fuel from uranium ore. © Energy Fuels Inc./Flickr Nuclear Regulatory Commission/CC BY 2.0

Mar 16 – The International Atomic Energy Agency (IAEA) reported Wednesday (March 16th) the disappearance of about 2.5 tons of natural uranium from a site in Libya, without giving further details of the site where the material should have been.
During a visit on Tuesday, inspectors from the UN body "*discovered that ten containers with about 2.5 tons of natural uranium in the form of uranium concentrate (*'yellow cake'*) were not present where they had been declared by the authorities*," Director-General Rafael Grossi wrote in a report to member states.
The IAEA specifies that it will conduct "*additional*" verifications to "*clarify the circumstances of the disappearance of this nuclear material and its current location*". No details are given on the site in question.
Libya abandoned its nuclear weapons development program in 2003 under former leader Muammar Gaddafi.
Since its fall in 2011 after 42 years of dictatorship, the country has been mired in a major political crisis, with rival powers based in the east and west, a myriad of militias, mercenaries scattered throughout the country, against a backdrop of foreign interference. Two governments are vying for power: one installed in Tripoli (West) and recognized by the UN, the other supported by the strongman of eastern Libya, Marshal Khalifa Haftar.



**Some additional info**

Yellowcake uranium **can be highly toxic** but does not contain significant radiation, according to the World Nuclear Association. It is transported from mines to conversion plants in drums within normal shipping containers, and the World Nuclear Association said no radiation protection is required to prevent exposure.

Because the yellowcake is just the separation of the uranium from the ore, it displays no more radiation than naturally occurring uranium. Due to natural uranium consisting of approximately 99.289% $^{238}$U, which has a half-life of roughly 4 billion years, **its radioactivity is very low**.

**UPDATE (16/3):** Armed forces in eastern Libya say they have found ten drums containing the near the border with Chad, said the head of the forces' media unit. There is only a confusion since a worker stated that the yellow cake was in 18 drums.

## Power plant in Thailand ups reward for missing radioactive cylinder to 100,000 baht

Source: https://thethaiger.com/news/national/power-plant-in-thailand-ups-reward-for-missing-radioactive-cylinder-to-100000-baht

Mar 16 – A **power plant** in Prachin Buri province in central **Thailand** has upped the **reward** for information on the whereabouts of a missing **radioactive** cylinder containing **Caesium-137** from 50,000 to **100,000 baht** (2,736 euro | 2,904 USD).

The Office of Atoms for Peace have checked CCTV and scoured second-hand shops in the Si Maha Phot district to no avail.

The radioactive cylinder was noticed missing on Friday but is believed to have been taken from the plant on February 23.

Prachin Buri governor Ron Nakhonchinda said that all factories within a 2-kilometre radius of the plant have been searched but the Caesium-137 is still missing. The search is being expanded to other provinces, said Governor Ron.

Given the grave danger the radioactive substance presents to human and environmental health, more than 20 power plant officials have been interrogated about the missing cylinder at Si Mada Phot Police Station, but none of them has provided information so far.

If you see the cylinder – a steel tube around five inches in diameter, eight inches long and weighing 25 kilogrammes – don't touch it.

Immediately call Khun Aree on 085-835-0190, Khun Phattana on 085-835-2735, or the Disaster Prevention and Mitigation hotline on 1784. Thai authorities are scrambling to find a steel tube containing the **radioactive** isotope **Caesium-137** believed to have gone missing from a **power plant** at an industrial estate in Prachin Buri province in central **Thailand** on February 23.

Staff noticed the cylinder was missing on Friday and filed a record at Sri Maha Phot Police Station that day.

The company said that anyone with information on the Caesium-137's whereabouts will be rewarded with 50,000 baht.

The substance is encased in a steel tube around five inches in diameter, eight inches long and weighs 25 kilogrammes.

Staff at the plant said the radioactive isotope will not cause damage to health or the environment unless the cylinder is dismantled.

Caesium-137 is invisible and has no odour. Any body part exposed to the substance will suffer from necrosis (body tissue decay) from beta and gamma radiation.

Permsuk Sutchapiwat, secretary of the Office of Atoms for Peace – Thailand's agency responsible for nuclear research – warned…

*"If someone breaks the cylinder, when you are directly exposed to it, you could be exposed to a high risk of cancer and serious illness, so please don't break the cylinder."*

According to the CDC…

*"External exposure to large amounts of Cs-137 can cause burns, acute radiation sickness, and even death. Exposure to Cs-137 can increase the risk of cancer because of exposure to high-energy gamma radiation.*

*“Internal exposure to Cs-137, through ingestion or inhalation, allows the radioactive material to be distributed in the soft tissues, especially muscle tissue, exposing these tissues to the beta particles and gamma radiation and increasing cancer risk.”*

National Power Plant 5A Co., Ltd., and the Office of Atoms for Peace set up a team of 50 people to search for the missing radioactive isotope but couldn’t find it anywhere on the plant grounds. They believe it has been taken away.

The team searched 26 locations in the Si Maha Phot district including scrap metal yards, second-hand shops and antique shops to no avail. The team are expanding their search for factories in Chachoengsao which buy steel from scrap metal yards/factories.

Current assessments detect no presence of the substance in the immediate area.

## Launch Under Attack: A Sword of Damocles

**By Natalie Montoya and R. Scott Kemp**

Source: https://warontherocks.com/2023/03/launch-under-attack-a-sword-of-damocles/

Mar 17 – On Jan. 10, 1984, a guidance computer in a U.S. Minuteman-III missile suffered a glitch. As a result, operators in the nearby command center received a message that the missile, aimed at Russia, was entering its launch sequence all on its own. It carried three nuclear warheads. Security forces scrambled to park a truck on top of the silo lid in an attempt to prevent the missile from launching. While the officer in charge later disclaimed that there was a real risk, the truck-parking procedure was in place because the risk of inadvertent launch was understood to be nonzero. This begs the question: Are Russian missiles guaranteed never to launch themselves? Are their missileers perfectly reliable? If the answer is no, then why does the United States maintain a policy that risks starting a nuclear war in the event something goes wrong?

Since the 1960s, the United States has deployed nuclear-tipped ballistic missiles in concrete silos. Barring an almost direct hit, the silo is designed to protect the missile from the crushing overpressure of nuclear explosions so that it can be used for retaliation. In addition to this physical protection, the United States maintains a posture it calls “launch under attack,” a doctrine that permits U.S. missiles to be loosed from their shelters after “multiple, independent sensors” detect an incoming attack from an adversary. The notional purpose of this policy is to provide extra assurance that U.S. silo-based missiles will not be destroyed, silo protections notwithstanding.

Launch under attack proponents argue that this posture improves strategic stability. We argue it does the opposite. A better description of the policy would be “launch on warning.” While multiple sensors are used, those sensors cannot discern whether the warheads on incoming missiles are armed. Because the posture forces a decision before these missiles land, it leaves the president somewhere between zero and 20 minutes to guess at whether the electronic warning messages received constitute an actual attack. This is scant time and an imperfect basis for definitively committing to a civilization-ending nuclear war.

Such a gamble might be deemed necessary if the United States were at risk of losing its weapons from a first strike — a nuclear Pearl Harbor, as the policy's proponents like to say — but this is not a reality. We argue from published data about missile accuracies and silo hardness that silos will work, and U.S. missiles will survive. In fact, because of a technical twist, the U.S. deterrent force may be stronger after the attack than before it, when measured as weapons available per target. This implies that launch under attack does not provide any additional deterrent against a first strike.

At the same time, there are many historical examples of early-warning systems generating false alarms or computer-generated messages pretending to be actual warnings. When combined with a launch-on-warning posture, these glitches create real risks of accidental war. It is thus not surprising that four-star generals George Lee Butler, Eugene E. Habiger, and James Cartwright — all of whom served as commander of U.S. Strategic Command — have argued forcefully that the United States should abandon its launch under attack policy. Both Presidents George W. Bush and Barack Obama called for severely reducing or eliminating the capacity, stating that it created unacceptable risks. As a candidate, President Bush also argued that the United States should not wait for Russia to reciprocate "because it is in our best interest and the best interest of the world" to act unilaterally. However, U.S. policy remains unchanged.

President Joe Biden's 2022 Nuclear Posture Review released in October maintains the status quo, but it also confesses that the policy is not needed, stating: "…while the United States maintains the capability to launch nuclear forces under conditions of an ongoing nuclear attack, it does not rely on a launch-under-attack policy to ensure a credible response. Rather, U.S. nuclear forces are postured to withstand an initial attack." Our simulations support this finding. Even under the most pessimistic assumptions, about 100-200 missiles are expected to survive in their silos — more than enough to inflict severe damage on an adversary.

### Silo Survivability Simulations

The scenarios investigated in our work were based on the assertion made in the 2018 Nuclear Posture Review that "To destroy U.S. ICBMs [silo-based missiles] on the ground, an adversary would need to launch a precisely coordinated attack with hundreds of high-yield and accurate warheads. This is an insurmountable challenge for any potential adversary today, with the exception of Russia."

Following this view, we developed four attack scenarios in which Russia targets each of the 400 U.S. silos with one warhead, two warheads, three warheads, and finally all of its deployed ballistic missiles (in silos, on road-mobile launchers, and on submarines). We used probabilistic computer simulations of missile accuracy and blast effects to estimate the number of silos that would survive the attack, and ran **10,000 simulations for each attack scenario**. (Details of missile accuracy and warhead yields are available in supplemental information). Most Russian ballistic missiles carry multiple warheads on independently targeted reentry vehicles, which imposes constraints on a Russian attack because there is a physical limit to how far apart the individual warheads carried by the same missile can be targeted. Our simulations target the individual warheads to optimize their performance.

The findings for each of the four attack profiles are shown in Figure 1. In each case, we assumed unrealistically high performance for Russia's weapons. Our findings therefore overestimated the damage Russia could do to U.S. nuclear forces. Specifically, our calculations assumed Russian missiles would suffer no launch failures, duds, navigation errors, flight-control errors, or any other failure that would prevent them from reaching their targets. We also assumed zero fratricide, which is to say Russia's nuclear detonations would not disrupt other incoming Russian warheads. The smallest attack left the United States with 205 ± 9 missiles, which is just over half of the existing force. The largest attack left 102 ± 9 missiles. In addition to these silo-based missiles, the United States would still retain about 1,000 nuclear warheads deployed on submarine-based missiles, and hundreds more to be delivered by bombers.

Under the brinkmanship construct, the ability to deter Russia's first strike rests on its assessment of both the probability that the United States would decide to retaliate as well as the damage inflicted by that retaliation. With respect to a decision to retaliate, adding launch under attack would not change anything. If the attack were genuine, the United States would respond. Launch under attack *does* make a decision to use weapons more probable, but only for the subset of cases where the early warning system gave a false alarm — exactly those cases where such a decision would be in error.

That leaves the question of whether the retaliation that the United States could inflict after riding out an attack is comparable to that under launch under attack. Leaving aside U.S. submarines, the number of silo-based missiles remaining would in all cases be sufficient to execute the planned catastrophic damage to Russia's war-making ability.

First, consider the case where the United States launched all of its silo-based missiles on warning of an incoming, large-scale attack. The Russian arsenal accounts for 138 "counterforce" targets (126 silos, seven mobile missile bases, three nuclear bomber bases, and two nuclear missile submarine bases). To compensate for imperfect accuracy and reliability, each aim point would likely be covered by multiple warheads, as evidenced by declassified Cold War plans. Geographically large targets, like bases, often have multiple aim points. Assuming two warheads per aim point, and that bases have two aim points each while silos have just one, the counterforce targets alone require 300 of the 400 available U.S. silo-based missiles. This would leave 100 weapons for the remaining non-missile counterforce targets, leadership targets, and strategic elements of Russia's war-making capability such as industry.

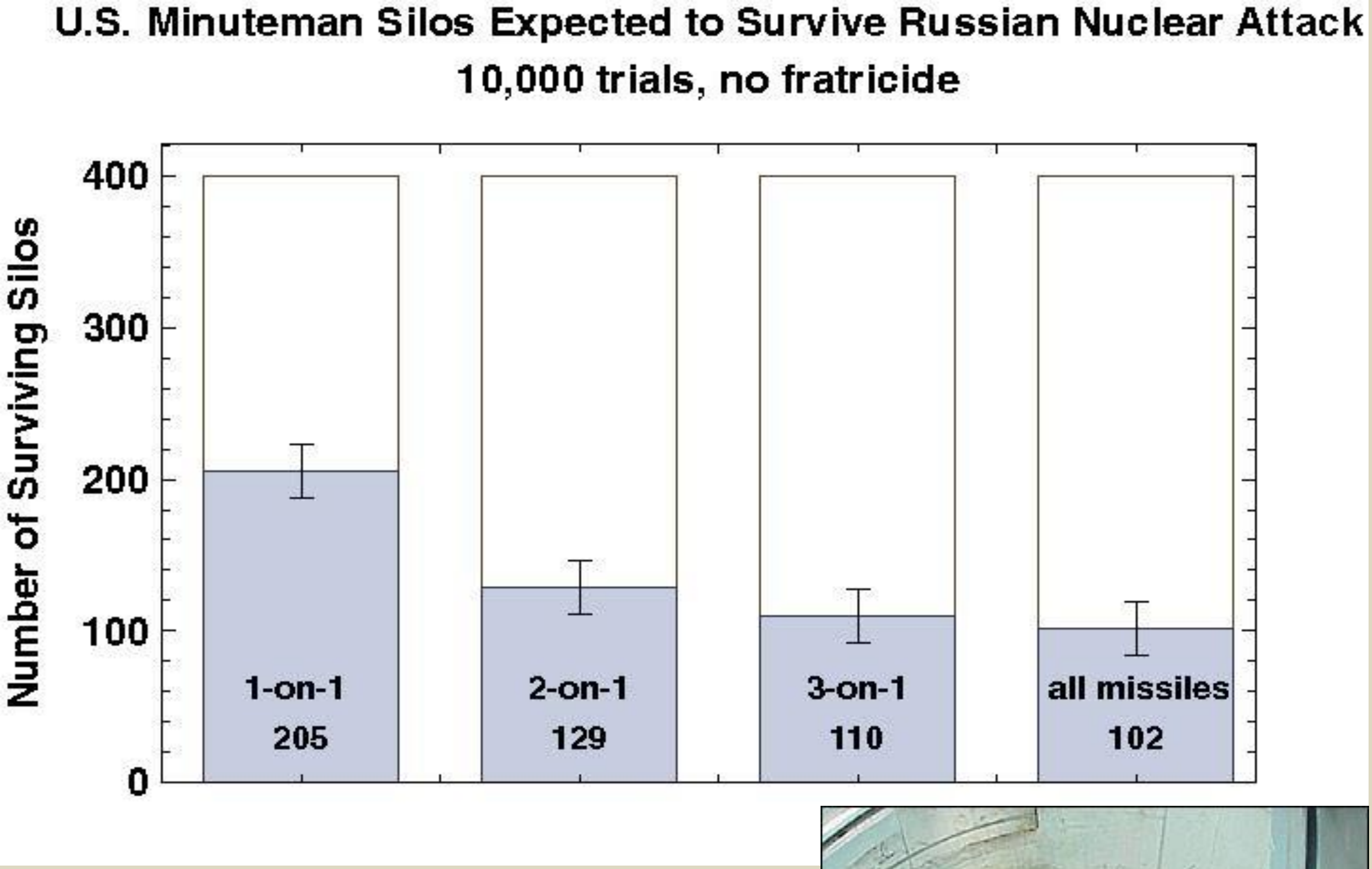


Figure 1: Results of simulated attacks on U.S. missile silos by Russian deployed ballistic missiles 1-, 2- and 3-warheads per silo, as well as all ballistic missiles (214 silos targeted at 3-to-1 and 186 silos targeted 4-to-1). Error bars are 95 percent confidence intervals.

Now consider the case after an all-out Russian attack in which the United States did not launch its missile on warning. The 300 counter-missile targets are no longer meaningful targets, since Russia used those weapons in its attack. The other types of targets remain, but now the United States can be expected to have, in the worst case, 102 warheads for these targets where the initial plan designated 100. The situation for the United States is nearly the same regardless of whether the land-based missiles were launched on warning of an incoming attack or not. The remaining U.S. land-based missile force would therefore be adequate to perform its original mission. Moreover, the hundreds of additional submarine- and bomber-based weapons would continue to provide an excellent deterrent against other adversaries or any rebuilt Russian force.

**The Counterargument**

Given these findings — which we assume are known to military planners — as well as longstanding criticism from former presidents and Strategic Command commanders, the perpetuation of the launch under attack option is curious. The last five Nuclear Posture Reviews have defended the policy using largely identical language:

From the 2002 Nuclear Posture Review: “U.S. forces are not on ‘hair trigger’ alert and rigorous safeguards exist to ensure the highest levels of nuclear weapons safety, security, reliability, and command and control. Multiple, stringent procedural and technical safeguards are in place to guard against U.S. accidental and unauthorized launch. ”

20 years later, the 2022 Nuclear Posture Review provides basically the same defense: “U.S. intercontinental ballistic missiles (ICBMs) are not on ‘hair trigger’ alert. These forces are on day-to-day alert, a posture that contributes to strategic stability. Forces on day-to-day alert are subject to multiple layers of control, and the United States maintains rigorous procedural and technical safeguards to prevent misinformed, accidental, or unauthorized launch.”

Unfortunately, these defenses are naive to the kinds of failures that can emerge in complex systems.

The United States uses “dual phenomenology” to assess missile launches prior to launching a retaliatory strike. As the name suggests, it depends on two independent sensor systems to provide warning of incoming ballistic missiles: The Space Based-Infrared System satellites detect missile launches, and the Upgraded Early Warning Radars track incoming missiles. To fulfill the requirements of dual phenomenology, an incoming missile must be detected by both satellite and radar. While this is a useful safeguard, it does not provide any assurance that the incoming missile carries a nuclear weapon or that those weapons are armed. For instance, missile flight tests are conducted unarmed, and Russia has conducted flight tests from Dombarovsky, which also hosts some of Russia’s silo-based missile forces. An accidental launch from that field may be an unarmed missile. There are other scenarios as well.

Once sensor information is received and evaluated, the alert is advanced up the chain of command through multiple “conferences” until it reaches the president. These conferences are intended to avoid mistakes. However, the whole process leaves only a few minutes to make critical decisions. The president would have at most 20 minutes for incoming land-based missiles and as little as zero minutes for Russian submarine-based missiles based near the United States to decide whether to retaliate. Particularly for Russia’s submarine-based missiles, this timeline is extremely tight, which puts immense pressure on all involved — all without knowing the intent, character, or payload of the incoming missiles. Even if these procedures constitute “rigorous procedural and technical safeguards,” the fact remains that sensors provide unacceptably incomplete information on which to base nuclear war.

Perhaps the biggest risk arises from nonrandom errors, like the one that occurred on Nov. 9, 1979, when North American Aerospace Defense Command received sensor warnings of incoming missiles. The early-warning system showed 250 and then 2,200 missiles incoming from the Soviet Union. The problem was not a technical malfunction: Rather, a training tape was accidentally left in place, and it simulated the information needed to confirm that the launches were authentic.

In addition to human error, there may be common-mode technical failures in electronics or software. Depending on where these occur, they may give the appearance of detections confirmed by redundant sensor systems. For example, on June 3, 1980, a circuit chip failure caused North American Aerospace Defense Command screens to display 200 incoming missiles rather than 000. A similar glitch was responsible for triggering the apparent self-launch of a U.S. missile mentioned at the start of this article.

The only way to be confident that the United States is being attacked with a nuclear weapon is to wait until sensors detect an actual detonation. Unpleasant as that may seem, it bears remembering that whether the United States launches its retaliation before or after the detonation does not change the number of detonations over U.S. soil. Launch under attack cannot reduce U.S. causalities, but it could increase them by unintentionally initiating a nuclear war that didn’t exist. With the stakes so high and missile survivability already adequate, it would be prudent to wait until detonations are confirmed.

## A Technical Imperative?

Prior to his becoming Secretary of Defense in 2017, Marine Corps Gen. James Mattis argued that the silo-based missiles were not needed because U.S. submarines were undetectable and would therefore always be capable of retaliation. Proponents of launch under attack now argue that advances in technology could make the submarines at sea vulnerable to attack. While it is true that vulnerable submarines could undermine America’s retaliatory capability, we have shown here that retaliation does not need to hinge on the availability of submarines: Plenty of silo-based missiles will survive. Moreover, there is no evidence that submarines are becoming vulnerable, but if they did, and if Russian forces improved to such a point that enough U.S. silo-based missiles were genuinely at risk, then the Lunch Under Attack policy could always be reinstated.

By contrast, the technical landscape that is actually emerging today suggests it might be time to look beyond Launch Under Attack, because it provides insufficient protection. Increasingly, U.S. adversaries are fielding delivery vehicles that are undetectable by the current suite of sensors, namely cruise missiles and hypersonic vehicles. Without the ability to detect and track all possible delivery vehicles, assured retaliation will require the use of other sources of intelligence beyond the sensors used for dual phenomenology. Thus, the logic of launch on warning, and the technical systems propping up that policy, provides a veil of strong protection but actually falls short of what is now needed.

Similarly, over-reliance on this system leaves the United States under-prepared for detection failures. For example, anti-satellite weapons, including simple ground-based lasers, could disable early-warning satellites. Without satellite detection, the requirements of dual phenomenology could not be fulfilled. It is unclear what would happen at this point. Would the launch under attack policy degenerate to a one-phenomenon launch policy? In that situation, it would take longer for incoming missiles to come within range of the radars, so decision makers would have even less time to evaluate missile threats, on top of needing to assess whether the blinded sensors were caused by a technical malfunction, a hostile act by the attacker, or a third party aiming to introduce confusion. Instead of holding fast to the idea of immediate launch, it is far sounder to build a nuclear capability that can survive a first strike and for which decision-makers are not pressed to make decisions with incomplete information. Fortunately, that condition already exists today, and such a launch policy should be implemented now.

### Bottom Line

The United States currently maintains the option to launch under attack so that in the event of first strike by Russia, U.S. silo-based missiles could be launched before they are be destroyed. However, our simulations find that 100-200 silo-based missiles would survive, which would likely leave the United States with more warheads per retaliatory target than before the Russian strike. As such, the United States would suffer no meaningful loss of capability and should update its policy to eliminate the Launch Under Attack option in order to reduce risks of accidental nuclear war caused by technical glitches, human error, or cyber-attack. Revising this policy does not lock the United States into any particular posture: If technologies change, the policy could be reinstated. In the meantime, the United States should strive to deploy a more robust, less provocative, and less dangerous system that is better tuned to emerging threats. There has not yet been a false alarm that prompted an actual nuclear launch, but there's no need to bet the entire world on the hope it will never happen.

**Natalie Montoya** is a technical associate at the Laboratory for Nuclear Security and Policy in the Department of Nuclear Science & Engineering at the Massachusetts Institute of Technology. Previously, Natalie was the 2021–2022 James C. Gaither Junior Fellow in the Nuclear Policy Program at the Carnegie Endowment for International Peace.
**R. Scott Kemp** is associate professor of nuclear science and engineering at the Massachusetts Institute of Technology and director of the Laboratory for Nuclear Security and Policy.

## The Biden administration overestimates radiological terrorism risks and underplays biothreats

**By Zachary Kallenborn**

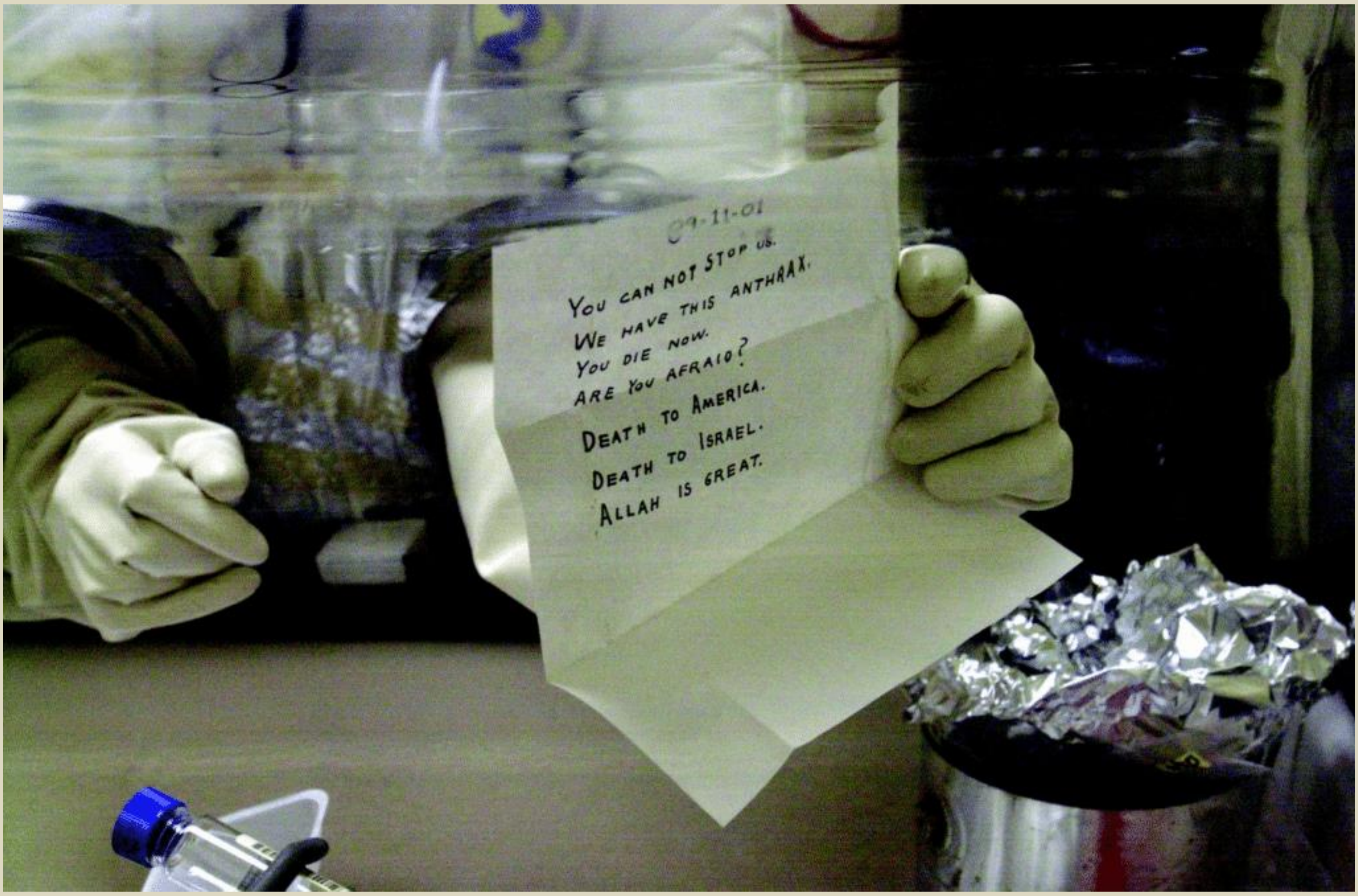
Source: https://thebulletin.org/2023/03/the-biden-administration-overestimates-radiological-terrorism-risks-and-underplays-biothreats/

Mar 17 – President Joe Biden earlier this month signed a new national security memorandum to counter weapons of mass destruction (WMD) terrorism. The memorandum is classified, but a publicly accessible fact-sheet sets out the American strategy to combat WMD terrorism, including by preventing terrorists from accessing WMD material, detecting and deterring threats, and enhancing domestic and international capabilities to counter WMD terrorism. In particular, the plan emphasizes the safeguarding of nuclear and radiological material, which could be diverted into weapons. In one crucial respect, however, the administration gets it wrong.
Although the anti-terror strategy's focus on nuclear security is somewhat justified given the potential for massive harm, the radiological security emphasis is not. Rather, the emphasis should have been on biological terrorism. Among WMD terrorism modes, bioterrorism risks are increasing most, even if the overall likelihood remains low. At the same time, new mass casualty terror threats are emerging that do not neatly fit into the WMD terrorism framework. The administration's memorandum can be compared to a police department that prioritizes serial killers and jaywalkers. One priority can be defended, but does not capture the full scope of concerns; the other is, frankly, a bit odd.

### An insignificant threat?

In a radiological attack, a terrorist might use an explosive like dynamite to contaminate a target with radioactive material. So-called "dirty bombs" are different from nuclear weapons like atomic bombs, which, by splitting atoms, release a huge amount of explosive energy. Of all the forms of WMD terror—usually conceived of as attacks that use chemical, biological, radiological, or nuclear weapons—radiological terrorism attacks are easily the lowest risk.
There have been basically no successful examples of radiological terrorism, and attempts are rare, even for already-rare WMD terrorism. START's Global Terrorism Database, which documents over 200,000 terrorist attacks domestically and internationally, includes only 13 incidents of radiological terrorism, none of which caused any injuries or deaths. And one man carried out 10 of the attacks: Tsugio Uchinishi, a Japanese man who mailed monazite powder, which contains the radioactive element thorium, to various Japanese agencies to warn the government about exports of uranium to North Korea. Although reports that the Islamic State

acquired 40 kilograms of uranium generated plenty of media attention, uranium is not actually all that radioactive and would have caused minimal harm, especially compared to other Islamic State attacks. The reality is radioactive material does not add much to a terror attack, except a tad bit more economic harm and unwarranted media attention.



09-11-01
YOU CAN NOT STOP US.
WE HAVE THIS ANTHRAX.
YOU DIE NOW.
ARE YOU AFRAID?
DEATH TO AMERICA.
DEATH TO ISRAEL.
ALLAH IS GREAT.

A piece of evidence from the Amerithrax investigation into anthrax-laced postings. Credit: FBI.

Even theoretically, the consequences of radiological terrorism are quite low. In a dirty bomb, most of the harm comes from the explosion. The radioactive material creates an increased risk of cancer while adding to potential clean-up costs. Even in the most extreme forms, the primary harm is as a weapon of mass disruption: closing an important port, say, until a costly clean-up can be completed. Although inciting a nuclear meltdown could conceivably cause mass harm, it's extraordinarily difficult due to existing protections and the administration's "radioactive material security" program does not appear to do anything for nuclear power plant security anyway. Compare the radiological terror consequence to a nuclear terrorist attack that could destroy a city, or an extreme bioterrorism attack that could conceivably kill more people than have died in the COVID-19 pandemic. The difference is stark.

In fairness, the accessibility of radiological material drives the risk. Blood transfusion devices in many hospitals use highly radioactive cesium-137, for example. Even household smoke detectors can have very small amounts of radioactive material, though a massive amount would be required to make a dirty bomb of any consequence. The memorandum, therefore, is useful in risk reduction, even if radiological terrorism does not deserve such a high priority in the administration's anti-terror plans.

### Emerging WMD threats

Among WMD terrorist threats, the barriers to bioterrorism are going down the most. Synthetic biology provides a pathway for terrorists to acquire highly controlled pathogens, such as the variola virus (the causative agent of smallpox). 3-D printing enables printing materials for lab equipment and potentially easier access to harmful pathogens, too. Online marketplaces also offer an avenue to acquire laboratory equipment usable in biological weapons programs with limited oversight. Plus, ubiquitous drone technology could be relatively easily used for the dispersal of chemical and biological weapons agents. Of particular concern are agricultural drones for dispersing pesticides, which are practically purpose-built to deliver biological weapons agents. These developments are leading to a broader de-skilling (or at least a shift in the type of skills required) of the expertise needed to develop and use biological weapons agents. This is not to say bioterrorism is easy. Even if a terrorist used synthetic biology to acquire a pathogen, acquired pesticide drones to deliver the aerosol, and used 3-D printing and online markets to acquire lab supplies and equipment, the terrorist would still need to mass produce the pathogen and weaponize it without a lab accident or discovery by law enforcement. Consequently, successful bioterror attacks are rare, and, despite alarms, COVID-19 is unlikely to change that possibility much.

But unlike radiological terrorism, terrorists have pulled off major biological weapons attacks and attempted extreme forms. The START Global Terrorism Database documents 38 incidents of bioterrorism, most significantly the Rajneeshee cult attack that sickened 751 in the Dalles, Oregon in 1984. And, of course, in the so-called Amerithrax attacks in 2001, mailed letters containing *bacillus anthracis* (the causative agent of anthrax) killed five and injured 17. There have also been major attempts, such as Aum Shinrikyo's failed attempts to use biological weapons to ignite an apocalyptic war, and the radical environmentalist group RISE's attempt to wipe out humanity and re-populate the Earth with environmentally sensitive revolutionaries.

At the same time, new WMD terrorist threats are emerging. Drone swarms are a new WMD, given their ability to cause mass harm and lack of reliability. Although terrorists still face considerable difficulty in acquiring true drone swarms with intra-swarm communication, the risk is trending upward. At the same time, developments in nanotechnology—a branch of technology interested in manipulating matter at the nano-scale (1 to 100 nanometers)—offer terrorists a new means to acquire chemical and biological-terrorism-like weapons. Cyberterrorism is also plausible, with the growth of the internet of things offering new vulnerabilities for hostile actors to cause harm.

**What should have been done?**

Overall, the Biden administration plan does provide a good baseline for addressing the continued threat of WMD terrorism. Despite the focus of US security policy moving away from terrorism to counter the rise of China, WMD terrorism still deserves serious attention, especially as governmental pressure on disrupting terror organizations wanes. But the policy specifics should align more directly with the threat landscape, current and future.

Given the growing risks of bioterrorism risks, US officials should have a particular focus on searching for and sharing information about radicalized experts. Access to relevant technical expertise still remains a major barrier, and building biological weapons requires significant tacit knowledge, the subtle knowledge that comes from working in a lab for a long time that cannot be explained. The best example is Aum Shinrikyo; despite being incredibly well-resourced, its biological weapons program struggled. In one case, a cult member fell into a fermenting tank of *clostridium botulinum*, the bacteria that produce the botulinum toxin that is lethal in microgram amounts—and emerged unharmed. The cult had over $1 billion in assets, yet was unable to acquire the necessary skills for a successful bioattack.

In addition, the United States should undertake national and global efforts to improve biosecurity and biodefense, especially concerning synthetic biology. For example, the United States might focus on facilitating and encouraging discussion between different scientific disciplines and global regulators concerning genetic engineering regulations, domestically and globally. Similarly, a recent US Government Accountability Office (GAO) review found 21 of 29 long-standing recommendations to improve US biodefense remain unimplemented. The United States could also encourage transparency, education, and risk reduction around the global proliferation of biosecurity level 3 and 4 (BSL-3 and BSL-4) laboratories that handle the world's deadliest pathogens.

The United States also needs to update the global framework for combating WMD terrorism to address new threats. UN Security Council Resolution 1540 prohibits states from providing support to chemical, biological, radiological, or nuclear terrorism and requires the adoption and enforcement of laws to prevent proliferation—but says nothing about the drone, nanotech, or cyber threats. Although it's unclear whether the resolution is the right vehicle for addressing emerging WMD concerns given a lack of appetite to expand the resolution's scope, the approach of encouraging countries to adopt legal controls on WMD-related material remains a good one. Similarly, the United States needs to adopt new measures to restrict the proliferation of new, WMD-related technologies, such as requiring new approvals on the production, purchase, and export of pesticide-delivery drones.

The reality is that terrorists do not require WMD to cause major, even existential harm. Terrorist attacks to incite or prevent the de-escalation of a conflict between the United States and China, for instance, may only require a bomb or a well-placed bullet. Moreover, the United States and the global community should not treat WMD terrorism as an isolated threat. Virtually all forms of WMD terrorism require significant financial resources and technical expertise. Degrading, disrupting, and destroying general terror organizational capacity is of tremendous value in reducing the threat.

WMD terrorism remains a serious threat to the country and the globe, but the American approach needs to be aligned with genuine risks to ensure security today and tomorrow.

**Zachary Kallenborn** is a research affiliate with the Unconventional Weapons and Technology Division of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), a policy fellow at the Schar School of Policy and Government, a US Army Training and Doctrine Command "Mad

Scientist," and national security consultant. His work has been published in a wide range of peer-reviewed, trade, and popular outlets, including Foreign Policy, Slate, War on the Rocks, and the Nonproliferation Review. Journalists have written about and shared that research in outlets including Forbes, Popular Mechanics, Wired, The Federalist, Yahoo News!, and the National Interest.

**EDITOR'S COMMENT:** Biden administration loves surprises! They also like to confuse "destruction" with "disruption" for their own reasons.

## Man arrested in radioactive mail case

**By Sandy Perle**

Source: http://health.phys.iit.edu/extended_archive/0006/msg00375.html

June 2000 – Police on Saturday arrested a 42-year-old man on suspicion of mailing radioactive material to 10 government offices last week with messages claiming that uranium was being smuggled to North Korea by a person related to an Education Ministry-affiliated foundation.

The suspect, Tsugio Uchinishi, has admitted to mailing **monazite** powder to the offices, saying he wanted to draw attention to his allegation that a 73-year-old man claiming to be an adviser to the dormant Nihon Bosei Bunka Kyokai foundation was smuggling uranium to North Korea, police officials said.

Uchinishi, who lives in Tokyo's Nakano Ward and runs a building-demolishing business, told police he wanted to block the alleged smuggling to North Korea and maintained that he acted alone, they said.

Police suspect that the alleged adviser wanted to smuggle monazite to North Korea, but that it is unlikely that monazite was actually exported to North Korea, the officials said. According to police, Uchinishi mailed 10 envelopes containing small amounts of monazite June 4 to 10 government offices, including the official residence of Prime Minister Yoshiro Mori, the Defense Agency and the Education Ministry, in violation of the Postal Law.

Monazite contains very small amounts of uranium and thorium, nuclear fuel materials. However, the quantities of monazite sent are believed to be too small to constitute a health hazard. Police said they confirmed the sender as Uchinishi through the handwriting on the envelopes. The Postal Law prohibits the mailing of explosives, combustibles or materials with radioactivity levels above 74 becquerels per gram. Violators are subject to a maximum fine of 500,000 yen.

The name of the alleged adviser appeared in a message included in the envelopes. The message claimed the adviser was smuggling 70 tons of uranium to North Korea via Niigata port on the Sea of Japan coast for the production of nuclear weapons, police sources said. Investigators are questioning Uchinishi as to how he obtained the monazite.

The director of the foundation, 84-year-old Hiroshi Ikeda, allegedly imported some 40 tons of monazite from Thailand about 20 years ago for research purposes and sale to hot springs that use radium and thorium.

Of the 40 tons, about 17 tons were found to have been stored in several locations in Japan, including 15 tons in Tatsuno, Nagano Prefecture, police said. Informed sources said the 15 tons of monazite had been stored in Ichikawa, Chiba Prefecture, but the adviser shipped them to Tatsuno, and later asked a transport firm to haul them to Niigata.

The monazite was not actually taken to Niigata, according to the sources. Whereabouts of the remaining 23 tons of monazite are not known.

**Sandy Perle** is the Director, Technical ICN Worldwide Dosimetry Division, ICN Biomedicals, Inc., USA

## Radioactive Leak at Minnesota Nuclear Plant Revealed Months After Accident

Source: https://www.sciencealert.com/radioactive-leak-at-minnesota-nuclear-plant-revealed-months-after-accident

Mar 20 – The operator of a nuclear facility in Minnesota said on Thursday the plant suffered a leak last November of water containing radioactive tritium, but that contamination was largely limited to the plant itself. Xcel Energy, operator of the nuclear plant northwest of Minneapolis in the Midwest state of Minnesota, did not say why it waited **more than three months** to acknowledge the leak to the public.

Buildings at the Monticello Nuclear Generating Plant. (Nuclear Regulatory Commission from US/CC BY 2.0/Wikimedia Commons)

The company said it notified state officials and the federal Nuclear Regulatory Commission (NRC) once it learned of the leak on November 22. "While this leak does not pose a risk to the public or the environment, we take this very seriously and are working to safely address the situation," Chris Clark, the utility's president, said in a statement. The Minnesota Pollution Control Agency said the company told it some 400,000 gallons of water containing tritium leaked at the site, but none "reached the Mississippi River or contaminated drinking water sources". State officials "are actively reviewing data" from the site and "overseeing remediation efforts," the agency said. The company said it has "recovered about 25 percent of the tritium released and will continue recovery over the course of the year". The leak originated in "a water pipe between two buildings" at the Monticello nuclear plant.

Tritium is a radioactive isotope of hydrogen that is a byproduct of the production of electricity at nuclear plants. It can also occur naturally in the environment. Monticello is 63 kilometers (39 miles) northwest of Minneapolis, the largest city in the state, and also where Xcel Energy has its headquarters. Xcel said it detected the spill while doing routine groundwater testing.

It said it contained the leak by diverting water to an in-plant treatment facility, and will need to build "large storage tanks… to store recovered water until it can be treated and reused." The company said it is conducting more frequent tests from some two dozen groundwater monitoring wells in and around the site. The US has suffered one major nuclear accident in its history – the meltdown of the Three Mile Island reactor in Pennsylvania on March 28, 1979. **Some 92 nuclear reactors provide power to tens of millions of US homes.** Smaller accidents have occurred over the years but usually contained with localized impacts.

## Are We Prepared for a North Korean Nuclear Attack?

**By Richard Weitz**

Source: https://nationalinterest.org/blog/korea-watch/are-we-prepared-north-korean-nuclear-attack-206279

Mar 06 – Since President Joe Biden assumed office in January 2021, North Korea has ended its provocation pause and test-launched more missiles than ever, aiming to perfect its means of attacking the United States and its allies with nuclear weapons. The United States and its partners have strived to parry these threats through enhanced diplomacy, sanctions, deterrence, and a combination of offensive and defensive military capabilities.

The Democratic People's Republic of Korea (DPRK) has resumed testing its intercontinental ballistic missiles (ICBMs), which are designed to deliver a nuclear warhead against the United States. On February 18, the DPRK simulated a short-notice launch of its Hwasong-15 ICBM, rehearsing how to initiate nuclear strikes before the United States and its allies fully mobilize their defenses. The missile flew deep into outer space, more than a dozen times higher than the International Space Station. It could have landed anywhere in the United States if launched on a flatter trajectory.

This test is further evidence that the DPRK missile arsenal is increasing in quantity and improving in quality. Since it began its "turbocharged testing spree" last year, the North launched more nuclear-capable missiles than in any previous year. Many of these launches displayed innovative techniques and technologies intended to negate existing U.S. and allied defenses, such as using many missiles concurrently to overwhelm defenders, launching missiles from rail-mobile and submarine-based platforms, and employing hypersonic glide technologies that enable the warhead's reentry vehicle to maneuver while descending on a target.

At the same time, the DPRK's leader, Kim Jong-un, has declared his country's nuclear status to be "irreversible." Furthermore, the DPRK adopted a new law that may authorize DPRK field commanders to launch preemptive nuclear strikes and automatic retaliatory attacks if Kim is de-capitated. Additional enhancements to the DPRK missile arsenal are coming. In December 2022, Kim called for an "exponential" augmentation in the country's weaponry, including serial manufacture of tactical nuclear weapons, reconnaissance satellites to assist with long-range missile strikes, and ICBMs intended for rapid counterstrikes against U.S. targets. Having resumed fissile material production, the DPRK might have several hundred nuclear-armed missiles by the end of this decade.

## Missile Motives

Pyongyang pursues nuclear-armed missiles for power, prestige, and profits. The missiles aim to deter and, if necessary, defeat the United States and its allies, boost the North's status and global attention, distract foreign and domestic observers from the DPRK's economic and political flaws, and enhance the North's leverage for extracting money and other Western concessions.

In peacetime, the North can leverage its missiles to coerce concessions from the United States and its allies. In a conflict, they provide the DPRK with a shield behind which to wage aggressive regional wars. Following the Russian playbook in Ukraine, Pyongyang's policymakers might aspire to attack another country and then brandish its nuclear arsenal to deter a U.S. military response. American officials have acknowledged that possibility could weaken Washington's extended deterrence guarantees to protect its Asian allies like Japan and South Korea. The DPRK wants these countries to doubt U.S. pledges to protect them—inducing them to appease rather than resist the North's demands.

## Fruitlessly Unconstrained

Three decades of negotiations, sanctions, and military countermeasures have failed to induce North Korea to relinquish its nuclear weapons aspirations. Past efforts to convince North Koreans that they would be more secure without nuclear weapons, offering the DPRK security assurances and confidence-building measures, or dangling visions of wealth and international acceptance have all proved insufficiently enticing. The DPRK has dismissed the Biden administration's offers to resume direct talks despite proposals for "calibrated" diplomatic measures to decrease tensions with the North, dispel misperceptions that the United States threatens the DPRK, and facilitate North Korea's return to compliance with its nuclear obligations.

The many sanctions adopted by the international community have restricted DPRK imports and exports, contributed to the isolation of the DPRK leadership, and constrained the North's financial resources, but they have not halted the North's missile development programs. Beijing and Moscow no longer enforce many existing sanctions and refuse to adopt new ones. Chinese and Russian leaders see DPRK provocations as mischievously helpful for distracting the United States from focusing on Beijing and Moscow.

**Spurring Proliferation**

The credibility of U.S. pledges to defend South Korea and Japan with all possible means, including U.S. nuclear weapons, was weakening even before the DPRK's recent provocations. For several years, opinion polls indicate that most South Koreans want to acquire their own nuclear weapons or induce Washington to return U.S. nuclear weapons to South Korea. Some Japanese leaders have also more openly discussed their country's nuclear weapons options in recent years. These views plausibly reflect the belief that the North will never abandon its nuclear weapons while the United States might prove unwilling to use its nuclear forces against North Korea if the DPRK could retaliate with nuclear strikes against U.S. territory.

U.S. officials and analysts have discouraged allies from pursuing nuclear weapons for fears of legitimizing the DPRK's nuclear arsenal, spurring further nuclear proliferation, promoting regional arms races, and decreasing crisis stability. By seeking nuclear weapons, Japan and South Korea would antagonize the United States and other governments, demean their countries' lofty international reputations, expose themselves to economic sanctions, and intensify first-strike incentives in a crisis. Instead, the United States has assisted its allies to enhance their missile defenses, damage limitation, and other non-nuclear capabilities.

Furthermore, the Biden administration made bolstering the credibility of U.S. extended security guarantees to these Asian partners one of the highest priorities of the recently completed U.S. Nuclear Posture and Missile Defense Reviews. The first review explicitly warns that the United States will destroy the DPRK regime should it use nuclear weapons: "Any nuclear attack by North Korea against the United States or its Allies and partners is unacceptable and will result in the end of that regime." The need to reassure allies like South Korea and Japan, which rely on U.S. nuclear weapons for defense against major non-nuclear as well as nuclear attacks, was a major factor leading the Biden administration to reject proposals to adopt a "sole-purpose" or "no-first-use" declaratory doctrine. Such a declaration would have committed the administration to employ nuclear weapons only after an aggressor country had used them against the United States.

**Opportunities for Defense**

Yet, there is no attractive offensive military option available to the United States. Even with U.S. nuclear forces, a limited preemptive strike may not destroy all DPRK weapons of mass destruction, which are widely dispersed in concealed and hardened facilities. A U.S. first strike could easily precipitate a conventional war on the Korean Peninsula even more destructive than the one seen in Ukraine. The United States and other defenders will attempt to disrupt North Korea's missiles through cyber attacks, electronic warfare, and other non-kinetic means, but DPRK designers have enhanced their missiles from such vulnerabilities.

The Biden administration's Missile Defense Review, therefore, insists that "the United States will also continue to stay ahead of North Korean missile threats to the homeland through a comprehensive missile defeat approach, complemented by the credible threat of direct cost imposition through nuclear and non-nuclear means." These words echo those of the Trump administration's Missile Defense Review, which affirmed that the United States would "continually improve [U.S.] defensive capabilities as needed to stay ahead of North Korean missile threats if they continue to grow, while also taking steps to preclude an arms race with China or Russia."

Following the most recent DPRK missile test, U.S. Representative Mike Rogers, Chairman of the House Armed Services Committee, released a statement affirming that "Protecting the U.S. homeland must be paramount as we develop our 2024 budget, and this includes fully-funding homeland missile defense assets." Even imperfect missile defenses can help deter and defeat attacks by complicating a potential missile aggressor's certainty of success. They can also reassure allies that they do not need nuclear weapons or to appease those who are threatening them.

The foundation of the U.S. homeland defense against DPRK missiles is the fleet of Ground-Based Interceptors (GBIs) in Alaska and California that underpin the Ground-Based Midcourse Defense architecture over North America. These multi-stage solid-fueled rocket boosters are equipped with an unarmed Exo-Atmospheric Kill Vehicle, that collides with a target in outer space, obliterating it with kinetic energy. Presently only a few dozen interceptors protect the continental United States from incoming ICBMs. Unfortunately, the United States rushed these GBIs into service in the early 2000s and has not yet comprehensively renewed them. Instead, they have received only patched upgrades and infrequent tests. At this point, the potential for further upgrading the original GBIs is limited given their decades-old technology, calling into question their efficacy of dealing with the North's rapidly expanding capabilities.

The United States is, therefore, developing a Next Generation Interceptor (NGI) to provide a more reliable kill vehicle to address the expanding North Korean missile threat. Though an entirely new system built from the ground up, the NGI technology maturation plan aims for an evolutionary rather than revolutionary increase in capabilities. Its improved command, control, communications, and sensor capabilities will increase the system's reliability. The NGI's larger payload can carry more than one kill vehicle on each interceptor. Its greater propulsion than the GBI will bring the kill vehicles faster to their interception points, giving warfighters makers more time to make decisions, more opportunities to address complex threats, and more assured means of discriminating between decoys and genuine targets. With planned deployment by 2028, the NGI's modularity and preplanned upgrades will enable the United States to address subsequent threats more rapidly and confidently.

The Missile Defense Agency, responsible for overseeing the systems requirements and design review for the interceptors, has admirably promoted competition between two contracting teams to accelerate the delivery timeline, drive down costs, and limit technical risk. Meeting this performance metric will require testing the GBI frequently in demanding scenarios, independently and in combination with other elements to enhance performance. For some of these enablers, it might be prudent for the Agency to accept more risks with technology development programs, such as those intended to thwart emerging threats like hypersonic missiles. The planned upgrades to the existing network of sensors, command-and-control nodes, cyber defenses, and other critical support systems will also make the current GBI fleet more effective, pending the eventual deployment of the NGI. Extending the NGI competition through a prototype fly-off would further ensure the fielding of the most capable interceptor.

To construct a multi-layered defense architecture against the DPRK's ICBM-class targets that protects Hawaii and Guam as well as the Continental United States, the Pentagon will need to integrate the NGIs with regional missile defenses. In the Indo-Pacific region, these include the Aegis-equipped Standard Missile interceptors deployed on ships along with the land-based Patriot and Terminal High Altitude Area Defense systems. Besides protecting U.S. deployed forces and allies, these regional missile defenses can provide important warning and tracking data of ICBMs launched from North Korea toward the United States. The potential effectiveness of such local systems has been evident in Ukraine, where even less advanced regional missile defenses have worked well in blunting the Russian missile onslaught. A comprehensive global defense architecture could also help protect the United States and its allies and forces from missiles launched by other countries.

The long-term solution to the Korean crisis is internal regime change and reunification under a government that resembles present-day South Korea. Yet, no one knows how long this process could take given the ruthless effectiveness of the DPRK's totalitarian regime. In the interim, having a robust spectrum of defense capabilities, suitable for a range of scenarios, is critical given the rapidly evolving threat environment.

**Richard Weitz** is the director of the Center for Political-Military Analysis and a senior fellow at the Hudson Institute.

## North Korea claims to have tested a nuclear-capable underwater drone

**By Brad Lendon and Yoonjung Seo** (CNN)

Source: https://edition.cnn.com/2023/03/23/asia/north-korea-underwater-drone-test-intl-hnk-ml/index.html

Mar 23 – North Korea on Friday claimed it had tested an underwater drone capable of carrying a nuclear warhead that could create a "radioactive tsunami" – however analysts urged skepticism.

A report from the state-run Korean Central News Agency (KCNA) said the drone, called the "Unmanned Underwater Nuclear Attack Craft 'Haeil,'" was tested from March 21 to 23, cruising in waters off the country's east coast for more than 59 hours before its test warhead was detonated on Thursday afternoon.

"The mission of the underwater nuclear strategic weapon is to stealthily infiltrate into operational waters and make a super-scale radioactive tsunami through underwater explosion to destroy naval striker groups and major operational ports of the enemy," the KCNA report said.

The KCNA report said the weapon has been in development since 2012 and has undergone more than 50 tests in the past two years. This week's test "verified its reliability and safety and fully confirmed its lethal strike capability," the KCNA report said, adding the drone can be deployed from any port or towed by a surface ship to begin its operations.

Analysts poured doubt on North Korea's claims.

"Pyongyang's latest claim to have a nuclear-capable underwater drone should be met with skepticism" because North Korea offered no proof, said Leif-Eric Easley, associate professor of international studies at Ewha Womans University in Seoul.

Writing on social media, Ankit Panda, a nuclear policy expert at the Carnegie Endowment for International Peace, said: "I tend to take North Korea seriously, but can't rule out the possibility that this is an attempt at deception/psyop."

"Would be ill-advised to allocate limited fizmat (fissile material) for a warhead to go in this thing, IMO, vs. more road-mobile ballistic missiles," Panda added.

The idea of an unmanned submersible carrying a nuclear warhead is not unique to North Korea.

Russia claims to have developed the Poseidon torpedo, a submarine-launched, nuclear-powered unmanned underwater vehicle capable of carrying both conventional and nuclear munitions. Its nuclear propulsion system would give the Poseidon virtually limitless range.

But Russia has offered no proof of a successful test of the Poseidon and analysts suspect it could be years from deployment.

**North Korea's purported new underwater weapon has important differences from the Poseidon. It is conventionally powered and is not launched from a sub, meaning it would not be on a par with the Russian torpedo, the analysts said.**

**Missile tests**

North Korea's drone test claim comes at the same time Pyongyang said it tested nuclear-capable cruise missiles this week.

Four of the subsonic missiles hit targets in the East Sea, also known as the Sea of Japan, after flying oval and figure-8 patterns of 1,500 and 1,800 kilometers (932 and 1,118 miles) on Wednesday, KCNA reported.

Wednesday's drill "let strategic cruise missile units get familiar with the procedures and processes for carrying out the tactical nuclear attack missions," the report said.

The state-run Rodong Sinmun released a series of photos on its website purportedly showing the cruise missiles and the underwater drone.

The KCNA report said Pyongyang's nuclear weapons development was necessary to counter "the reckless military provocations being escalated by the U.S. and the South Korean authorities."

US and South Korean forces have been holding their biggest war games in five years on the southern part of the Korean Peninsula.

North Korea has been testing various missiles at the same time, including the test of an intercontinental ballistic missile last week and the tests of smaller range missiles like the cruise missiles tested on Wednesday.

Analysts say Pyongyang is delivering a message to the US and its allies in the region.

"North Korea's ICBM tests are thinly veiled threats that it could potentially destroy American cities," Easley said. "Its recent short-range missile firings attempt to increase the credibility, command, and control of its self-proclaimed tactical nuclear weapons units aimed at South Korea and Japan."

YOU KNOW, UN EXPERTS SAY THAT FUKUSHIMA'S RADIATION HAS CAUSED NO PARTICULARLY HARMFUL EFFECTS FOR OUR HEALTH
OH, THAT'S REASSURING
@ferranmartin
Ferran 2021

International CBRNE Institute

CBRNE-Terrorism Newsletter

C2BRNE DIARY

# EXPLOSIVE NEWS

## Dozens of bomb manuals found in crackdown on terrorist groups

Source: https://www.thenationalnews.com/world/europe/2023/02/24/dozens-of-bomb-manuals-found-in-crackdown-on-terrorist-groups/

Feb 24 – Police forces across Europe have discovered dozens of bomb manuals for creating chemical weapons.

Special counter-terrorism units from 17 countries worked together with Europol's European Counter Terrorism Centre to restrict access to instructions online on how to use high-risk chemicals for terrorist attacks.

Investigators scoured the web to identify and refer for removal, propaganda and instructions on the use of high-risk chemicals, and the toxic gases they generate, in terrorist material.

A number of chemicals routinely used in industrial processes or professional functions can react upon mixing, producing hazardous substances that could be used to carry out chemical terrorist attacks.

The investigation resulted in more than 120 instances of content being referred to 21 online service providers to ensure their swift removal.

The referred content covered five languages and was disseminated by terrorist-supporting networks, including Islamist, right-wing and left-wing terrorist groups. **Participating countries included Denmark, France, Germany and the United Kingdom.**

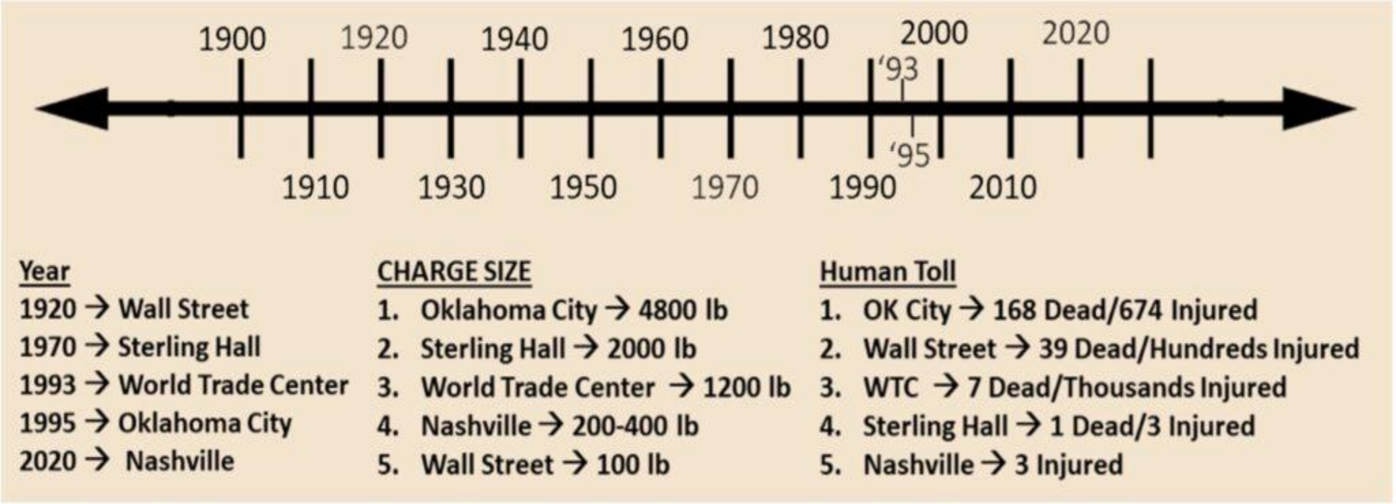
## Explosive Precursor Chemicals

Source: https://nct-cbnw.com/explosive-precursor-chemicals/

Feb 27 – **Dr. Kirk Yeager warns us of possible CBRNe terrorist attacks using explosives.** Ever since the discovery of high explosives, bombers have subverted these materials to lash out against their perceived adversaries. Many explosive charges can be produced with seemingly innocuous materials. The Nashville Christmas Day Bomber used such chemicals to produce a charge of great devastation. This was done despite the best efforts of law enforcement to educate vendors of this lurking danger. Hopefully a lesson can be drawn from this attack which can be used to avoid a tragic repeat.

### History of vehicle bombs

The United States is very fortunate in that it has not experienced a great number of vehicle bombs throughout its history. Prior to Nashville only four vehicle bombs of significant impact occurred.  A summary of these vehicle attacks is provided down below.



| Year | CHARGE SIZE | Human Toll |
|---|---|---|
| 1920 → Wall Street | 1. Oklahoma City → 4800 lb | 1. OK City → 168 Dead/674 Injured |
| 1970 → Sterling Hall | 2. Sterling Hall → 2000 lb | 2. Wall Street → 39 Dead/Hundreds Injured |
| 1993 → World Trade Center | 3. World Trade Center → 1200 lb | 3. WTC → 7 Dead/Thousands Injured |
| 1995 → Oklahoma City | 4. Nashville → 200-400 lb | 4. Sterling Hall → 1 Dead/3 Injured |
| 2020 → Nashville | 5. Wall Street → 100 lb | 5. Nashville → 3 Injured |

Vehicle Bomb Timeline

The first attack over a century ago consisted of dynamite in a horse drawn carriage exploded in the financial district of Wall Street. In 1970 anti-war radicals detonated a ton of ANFO outside University of Wisconsin's Sterling Hall, a building that housed a defense department research center, in protest of the Vietnam War. During the 1990's two terrorist bombings, one international and one domestic, targeted the World Trade Center in New York City and the Murrah Federal building in Oklahoma. Unlike the previous attacks, the bomb in Nashville was not set off as an act of terrorism. Nor was it deployed to create a body count. It is only through the intention of the bomb builder that the explosion did not result in a much more significant loss of life.

**Chemical purchases**

A review of the purchase history of the Nashville bomber was conducted to ascertain which explosive precursor chemicals (EPCs) he procured. Both big-box store purchases from Walmart and Sam's Club as well as purchases from specialty chemical companies over a 10-year span were examined. An overview of significant EPCs obtained, along with rough quantities, is provided in the following table.

| Consumer Chemicals (Pounds and Gallons) | Pyrotechnic Chemicals (Tens of Pounds) | Bulk Chemicals (Hundreds of Pounds) |
|---|---|---|
| **Sulfuric Acid Drain Opener** | Potassium Permanganate | Sodium Nitrate |
| **Camping Stove Tablets** | Hexamine | Potassium Nitrate |
| **Peroxide Pool Cleaner** | Ammonium Perchlorate | |
| **Salicylic Acid** | Magnesium Powder | |
| **Citric Acid** | Zinc Powder | |
| **Urea Cold Packs** | Sulfur | |
| **Urea** | Potassium Chlorate | |
| | Aluminum Powder | |

EPC Purchases over 10 Year Period

Overall, the bomber purchased approximately 1550 pounds of oxidizers and 92 pounds of highly reactive fuels. Most terrorist explosives are based on simple combinations of these two ingredients. Assuming an ideal ratio of fuel and oxidizer, these purchases could have produced an explosive charge ranging between 460-920 pounds.

The exact nature of the explosive charge produced remains unknown. Chemical analysis from the post-blast scene showed residues consistent with Nitrates, Perchlorates and Chlorates. Chemical analysis of residues collected from the bombers residence revealed the presence of Erythritol Tetranitrate (ETN) and Picric Acid (PA).

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

## Pennsylvania man arrested after allegedly trying to bring explosives in his suitcase on a flight

Source: https://edition.cnn.com/2023/03/01/us/explosives-suitcase-flight-arrest/index.html

Mar 02 – Federal agents arrested a Pennsylvania man this week after he allegedly tried to bring explosives in his suitcase on a flight from Lehigh Valley International Airport to Florida.

According to court documents, an alarm alerted that the baggage belonging to Marc Muffley contained explosives. **Transportation Security Administration agents paged Muffley over the airport intercom system and asked him to report to the airport's security desk, prosecutors said, but he did not show up.**

Soon after, security cameras allegedly caught Muffley leaving the airport. He had checked his luggage on Flight 201 bound for Orlando Sanford International Airport, according to court documents.

The FBI contacted the Carbon County chief of detectives who said he knew Muffley personally, according to court documents, and confirmed that Muffley's address matched the one on his driver's license.

“The FBI arrested Marc Muffley, 40, without incident at his Lansford, Pa., residence late Monday night,” an FBI spokesperson said in a statement to CNN.

Muffley remains in custody and will make his first court appearance on Thursday, the FBI spokesperson said.

According to the complaint, an alarm alerted Muffley’s baggage to TSA agents as it was being screened. Agents inspected baggage and found a “circular compound approximately three inches in diameter, wrapped in a wax-like paper and clear plastic wrap hidden in the lining of the baggage, among other items,” court documents stated.

**A safety bomb technician X-rayed the bag, investigators said, and found that it contained a powder concealed in the plastic wrap consistent with “commercial-grade fireworks.” Investigators also said a fuse was attached to the circular compound. “The baggage also contained a can of butane, a lighter, a pipe with white powder residue, a wireless drill with cordless batteries, and two GFCI outlets taped together with black tape,” the complaint stated.**

TSA said in a statement that “out of an abundance of caution, the immediate area of airport was evacuated and the Lehigh-Northampton Airport Authority Police and the Federal Bureau of Investigation were notified.”

Bomb technicians determined the item “was indeed a live explosive device,” according to TSA.

“Transportation Security Officers are highly trained and highly skilled professionals at the front line of aviation security and catches such as this illustrate the point,” TSA said in its statement. The airport was closed for more than two hours after the incident, according to Colin Riccobon, public relations director of the airport. Numerous agencies responded, including two bomb squads, and it demonstrated “tremendous teamwork,” Riccobon said. Checked baggage at the Lehigh Valley airport is handed by passengers to airline personnel at the check in counter. The baggage is then transferred to a TSA agent for screening. TSA agents screen about 800-1,600 passengers a day at the airport, the agency told CNN.

### Suspect’s criminal history had been relatively minor, former PD chief says

Pennsylvania court records show that Muffley had been charged more than a half-dozen times over the last decade for possession of controlled substances, harassment and minor theft, among other crimes. Jack Soberick, the former police chief in Lansford, Pennsylvania, who federal authorities consulted with before arresting Muffley, said he’d come into contact with the suspect numerous times during his 25 years with the department in northeastern Pennsylvania. In a brief interview with CNN, Soberick said he did not recall details but that all of the incidents were minor in nature, such as drug arrests or misdemeanor domestic issues. Soberick had encountered Muffley both as a suspect and a victim, he said. Any violence, he said, would have been limited to a fist fight. “There’s nothing that would light up and say, ‘Hey, this guy’s gonna try to bomb an aircraft,’” Soberick said. “I don’t think he’s radicalized or anything like that.” James Desanto, a lawyer who represented Muffley in several of his cases, said he hadn’t spoken to him in years but that he had also never had any indication that Muffley had radical beliefs or would have brought an explosive on a plane.

Some of Muffley’s arrests made local news. In April 2017, Muffley was arrested after stealing about $22 worth of batteries from a Family Dollar store, the Hazleton Standard-Speaker newspaper reported.

Court records show that Muffley was charged with retail theft. He pleaded guilty in September 2017 and was sentenced to a year of probation. Court documents suggest that Muffley failed to pay required fines related to several of his court cases as recently as December 2022. At several points, prosecutors moved to revoke his probation, although it’s unclear whether it was ultimately revoked.

**EDITOR’S COMMENT:** I am not a police officer, but I think that when you page a suspect at the same time you block airport’s exits and ask for IDs.

# Boston Marathon Bombing (2013) As a Case Study and Possible Insight Regarding Planning and Deploying Security Technologies

**By Or Shalom**

Source: https://i-hls.com/archives/118312

Mar 01 – A decade has gone by since the Boston marathon bombing, and there is much insight that can be learned by analyzing and studying how to characterize and adapt technological abilities and advanced security applications as part of the preparations for terror attack prevention. The embedded abilities in smart city technology, AI and ML can improve performance when working against terror attacks, even in multi-participant events such as marathons, sport Olympics, festivals, etc.

The basic assumptions in this analysis, are based on the possible complexity in detecting and dealing with terror cells or lone suicide bombers. However, an additional assumption is that there are abnormal patterns and deviation from normal and expected behavior vis digital means and OSINT, as well as possible anomalies in detecting on field and in the arena itself. The finding of the many investigations done on this terror attack, carried out by the brothers Tamerlan and Dzhokhar Tsarnaev, showed that the attack was carried out on Boylston street at the finish line, using two bombs that were placed approximately 170 meters apart, killing three people and injuring close to 264 others. This piece of data strengthens the claim that there are irregular pattens of behavior which can be collected and examined via analytics, and in this case set an anomaly in place concerning the connection and divergence of the two elements to two differing directions. Similarly, placing and leaving a bag with no supervision is a deviation from normal behavior, as one of the brothers was seen leaving the event without the bag which he was previously documented carrying. 1

Forensic efforts and evidence collection following the bombing were concluded in four days, as there is quite a few pieces of information and data that could be retrospectively analyzed online. This data, allowed for researchers to led law enforcement to the suspects and their connection to the attack. As long as analytical capabilities are employed to monitor similarly possible suspicious behavioral patterns, the abilities of the security systems to support the decision making of security teams will improve and lead to better foiling of such events. For example, embracing possible characteristics, as insight from this event and additional similar events, to detect irregular patterns as follows:

- Cumbersome leg movements that can be seen in security footage where the weight influences movement
- Opposite flow of movement when compared to the crowd
- Irregular patterns between connected individuals, such as the separation of the Tsarnaev brothers
- Loitering around side streets as a possible indication of suspicious behavior
- Passing of an object between two elements, similarly to the terror attack at Mogadishu Airport in 2016 where a rigged computer was passed between two internal airport workers and led to an explosion of an airplane during flight, etc. 2
- Demarcation for the purpose of detecting movement in sensitive or problematic areas.

The fact that today's technologies are capable of converting information to text improves analysis capabilities and allows for fast extraction of information using textual queries. This way, the information yielded from a photograph is translated to text (image to text) and allows for further examination of the queries. These abilities improve the speed of information analysis yielded from camera as it is gathered into a few minutes as opposed to watching back all available security footage. That way law enforcement can carry out queries based on colors (apparel and hair color), movement trajectory, hours, license plates, ages, and more.

Furthermore, there is significant advantage to deploy analytical information collecting applications in the OSINT space, routinely, prior to a possible terror attack, during and following. These advanced collection abilities allow for the collection of valuable information yielded from the online meta data which can help point out possible suspects. These processed are not only based on the content of a conversation or a particular action but also on connecting different pieces of information regarding time, location, articles and online posts on social media, cross referencing names throughout different databases in connection to terror activity, terror attacks, etc. These abilities depend on being able to cover vast amounts of information and databases throughout the internet (and commonly the dark web), in collaboration with nations, intelligence agencies and law enforcement, quite the complicated task. This method of action allowed for the retrospective collection of posts and tweets indicating levels of radical thinking following the Boston bombing. These, when cross referenced with a visit of one of the brothers (Tamerlan) in Czechia, was a possible indication for radicalism that could have led the brothers to plan the attack, since the aforementioned visit lasted for approximately six months. An additional significant point of indicative information was that previously in 2011, the Russians turned to the FBI with a request to receive information on Tamerlan as there were existing suspicions of his affiliation with radical Islam and his enlistment into underground forces.

Although there are ethical and legislative limitation (in accordance with the different regulations around the world), there are operative capabilities that allow for the use of queries and cross reference between possible suspects and geographical data. This type of activity can provide additional value during preparations by utilizing advanced technological means (many solutions and abilities are offered today in the HLS market). This information can also be used in supportive roles such as random checkpoints while attempting to create additional venues of security to not depend on technological monitoring alone.

Controlling the crowd during an event and afterwards is also critical. In video footage showcasing the aftermath of the Boston terror attack, you can see the ensuing chaos caused by panic. Today, there are many technological developments based on drone cameras, optic detectors and AI that allow for better crowd control, alert levels of crowd density in real time and direct crowd via indoor and outdoor digital signs. 3

Between all the challenges added during the last few years, there is also a rising demand in dealing with drone operators. We have seen drones being used for nefarious means such as intelligence collection, harassment and defiance such as was the case with the Angela Merkel case. Preparations to deal with these threats must be based on tactical and technological solutions accordingly to the characteristics of the field, communication methods, all while considering safety, etc. During the last few years, technological concepts and research have been tested to improve detection abilities regarding drone operators in close proximity. 4

There are still gaps in commercial performances of available UAV manufactures, the need for close proximity for detection and limitations regarding encryption of communication. Research conducted by the Ben Gurion University, Israel, has suggested an interesting method to collect information of the operator by analyzing the aerial course of the UAV (accordingly to the research, with accuracy of 72%). 5

During the last decade, many technological security abilities were enhanced in light of new vast information processing capabilities, combining AI and ML capabilities allows for better adaption to different situations and analytical abilities. Therefore, examining requirements, environments and threats can provide a better security solution for spot events, infrastructure and critical sites, airports and more.

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

## EOD robots are potential confined space lifesavers

**By Donovan Potter** (75th Air Base Wing Public Affairs)
Source: https://www.eglin.af.mil/News/Article-Display/Article/3316992/eod-robots-are-potential-confined-space-lifesavers/

Feb 28 – Generally, Liquid Fuels Maintenance and Explosive Ordnance Disposal technicians don't perform duties simultaneously for safety's sake, but that's what happened Feb. 8 near building 825 on Hill AFB.

To avoid sending a human into a potentially dangerous confined space to perform a structural integrity inspection, EOD deployed robots equipped with video cameras to do the job while civil engineers looked at monitors outside in the fresh air.

"We needed to inspect two fuel storage tanks that hadn't been used for years so we could put them back into service," said Christopher Hayes, 75th Civil Engineer Squadron, Utilities Systems operator. "Using the robots kept us from having to suit up and enter the confined space to check the welds and the condition of the metal."

To send a person in the tank, a confined space program team would have been assembled to be onsite, which includes 75th Air Base Wing Safety, Fire Department and Bioenvironmental Engineering representatives.

"CE would have put together a minimum of a three-person team where one person would enter the tank, one person would monitor an atmospheric meter and observe for emergencies, and the third person would supervise the entry," said Shane Poulsen, 75th Air Base Wing Occupational Health and Safety manager.

"Putting a person in the space potentially exposes them to atmospheric hazards which can quickly cause harm or even death to the entrant and potential rescuers."

Staff Sgt. Daniel Green, 775th Explosive Ordnance Disposal technician said he was excited to partner with other base organizations to accomplish this operation more safely.

"Our job is to help people," he said. "We solve unique problems for various customers and this was another great opportunity for myself and my Airmen to not only help out another base agency but also test our robot driving skills."

EOD used two robots to accomplish the mission. The medium-sized MTTRS 2 and man transportable, dismount MTGR, normally used to detect, confirm and identify hazards such as landmines, unexploded ordnance and improvised explosive devices in the path of maneuvering forces.

"The robots are extremely versatile, as we found in this situation," Green said. "They inspected the structural integrity of the two 90,000-gallon fuel tanks and with the abilities of our operators, they confirmed that the tanks are structurally sound and can continue their service life without putting anyone at risk by sending them into a confined space with a fuel-vapor hazard."

The recertified fuel tanks will be used to store approximately 140,000 gallons of fuel oil worth more than $500,000 that will be transferred from five underground tanks supplying fuel to the base boiler plant in building 260. The underground tanks are being replaced. Green said the mission was a success for everyone.

"It was a homerun," he said. "We executed safely and efficiently and satisfied the requirements to keep the fuel tanks operational, all with minimized risk. My Airmen, with their driving abilities, made the whole thing possible and were true professionals from start to finish."

## March 11, 2004 - Terrorists bomb trains in Madrid

Source: https://www.history.com/this-day-in-history/terrorists-bomb-trains-in-madrid

On March 11, 2004, 193 people are killed and nearly 2,000 are injured when 10 bombs explode on four trains in three Madrid-area train stations during a busy morning rush hour. The bombs were later found to have been detonated by mobile phones. The attacks, the deadliest against civilians on European soil since the 1988 Lockerbie airplane bombing, were initially suspected to be the work of the Basque separatist militant group ETA. This was soon proved incorrect as evidence mounted against an extreme Islamist militant group loosely tied to, but thought to be working in the name of, al-Qaida.

Investigators believe that all of the blasts were caused by improvised explosive devices that were packed in backpacks and brought aboard the trains. The terrorists seem to have targeted Madrid's Atocha Station, at or near which seven of the bombs were detonated. The other bombs were detonated aboard trains near the El Poso del Tio Raimundo and Santa Eugenia stations, most likely because of delays in the trains' journeys on their way to Atocha. Three other bombs did not detonate as planned and were later found intact.

Many in Spain and around the world saw the attacks as retaliation for Spain's participation in the war in Iraq, where about 1,400 Spanish soldiers were stationed at the time. The attacks took place two days before a major Spanish election, in which anti-war Socialists swept to power. The new government, led by Prime Minister Jose Luis Rodriguez Zapatero, removed Spanish troops from Iraq, with the last leaving the country in May 2004.

A second bombing, of a track of the high-speed AVE train, was attempted on April 2, but was unsuccessful. The next day, Spanish police linked the occupants of an apartment in Leganes, south of Madrid, to the attacks. In the ensuing raid, seven suspects killed themselves and one Spanish special forces agent by setting off bombs in the apartment to avoid capture by the authorities. One other bomber is believed to have been killed in the train bombings and 29 were arrested. After a five-month-long trial in 2007, 21 people were convicted, although five of them, including Rabei Osman, the alleged ringleader, were later acquitted.

In memory of the victims of the March 11 bombings, a memorial forest of olive and cypress trees was planted at the El Retiro park in Madrid, near the Atocha railway station.

## "Switchable" High Explosives Mitigate Risk of Accidental Detonation

Source: https://www.homelandsecuritynewswire.com/dr20230320-switchable-high-explosives-mitigate-risk-of-accidental-detonation

Mar 20 – In an effort to mitigate accidental detonations of stored explosives, a multidisciplinary team of Los Alamos National Laboratory scientists developed a way to create "switchable" high explosives that won't detonate unless activated by being filled with an inert fluid, such as water. Their findings were published in *Physical Review Letters*.

"A system that is completely insensitive to unplanned stimuli but switches to high performance during use is the holy grail of high explosives," said Los Alamos scientist Alexander Mueller, principal investigator for the project. "We've designed a high explosive system that won't work when it's not supposed to, like during transport and storage, but can quickly be made ready when required."

For military planners, personnel who might work with explosives and communities near operations such as mining and munitions, the volatility of certain high explosives presents a potential hazard. Impact, heat and friction are all sensitivities that can produce an unplanned explosion with high explosive materials.

For example, the accidental detonation of stored ammonium nitrate in Beirut, Lebanon, in 2020 killed more than 200 people, including workers and nearby residents. Equivalent to an earthquake, the explosion leveled the port district and was felt across the country and the region. While unusually large, the event was not unprecedented; one estimate showed that 500 unplanned explosions occurred at munitions plants from 1979 to 2013.

The Los Alamos team used additive manufacturing techniques to fabricate high-explosive charges with a lattice structure that by themselves cannot sustain detonation. In experimentation that marked the first time quantifying the effectiveness of the high-explosive charges, the team found that an unfilled charge's Gurney energy — the propulsion resulting from an explosive's gaseous products expanding — was 98 percent lower than that of an equivalent water-filled charge.

That means that the unfilled high-explosive charges can be safely transported, handled and stored without risk of detonation.

Their experimentation also had the team tuning the detonative performance of the system by changing the mechanical properties of the fluids in fluid-filled charges. The team found that replacing water with higher density fluids increased propulsion by up to 8.5 percent and decreased detonation velocity by 13.4 percent. The results point to the technology's possible tenability for a variety of industrial purposes.

"The data suggest a tuneability allowing to optimize the energy delivery for different applications," said Cameron Brown, scientist at Los Alamos and lead author on the paper. "Insight into the Gurney energy and detonation velocity of filled and unfilled charges presents a path forward for quantifying the detonative performance of switchable explosives with different structural parameters, and optimizing them for mining, oil and gas exploration, blasting or military applications."

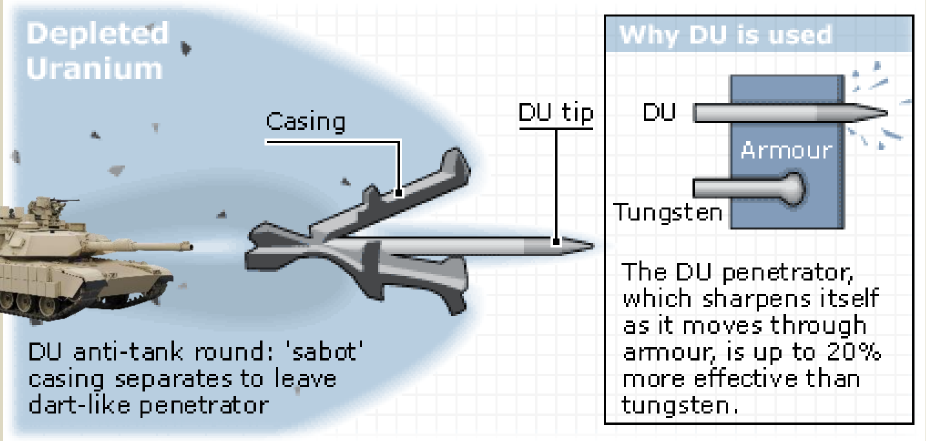
Further experimentation and data will help evaluate performance with different charge structures and fill fluids. The improved technology, though, offers a path for improving industrial safety and even for making safe things like unexploded ordinance, which in many places can be a hazard for civilians during or after conflicts. The development of switchable high explosives technology, it is hoped, may make disasters and accidents a thing of the past.

## Putin warns UK over depleted uranium tank shells for Ukraine

Source: https://www.aljazeera.com/news/2023/3/22/putin-warns-uk-over-depleted-uranium-tank-shells-for-ukraine

Mar 22 – Russian President Vladimir Putin has warned that Moscow would be "forced to react" if the United Kingdom provides Ukraine with armour-piercing tank ammunition that contains depleted uranium.

Putin was reacting on Tuesday to news the UK's minister of state for defence, Annabel Goldie, had confirmed that ammunition containing depleted uranium was part of a military aid package being sent to Ukraine along with Challenger 2 battle tanks.


Depleted Uranium
Casing
DU tip
DU anti-tank round: 'sabot' casing separates to leave dart-like penetrator
Why DU is used
DU
Armour
Tungsten
The DU penetrator, which sharpens itself as it moves through armour, is up to 20% more effective than tungsten.

"The United Kingdom… announced not only the supply of tanks to Ukraine but also shells with depleted uranium. If this happens, Russia will be forced to react," Putin told reporters after talks with China's leader Xi Jinping at the Kremlin.

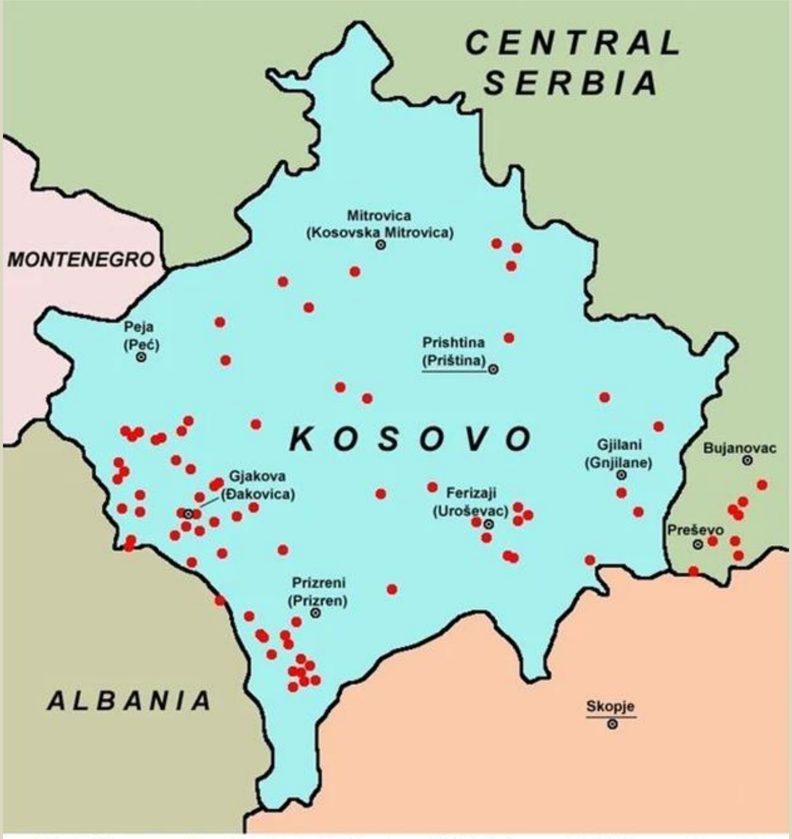
"If all this happens, Russia will have to respond accordingly, given that the West collectively is already beginning to use weapons with a nuclear component," Putin said, without elaborating.

In response to questions about the ammunition, Goldie said on Monday that "alongside our granting of a squadron of Challenger 2 main battle tanks to Ukraine, we will be providing ammunition including armour-piercing rounds which contain depleted uranium".

The ammunition was "highly effective in defeating modern tanks and armoured vehicles", she said.

Depleted uranium is a by-product of the nuclear enriching process used to make nuclear fuel or nuclear weapons. Its heaviness lends itself for use in armour-piercing rounds as it helps them easily penetrate steel.

The United Nations Environment Programme has described such ammunition as "chemically and radiologically toxic heavy metal".



● - Sites in Kosovo and southern Central Serbia where NATO aviation used forbidden munition with depleted uranium during 1999 bombing

The UK's Ministry of Defence dismissed Putin's warning on Tuesday, saying the armour-piercing shells had been standard equipment for decades and were "nothing to do with nuclear weapons or capabilities".

The ministry accused Russia of deliberate disinformation for describing the ammunition as "weapons with a nuclear component".

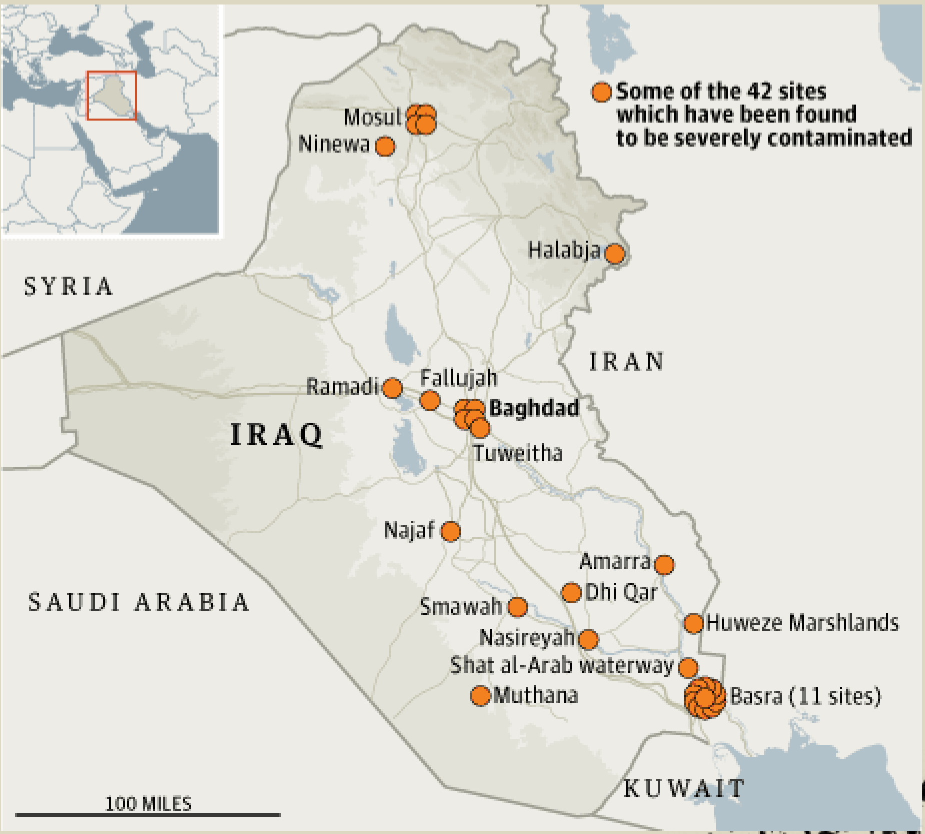
The Institute for the Study of War, a US-based think tank, said on Wednesday that Putin had portrayed the ammunition as "escalatory in order to deter Western security assistance despite the shells not containing any fissile or radiological material".

Russia's Defence Minister Sergei Shoigu said the UK's decision left fewer steps before a potential "nuclear collision" between Russia and the West.

"Another step has been taken, and there are fewer and fewer left," he told reporters in remarks cited by Russian news agencies.

Russian politicians and commentators have made a series of combative remarks since the invasion of Ukraine last year, suggesting Moscow would – if necessary – be prepared to deploy its vast nuclear arsenal.

The Campaign for Nuclear Disarmament (CND), an anti-nuclear organisation, condemned the UK decision to send the ammunition, calling it an "additional environmental and health disaster for those living through the conflict" as toxic or radioactive dust can be released on impact.

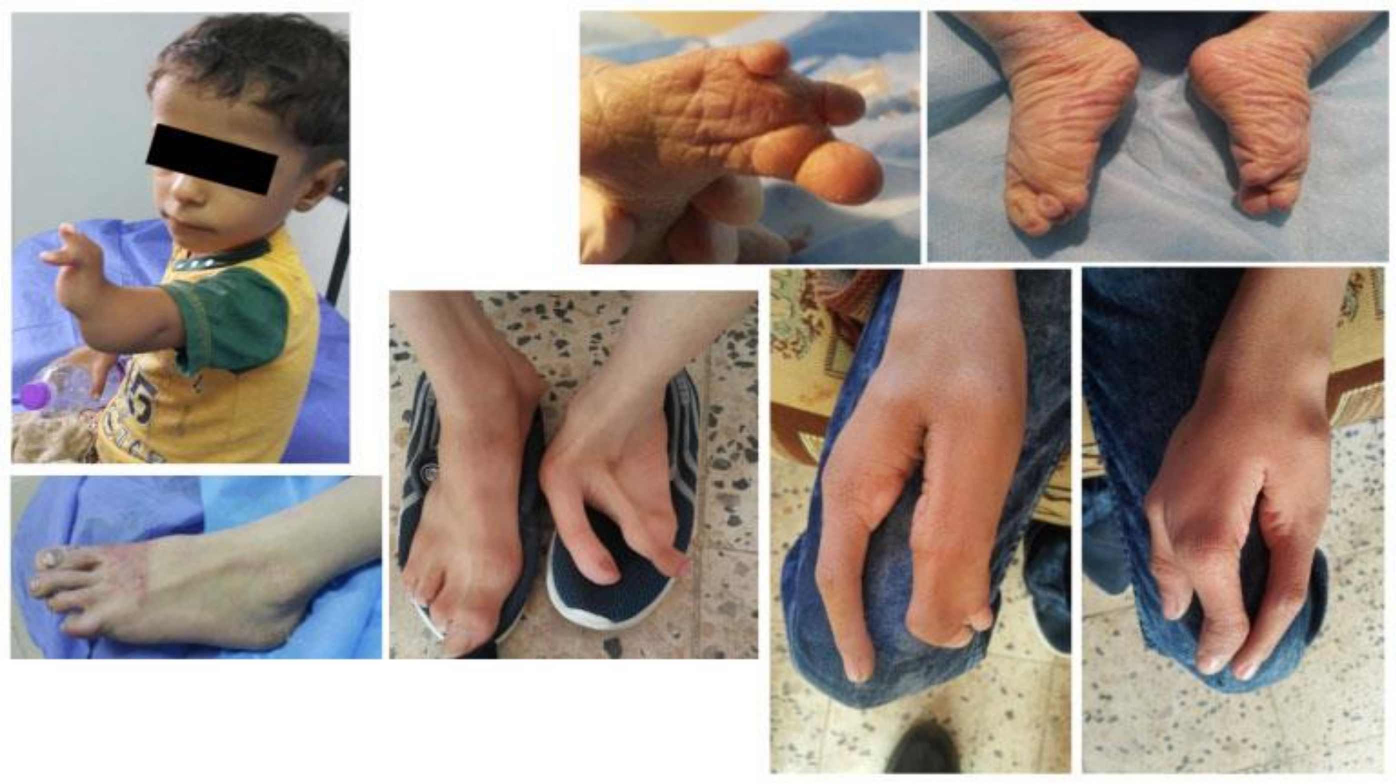


"CND has repeatedly called for the UK government to place an immediate moratorium on the use of depleted uranium weapons and to fund long-term studies into their health and environmental impacts," CND's general secretary, Kate Hudson, said, according to Agence France-Presse.

Earlier, Russia's Foreign Ministry spokesperson Maria Zakharova called the plan the "Yugoslavia scenario", saying the ammunition caused cancer and infected the environment. Russian Foreign Minister Sergey Lavrov said the plan showed that the UK "have lost the bearings".

Hamish de Bretton-Gordon, former commander of the UK's Royal Tank Regiment, said it was "reckless" of Putin "to try and suggest Britain is sending nuclear material" to Ukraine.

He said depleted uranium is a common component of tank rounds, possibly even used by Russia. "Putin insinuating that they are some sort of nuclear weapon is bonkers," de Bretton-



Gordon told The Associated Press. “Depleted uranium is completely inert. There is no way that you could create a nuclear reaction or a nuclear explosion with depleted uranium.”

In a joint statement issued at the end of their meeting in Moscow on Tuesday, Putin and Xi cautioned against any steps that might push the Ukraine conflict into an “uncontrollable phase”, adding pointedly that there could be no winners in a nuclear war.

**EDITOR’S COMMENT:** Brits do not care! Do not learn from past! Next generations will face the consequences of the proxy war. UN wake up!

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

# CYBER NEWS

C²BRNE DIARY

# The Sharks Are Circling - Russia and China Take Aim At The World's Undersea Cable Network

**By Sam Faddis**

Source: https://andmagazine.substack.com/p/the-sharks-are-circling-russia-and

Feb 23 – We live in a world created in 1945. The United States is the world's dominant political, economic, and military power. We treat those facts as if they are somehow immutable. They are not. We are standing on the brink of losing it all.

The Biden administration continues to blunder forward with its reckless policy of escalation in Ukraine treating the entire enterprise as if it were a video game of some sort. There are in the minds of these men and women no consequences for their actions. Only the other side takes losses. Only the other side feels pain.

AND Magazine is a reader-supported publication. To receive new posts and support my work, consider becoming a free or paid subscriber.

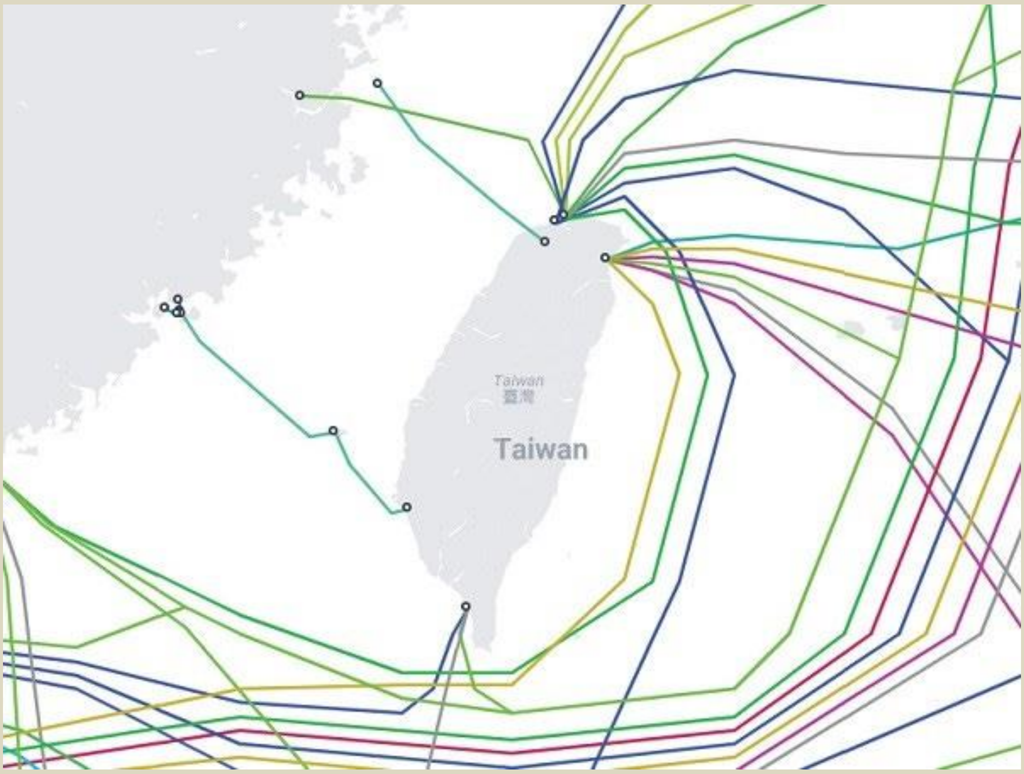
That's not how war works. That's not how the world works.

Out there in the shadows, as tensions escalate and the world moves closer to a world war, the sharks are circling. Our enemies are already well down the road to responding to our actions and making us pay a price for our arrogance.

The world's economy runs on internet communications. Those communications move primarily on a vast network of undersea cables. Without those cables, you do not run your business. You do not access your checking account. You do not do anything in the real world.

Without those cables, the world's economy shuts down, and you fend for yourself.

For some time our allies in Europe have been tracking Russian vessels believed to be mapping undersea cables in the North Sea and surrounding bodies of water. The concern is that the Russians are preparing to stage attacks on these cables in retaliation for European and American support for Ukraine. Dutch military intelligence is now warning that Russian attacks could be expanded to include energy infrastructure in the region.



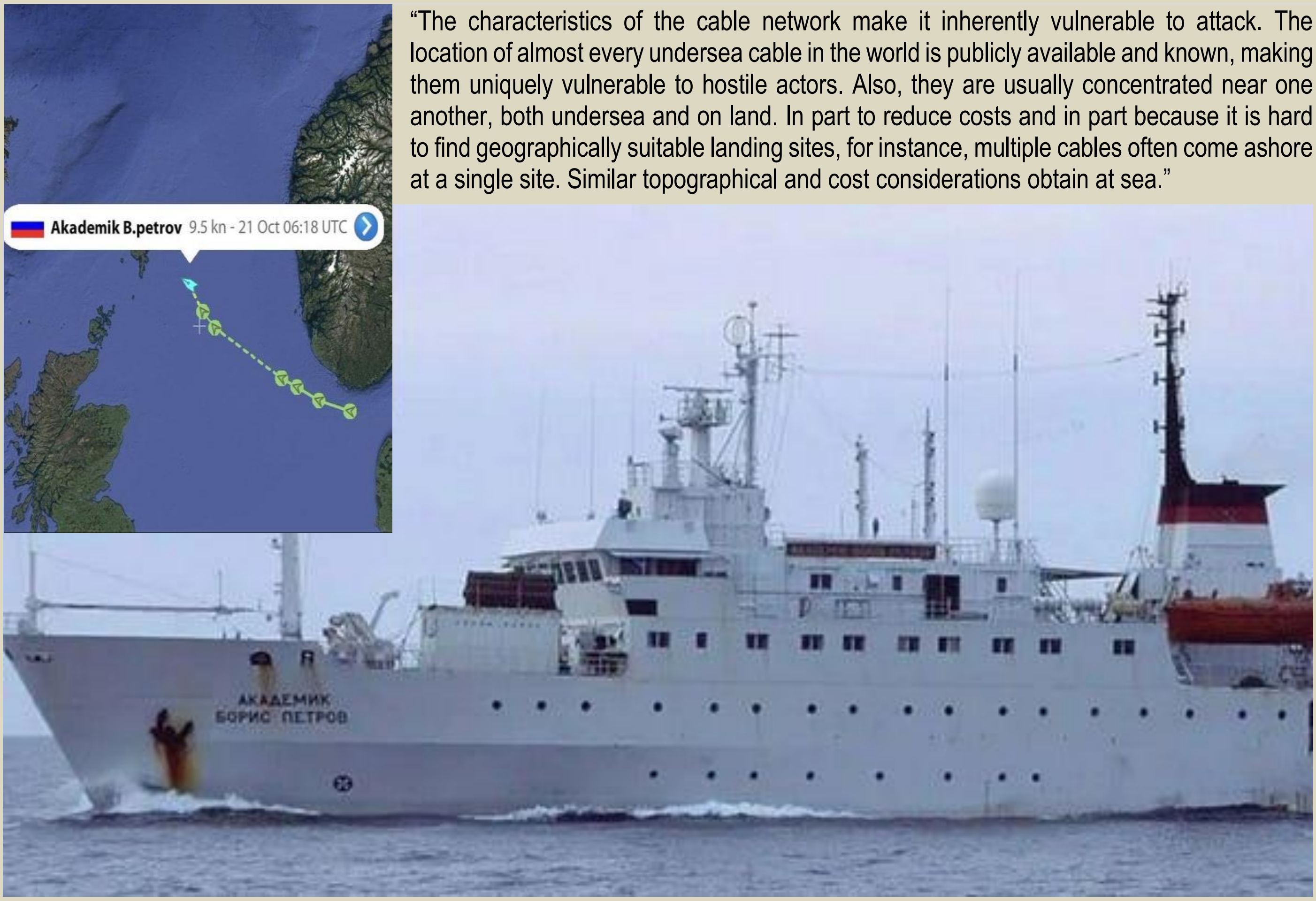
There have already been multiple instances of breaks in undersea cables in which the Russians are suspected. There was also recently a suspicious case of what looks very much like Russian casing in preparation for a sabotage attack on a Polish oil terminal.

On the other side of the world, Moscow's new Chinese allies are showing the same kind of interest in the undersea cables that run to Taiwan. Two of those cables were recently cut by Chinese vessels. The Chinese appear to be billing the actions as "accidents". There is a strong suspicion that the actions were a dry run for a much broader attack on communication with Taiwan.

On February 2, 2023, a Chinese fishing vessel sailing close to the Matsu Islands severed one of the two cables, which connect the islands with Taiwan proper. Six days later, a Chinese freighter cut the second cable. The Matsu Islands, which belong to Taiwan, are now left with rudimentary communications. The Matsu Islands, which lie close to the coast of mainland China, have been a flashpoint for decades. In 1958 China shelled the islands. Last year the People's Liberation Army Navy conducted large exercises near the islands.

A recently released research paper on undersea cables had this to say about their vulnerability.

"The characteristics of the cable network make it inherently vulnerable to attack. The location of almost every undersea cable in the world is publicly available and known, making them uniquely vulnerable to hostile actors. Also, they are usually concentrated near one another, both undersea and on land. In part to reduce costs and in part because it is hard to find geographically suitable landing sites, for instance, multiple cables often come ashore at a single site. Similar topographical and cost considerations obtain at sea."



The mystery over severed undersea power cables off Shetland has deepened after it emerged a Russian "research ship" was clocked in the area.

Retired Navy Admiral James G. Stavridis, former Supreme Allied Commander NATO had this to say on the topic.

"It is a little-known or appreciated fact that well over 95% of everything that moves on the global internet passes through a network of just 200 undersea fibreoptic cables; some as far below the surface as Everest is above it. It is not satellites in the sky, but pipes on the ocean floor that form the backbone of the world's economy…we have allowed this vital infrastructure of undersea cables to grow increasingly vulnerable. This should worry us all. Cables are isolated in the midst of the oceans, their locations are known, and they are often subject to only minimal security at on-shore landing sites. Furthermore, the technical capabilities required to damage cables are relatively low and unsophisticated. The risk posed to these garden hose-thin connections that carry everything from military intelligence to global financial data is real and growing. In the most severe scenario of an all-out attack upon undersea cable infrastructure by a hostile actor the impact of connectivity loss is potentially catastrophic, but even relatively limited sabotage has the potential to cause significant economic disruption and damage military communications…Recent reports make clear that Russian submarine forces have undertaken detailed monitoring and targeting activities in the vicinity of North Atlantic deep-sea cable infrastructure. And as another example of Russian interest in asymmetric targets, it is worth remembering that in Crimea, Russia successfully took control of land based communications infrastructure early in its annexation of the peninsula. Russia's relative weakness also attracts it to conducting hybrid warfare. The fundamental idea of hybrid warfare is hostile activity that stops short of full, overt, offensive action and is sufficiently ambiguous that it allows the aggressor plausible deniability and makes international response more difficult. Hybrid warfare has traditionally been land-based, but as I have argued previously, this is about to change and we should prepare for increased maritime hybrid activity. Chinese activities in the South China Sea and Iranian actions in the Arabian Gulf already show characteristics of a hybrid approach, using civilian vessels rather than easily identifiable 'gray hull' naval platforms to obfuscate the involvement of state actors. Underwater cables are an obvious target for such hostile action: they are a vital infrastructure asset with ambiguous protection in international law that can be damaged with relatively unsophisticated, non-military hardware."

Before Japanese forces staged their air attack on Pearl Harbor in 1941 a U.S. destroyer escort, the U.S.S. Ward reported sighting a Japanese mini-sub entering the harbor and staged a depth charge attack on the target. The command at Pearl Harbor ignored the report. No alert was sounded. The fleet was caught unprepared and decimated.

We stand in a similar position today. Our enemies smell blood in the water. They are preparing for action. Time to sound the alarm before it is too late.

**Sam Faddis** is a retired CIA Operations Officer. Served in Near East and South Asia. Author, commentator. Senior Editor AND Magazine. Public Speaker. Host of Ground Truth.

## Can a Cyber shuffle Stop Hackers from Taking Over a Military Aircraft?

Source: https://www.homelandsecuritynewswire.com/can-cyber-shuffle-stop-hackers-taking-over-military-aircraft

Feb 27 – A cybersecurity technique that shuffles network addresses like a blackjack dealer shuffles playing cards could effectively befuddle hackers gambling for control of a military jet, commercial airliner or spacecraft, according to new research. However, the research also shows these defenses must be designed to counter increasingly sophisticated algorithms used to break them.

Many aircraft, spacecraft and weapons systems have an onboard computer network known as military standard 1553, commonly referred to as MIL-STD-1553, or even just 1553. The network is a tried-and-true protocol for letting systems like radar, flight controls and the heads-up display talk to each other.

Securing these networks against a cyberattack is a national security imperative, said Chris Jenkins, a Sandia National Laboratories cybersecurity scientist. If a hacker were to take over 1553 midflight, he said, the pilot could lose control of critical aircraft systems, and the impact could be devastating.

Jenkins is not alone in his concerns. Many researchers across the country are designing defenses for systems that utilize the MIL-STD-1553 protocol for command and control. Recently, Jenkins and his team at Sandia partnered with researchers at Purdue University in West Lafayette, Indiana, to test an idea that could secure these critical networks.

Their results, recently published in the scientific journal IEEE Transactions on Dependable and Secure Computing, show that done the right way, a technique already known in cybersecurity circles, called moving target defense, can effectively protect MIL-STD-1553 networks against a machine-learning algorithm. Sandia's Laboratory Directed Research and Development program funded the research.

"When we talk about protecting our computer systems, frequently there are two main pieces we rely on," said Eric Vugrin, a Sandia cybersecurity senior scientist who also worked on the project. "The first approach is just keeping the bad guy out and never permitting access to the system. The physical analogue is to build a big wall and don't let him in in the first place. And the backup plan is, if the wall doesn't work, we rely on detection. Both of those approaches are imperfect. And so, what moving target defense offers as a complementary strategy is, even if those two approaches fail, moving target confuses the attacker and makes it more difficult to do damage."

### Moving Target Defense Must Keep Cyberattackers Guessing

Like a game of three-card monte, in which a con artist uses sleight of hand to shuffle cards side-to-side, moving target defense requires randomness. Without it, the defense unravels. Researchers wanted to know whether a moving target defense would work to constantly change network addresses, unique numbers assigned to each device on a network. They weren't sure it would work because, compared to other types of networks, MIL-STD-1553's address space is small and therefore difficult to randomize.

For example, the strategy has proven useful with internet protocols, which have millions or billions of network addresses at their disposal, but 1553 only has 31. In other words, Sandia had to come up with a way to surreptitiously shuffle 31 numbers in a way that couldn't easily be decoded.

"Someone looked me in the face and said it's not possible because it was just 31 addresses," Jenkins said. "And because the number is so small compared to millions or billions or trillions, people just felt like it wasn't enough randomness."

The challenge with randomizing a small set of numbers is that "Nothing in computer software is truly random. It's always pseudorandom," said Sandia computer scientist Indu Manickam. Everything must be programmed, she said, so there's always a hidden pattern that can be discovered.

With enough time and data, she said, "A human with an Excel sheet should be able to get it."

Manickam is an expert in machine learning, or computer algorithms that identify and predict patterns. These algorithms, though beneficial to cybersecurity and many other fields of research and engineering, pose a threat to moving target defenses because they can potentially spot the pattern to a randomization routine much faster than a human.

"We're using machine-learning techniques to better defend our systems," Vugrin said. "We also know the bad guys are using machine learning to attack the systems. And so, one of the things that Chris identified early on was that we do not want to set up a moving target defense where somebody might use a machine-learning attack to break it and render the defense worthless."

Sophisticated algorithms don't necessarily spell the end for this type of cyberdefense. Cybersecurity designers can simply write a program that changes the randomization pattern before a machine can catch on.

But the Sandia team needed to know how fast machine learning could break their defense. So, they partnered with Bharat Bhargava, a professor of computer science at Purdue University, to test it. Bhargava and his team had been involved previously in researching aspects of moving target defenses.

For the last seven years, Bhargava said, the research fields of cybersecurity and machine learning have been colliding. And that's been reshaping concepts in cybersecurity.

"What we want to do is learn how to defend against an attacker who is also learning," Bhargava said.

### Test Results Inform Future Improvements to Cybersecurity

Jenkins and the Sandia team set up two devices to communicate back and forth on a 1553 network. Occasionally, one device would slip in a coded message that would change both devices' network addresses. Jenkins sent Bhargava's research team logs of these communications using different randomization routines. Using this data, the Purdue team trained a type of machine-learning algorithm called long short-term memory to predict the next set of addresses.

The first randomization routine was not very effective.

"We were not only able to just detect the next set of addresses that is going to appear, but the next three addresses," said Ganapathy Mani, a former member of the Purdue team who contributed to the research.

The algorithm had scored 0.9 out of a perfect 1.0 on what's called a Matthews correlation coefficient, which rates how well a machine-learning algorithm performs.

But the second set of logs, which used a more dynamic routine, resulted in a radically different story. The algorithm only scored 0.2.

"0.2 is pretty close to random, so it didn't really learn anything," Manickam said.

The test showed that moving target defense can fundamentally work, but more importantly it gave both teams insights into how cybersecurity engineers should design these defenses to withstand a machine-learning-based assault, a concept the researchers call threat-informed codesign.

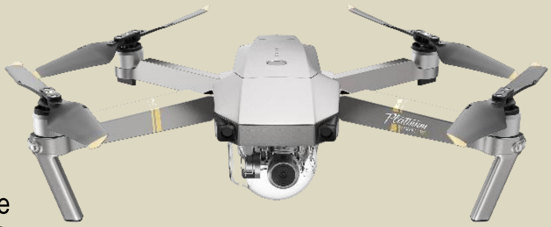
Defenders, for example, could "Add fake data into it so that the attackers cannot learn from it," Mani said.

The findings could help improve the security of other small, cyber-physical networks beyond MIL-STD-1553, such as those used in critical infrastructure.

Jenkins said, "Being able to do this work for me, personally, was somewhat satisfying because it showed that given the right type of technology and innovation, you can take a constrained problem and still apply moving target defense to it."

## This Hacker Tool Can Pinpoint a DJI Drone Operator's Exact Location

Source: https://www.wired.com/story/dji-droneid-operator-location-hacker-tool/

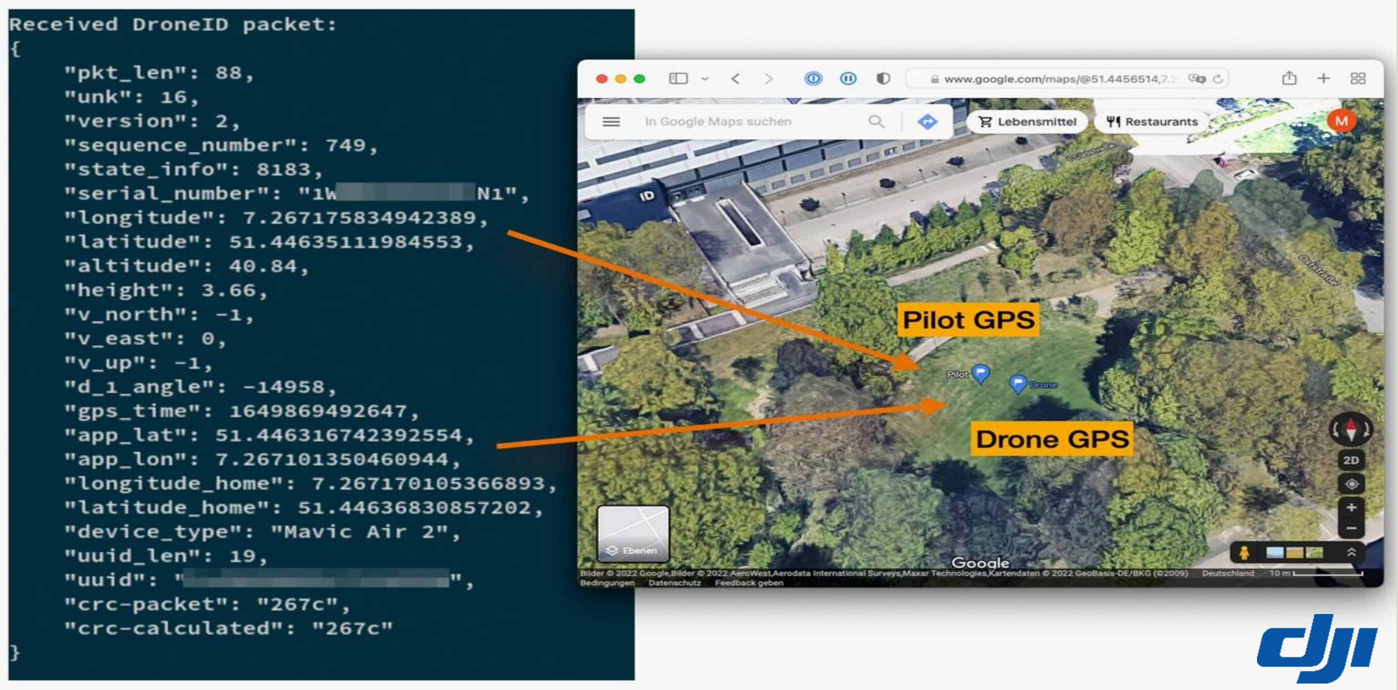


Mar 02 – There's a reason consumer drones have evolved from an expensive toy into a tool of war: They can perform high-altitude surveillance, carry out reconnaissance, or even deploy weapons, with their operator safely hidden as far as miles away. But hackers are revealing that for quadcopters sold by the world's biggest drone manufacturer, operators aren't nearly as hidden as they might think. In fact, these small flying machines are continually broadcasting their pilots' exact locations from the sky, and anyone with some cheap radio hardware and a newly released software tool can eavesdrop on those broadcasts and decode them to extract their coordinates.

At the Network and Distributed System Security Symposium (NDSS) in San Diego this week, researchers from Ruhr University Bochum and the CISPA Helmholtz Center for Information Security demonstrated that they were able to reverse engineer the radio signals of drones sold by DJI, the leading manufacturer of consumer quadcopter drones, to decode a radio protocol they use called DroneID. By deconstructing this signal, the researchers could see that every DJI drone's DroneID communications transmit not only its own GPS location and a unique identifier for that drone, but also the GPS coordinates of its operator.

Courtesy of Ruhr University Bochum and CISPA Helmholtz Center for Information Security

That DroneID system was designed to allow governments, regulators, and law enforcement to monitor drones and prevent their abuse. But hackers and security researchers have warned for the past year that DroneID is unencrypted and open to anyone who can receive its radio signals. The German researchers, as well as another researcher working separately at the University of Tulsa, have now shown just how completely that signal can be decoded and read, allowing any hacker who can eavesdrop on DroneID to pinpoint a drone's hidden operator, even if that drone pilot is miles away.



```
Received DroneID packet:
{
    "pkt_len": 88,
    "unk": 16,
    "version": 2,
    "sequence_number": 749,
    "state_info": 8183,
    "serial_number": "1W[redacted]N1",
    "longitude": 7.267175834942389,
    "latitude": 51.44635111984553,
    "altitude": 40.84,
    "height": 3.66,
    "v_north": -1,
    "v_east": 0,
    "v_up": -1,
    "d_1_angle": -14958,
    "gps_time": 1649869492647,
    "app_lat": 51.446316742392554,
    "app_lon": 7.267101350460944,
    "longitude_home": 7.267170105366893,
    "latitude_home": 51.44636830857202,
    "device_type": "Mavic Air 2",
    "uuid_len": 19,
    "uuid": "[redacted]",
    "crc-packet": "267c",
    "crc-calculated": "267c"
}
```

A screenshot of the German researchers' tool shows how it decodes the radio broadcasts of a DJI drone to extract both the drone and operator locations.

To publicly prove their findings, the German group has released a prototype tool to receive and decode DroneID data here.

The researchers' discovery—and their public tool—provide new evidence of the serious privacy and operational security concerns DroneID presents for operators, especially considering that DJI drones are now often used in war zones, where revealing a drone operator's location can draw enemy fire. And while DJI has an enormous majority share of the consumer drone market, the problem will only grow when new US Federal Aviation Administration regulations go into effect in September, mandating that all consumer drones implement systems similar to DroneID.

"This is a big problem, right?" says Moritz Schloegel, one of the Ruhr University graduate researchers presenting the DroneID findings at NDSS. "You might think your drone transmits its position. But suddenly, it's transmitting *your* position as well. Whether you're privacy-minded or you're in a conflict zone, nasty stuff can happen."

DJI's DroneID became the subject of controversy last spring when the Ukrainian government criticized the company because Russian military forces were using DJI drones for their missile targeting and using the radio signals broadcast from Ukraine's own DJI drones to locate Ukrainian military personnel. China-based DJI has long sold a suitcase-sized device called Aeroscope to government regulators and law enforcement agencies that allows them to receive and decode DroneID data, determining the location of any drone and its operator from as far as 30 miles away.

DJI's DroneID and Aeroscope devices are advertised for civilian security uses, like preventing disruptions of airport runways, protecting public events, and detecting efforts to smuggle cargo into prisons. But Ukraine's vice minister of defense wrote in a letter to DJI that Russia had repurposed Aeroscope devices from Syria to track Ukrainian drones and their operators, with potentially deadly consequences.

DJI responded by warning against any military use of its consumer drones and later cutting off all sales of its drones to both Ukraine and Russia. It also initially claimed in response to the Verge's reporting on the controversy that DroneID was encrypted, and thus inaccessible to anyone who didn't have its carefully controlled Aeroscope devices. But DJI later admitted to the Verge that the transmissions were *not* in fact encrypted, after security researcher Kevin Finisterre showed that he could intercept some DroneID data with a commercially available Ettus software-defined radio. The German researchers—who also helped debunk DJI's initial encryption claim—have gone further. By analyzing the firmware of a DJI drone and its radio communications, they've reverse engineered

DroneID and built a tool that can receive DroneID transmissions with an Ettus software-defined radio or even the much cheaper HackRF radio, which sells for just a few hundred dollars compared to over $1,000 for most Ettus devices. With that inexpensive setup and their software, it's possible to fully decode the signal to find the drone operator's location, just as DJI's Aeroscope does. While the German researchers only tested their radio eavesdropping on a DJI drone from ranges of 15 to 25 feet, they say they didn't attempt to optimize for distance, and they believe they could extend that range with more engineering. Another hacker, University of Tulsa graduate researcher Conner Bender, quietly released a pre-publication paper last summer with similar findings that will be presented at the CyCon cybersecurity conference in Estonia in late May. Bender found that his HackRF-based system with a custom antenna could pick up DroneID data from hundreds or thousands of feet away, sometimes as far as three-quarters of a mile. WIRED reached out to DJI for comment in multiple emails, but the company hasn't responded. The former DJI executive who first conceived of DroneID, however, offered his own surprising answer in response to WIRED's query: DroneID is working exactly as it's supposed to. Brendan Schulman, DJI's former VP of policy and legal affairs, says he led the company's development of DroneID in 2017 as a direct response to US government demands for a drone-monitoring system, and that it was never intended to be encrypted. The FAA, federal security agencies, and Congress were strongly pushing at the time for a system that would allow anyone to identify a drone—and its operator's location—as a public safety mechanism, not with hacker tools or DJI's proprietary ones, but with mobile phones and tablets that would allow for easy citizen monitoring.

"As we were told in 2017 during a summer-long FAA advisory committee process, the location of the operator is an essential aspect of remote identification for US government security purposes," Schulman says. "And the US government *wanted* members of the public to have access to that information, just like how a car's license plate is accessible to everyone who can see it, so they can file a report with authorities if they have concerns about how a drone is being used."

Schulman notes that he advocated for that broadcasting system over what he saw as a far more invasive suggestion from the government, that drone makers should both broadcast operators' locations *and* connect all drones to a network of drone-monitoring services that would record every operator's detailed flight records in government-accessible databases. He also notes that the DroneID issue isn't unique to DJI: He expects that all consumer drones will have a function similar to DroneID when the new FAA regulations take effect later this year.

But none of that changes the fact that DJI drone operators don't expect to have their locations revealed by their drone's radio broadcasts, says University of Tulsa's Bender. "The average drone user definitely doesn't know that their location is being broadcasted in a way anyone with a cheap receiver can view in real time," Bender says. He adds that DJI's handling of the issue—claiming last year that the broadcast was encrypted when it wasn't—further confused users. "I don't know if they intentionally marketed Aeroscope this way, but they made it seem like you could really only intercept DroneID with this one device. And that wasn't the case." Regardless of DJI's motives in including drone pilots' location in the data their drones continually transmit, the fact that this location data can be intercepted—not just with DJI's Aeroscope devices but by any knowledgeable hacker—will have a significant impact on how the world's most common quadcopter drones are used in war zones and other adversarial settings, says August Cole, a futurist and fellow at the Scowcroft Center for Strategy and Security at the Atlantic Council.

"The ability to ID an operator of a drone is sort of the holy grail right now in terms of targeting," Cole says. "And to be able to do this so easily, when a drone maker adds that through either intentional or unintentional engineering, it's a pretty profound revelation for this new kind of warfare."

## A Personal AI Assistant? Internet Inventor Says Yes

Source: https://i-hls.com/archives/118364

Mar 06 – When the inventor of the World Wide Web has something to say, we better listen. **Internet inventor Sir Tim Berners-Lee** spoke recently to CNBC were he detailed a vision for a new future, which includes personal artificial intelligence assistants for everyone.

Berners-Lee said that when he invented the web in 1989, "if you were sufficiently switched on geeky, you could get yourself a computer. And you could put a web server on it, you could plug it into the internet. And you could have a website." But in his view, something has gone wrong since, with the concentration of power now in the hands of large internet companies.

His solution? A product that allows users to control their data and how it's used. Currently, internet companies collect data on users by default, as a way of using their services.

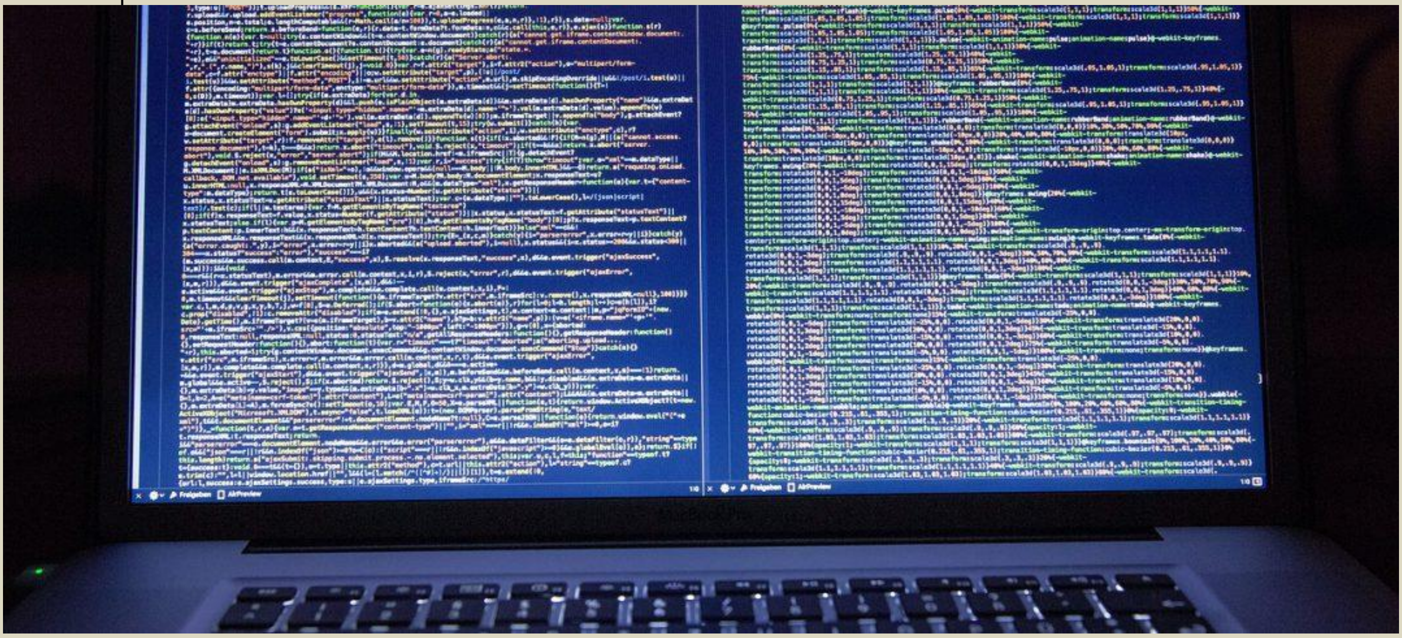
But Berners-Lee and Bruce's start-up Inrupt is working on a different way forward. The aim is for users to have a single sign-on across different products and services on the internet.

Data will be stored in so-called "pods," which are basically a person's personal data online storage container. Individuals can grant a website or service access to their pod, or silo of data, rather than websites taking data by default.

Berners-Lee said that users can run their own AI, much like their own personal version of Amazon’s Alexa or Apple’s Siri, when they have their own data pods. That’s because in the future that Berners-Lee sees, users will have all sorts of data stored in their pods — from fitness information to online shopping habits. The AI could use all that data to learn and be able to assist a user.

## Pakistani Military Organizations Targeted by New Intelligence Tool

Source: https://i-hls.com/archives/118053



Feb 21 – According to recent reports, a new identified hostile tool has targeted military organizations in Pakistan. The tool which was used to send phishing emails that included weaponized documents was traced as NewsPenguin, a seemingly new sophisticated malware.

Once the target opened the attachments to the email, the lure document would use a remote template injection technique to fetch the next stage from a remote server that only serves the payload to Pakistani IP addresses. The victim is promoted to enable editing in the document, which beginning a series of commands to save files and download malicious ones on the victims computer.

The researchers discovered that the malware waits five minutes between commands, likely another attempt to bypass sandboxes, which typically have a time limit of fewer than five minutes per sample.

Based on received commands, the malware collects and sends information about the machine, runs an additional thread, copies or moves files, deletes files, creates directories, sends the content of files to the server, executes files, and uploads or downloads files from the server.

## Quantity Over Quality in Cyber Crime

Source: https://i-hls.com/archives/118292

Mar 01 – As opposed to launching one complex attack against companies and organizations, cyber criminals are looking into expanding their economic scale by simply attacking more than ever before. Instead of using one attack vector against one company, threat actors are targeting an entire supply chain.

“Attackers are moving toward conducting their operations as efficiently as possible,” Wendi Whitmore, SVP at Palo Alto Networks said. “Attackers are now often looking to build an economy of scale.”

Likewise, instead of encrypting data, then decrypting it on the back end, ransomware groups can just steal the information and threaten to release it publicly if their ransom demand isn’t met. When data is stolen, organizations’ top priority is to quickly resolve issues and ensure client data isn’t exposed.

Threat actors know that and they’re optimizing business operations not just in techniques or processes, but also in the tooling they use, Whitmore said.

“We’re seeing this concept of commonality and convergence of these actual toolsets they’re using,” she said. This includes tools originally developed by red team security researchers.

“What we expect to see moving forward is even more actors using whatever tooling it takes to get the job done and increasing their efficiency as much as possible,” Whitmore said. “As long as there are secrets to be stolen and money to be made, there are going to be new attacks and new attackers for us to deal with.”

## The US has announced its National Cybersecurity Strategy: Here’s what you need to know

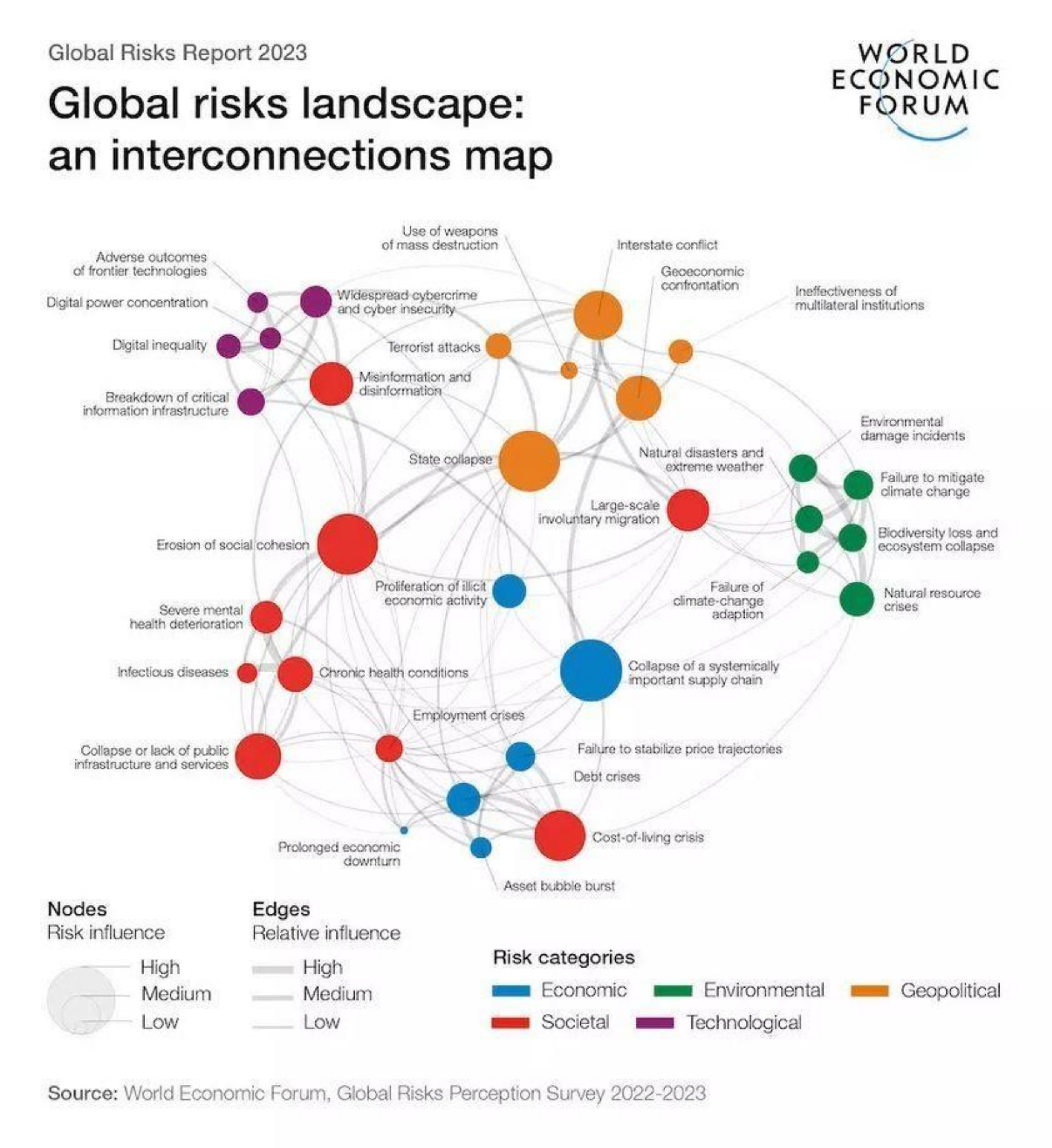
**By Akshay Joshi** (Head of Industry and Partnerships, Centre for Cybersecurity, World Economic Forum) **and Daniel Dobrygowski** (Head of Governance and Trust, World Economic Forum)
Source: https://www.weforum.org/agenda/2023/03/us-national-cybersecurity-strategy/

March 09 – The US government is continuing efforts to strengthen the country's cybersecurity prowess as well as bolster its overall technology governance strategy. Earlier this month, President Joe Biden released a new National Cybersecurity Strategy, which outlines steps the government is taking to secure cyberspace and build a resilient digital ecosystem that is easier to defend than attack — and that is open and safe for all. "When we pick up our smart phones to keep in touch with loved ones, log on to social media to share our ideas with one another, or connect to the internet to run a business or take care of any of our basic needs, we need to be able to trust that the underlying digital ecosystem is safe, reliable and secure," Biden wrote in the framework's preface.
The strategy is part of a larger effort by the Biden administration to strengthen cyber and technology governance. This included efforts to increase accountability for tech companies, boost privacy protections and ensure fair competition online.

**Why does the US need a National Cybersecurity Strategy?**
The world is increasingly complex and cyberthreats are growing more sophisticated, with ransomware attacks running into millions of dollars in economic losses in the US. In 2022, the average cost of a ransomware attack was more than $4.5 million, according to IBM. The greatest risks we face are interconnected, creating the threat of a "polycrisis", whereby the overall combined impact of these events is greater than their individual impact.
This is equally true of technological risks, where, for example, attacks on critical information infrastructure could have disastrous consequences for public infrastructure and health, or where growing geopolitical tensions heighten the risk of cyberattacks.
Cybercrime and cyber insecurity were seen by risk experts surveyed for the World Economic Forum's *Global Risks Report* as the 8th biggest risk in terms of severity of impact, across both the short term (next two years) and over the coming decade.
In 2022, state-sponsored cyberattacks targeting users in NATO countries increased by 300% compared to 2020, according to Google data. With cyberattacks on the rise, experts at the World Economic Forum's Annual Meeting at Davos predicted that 2023 would be a "busy year" for cyberspace with a "gathering cyber storm".
“This is a global threat, and it calls for a global response and enhanced and coordinated action,” Jürgen Stock, Secretary-General of the International Criminal Police Organization (INTERPOL), said at Davos.
The Forum's *Global Cybersecurity Outlook 2023* also found that 93% of cybersecurity experts and 86% of business leaders believe that global instability will have a negative impact on their ability to ensure cybersecurity over the next two years.
Robust cybersecurity is key to building on the promise of emerging technologies to enable growth and shared prosperity, while minimizing the perils they pose. As Biden notes, "Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defence. "We must ensure the internet remains open, free, global, interoperable, reliable, and secure – anchored in universal values that respect human rights and fundamental freedoms."

**What are the 5 pillars of the National Security Strategy?**
The COVID-19 pandemic accelerated the world's digital transformation, which means we rely on connected devices and digital technology to do more than ever before – putting our lives and livelihoods at greater risk from cyberthreats.
The US' National Security Strategy recognizes the need to rebalance the burden of responsibility for cybersecurity away from small businesses and individuals and onto the public and private organizations best placed to defend cyberspace through "robust collaboration". It also seeks to build cyberspace resilience by balancing the need to address immediate threats, with incentivizing investment in the secure, long-term future of the digital ecosystem. The World Economic Forum’s Centre for Cybersecurity drives global action to address systemic cybersecurity challenges and improve digital trust. It is an independent and impartial platform fostering collaboration on cybersecurity in the public and private sectors.

- Salesforce, Fortinet and the Global Cyber Alliance, in partnership with the Forum, are delivering free and globally accessible training to a new generation of cybersecurity experts.


Global Risks Report 2023
Global risks landscape: an interconnections map
WORLD ECONOMIC FORUM
Use of weapons of mass destruction
Interstate conflict
Adverse outcomes of frontier technologies
Geoeconomic confrontation
Ineffectiveness of multilateral institutions
Digital power concentration
Widespread cybercrime and cyber insecurity
Digital inequality
Terrorist attacks
Misinformation and disinformation
Breakdown of critical information infrastructure
Environmental damage incidents
State collapse
Natural disasters and extreme weather
Failure to mitigate climate change
Large-scale involuntary migration
Biodiversity loss and ecosystem collapse
Erosion of social cohesion
Proliferation of illicit economic activity
Failure of climate-change adaption
Natural resource crises
Severe mental health deterioration
Collapse of a systemically important supply chain
Infectious diseases
Chronic health conditions
Employment crises
Failure to stabilize price trajectories
Collapse or lack of public infrastructure and services
Debt crises
Cost-of-living crisis
Prolonged economic downturn
Asset bubble burst
Nodes
Risk influence
High
Medium
Low
Edges
Relative influence
High
Medium
Low
Risk categories
Economic
Environmental
Geopolitical
Societal
Technological

**Source:** World Economic Forum, Global Risks Perception Survey 2022-2023

How cybercrime and cyber insecurity connect to other global risks - Image: World Economic Forum Global Risks Report 2023

- The Forum, in collaboration with the University of Oxford – Oxford Martin School, Palo Alto Networks, Mastercard, KPMG, Europol, European Network and Information Security Agency, and the US National Institute of Standards and Technology, is identifying future global risks from next-generation technology.
- The Forum has improved cyber resilience in aviation while working with Deloitte and more than 50 other companies and international organizations.
- The Forum is developing a unique exchange platform for cybersecurity leaders across the electricity industry in collaboration

- The Council on the Connected World agreed on IoT security requirements for consumer-facing devices to protect them from cybers threats, calling on the world's biggest manufacturers and vendors to take action for better IoT security.
- The Forum is also a signatory of the Paris Call for Trust and Security in Cyberspace, which aims to ensure global digital peace and security.

Each of the five pillars it sets out are broken down into strategic objectives, but here's a quick overview of what they entail:

**1. Defend critical infrastructure**

To build confidence in the resilience of US critical infrastructure, regulatory frameworks will establish minimum cybersecurity requirements for critical sectors.

**2. Disrupt and dismantle threat actors**

Working with the private sector and international partners, the US will seek to address the ransomware threat and disrupt malicious actors.

**3. Shape market forces to drive security and resilience**

Grant schemes will promote investment in secure infrastructure, while liability for secure software products and services will be shifted away from the most vulnerable and good privacy practices will be promoted.

**4. Invest in a resilient future**

A diverse cyber-workforce will be developed and cybersecurity R&D for emerging technologies including postquantum encryption will be prioritized.

**5. Forge international partnerships to pursue shared goals**

The US will work with its allies and partners to counter cyberthreats and create reliable and trustworthy supply chains for information and communications technology.

**How do the Forum's cybersecurity efforts support the priorities identified in the US strategy?**

In response to the need for global public-private collaborative efforts to address the growing cybersecurity challenges, the World Economic Forum launched the Centre for Cybersecurity in 2018. The Centre's community, which spans over 150 organizations from the public and private sector, has identified three key priorities: building resilience, strengthening global cooperation to address cyberthreats, and understanding future networks and technology to build trust. To build resilience and help to protect critical infrastructure from cyberattacks, the Forum has convened stakeholders from across the oil and gas and electricity industries and developed best practices to address shared challenges. These include leadership responsibility for organizational security and resilience across the supply chain, among others. Moreover, the Forum's Partnership against Cybercrime initiative released recommendations for public and private organizations that aim to facilitate dialogue and cooperation on confronting cybercrime. Building on these recommendations, at the Annual Meeting 2023, the Forum — with support from Fortinet, Microsoft, PayPal and Santander — launched the Cybercrime Atlas, an initiative to map cybercriminal activities and identify joint public and private sector responses. To ensure that technologies are more secure and trustworthy, the Forum also launched a Digital Trust Initiative that focuses on better decision-making around cybersecurity, privacy, human rights and ethics. The initiative's latest report emphasizes the need for a comprehensive view on technology development that protects and supports individual citizens and their rights and values. The Forum, in partnership with UC Berkeley's Center for Long-Term Cybersecurity, is also working on the Cybersecurity Futures 2030 programme — a foresight-focused scenario planning exercise to inform cybersecurity strategic plans around the globe. As the Forum's *Global Cybersecurity Outlook 2023* notes, cybersecurity is increasingly influencing how and where businesses invest, with half re-evaluating the countries they do business with. A lack of skilled cyber-experts is another threat to business and societies, the report found, with key sectors such as energy utilities reporting a 25% gap in critical skills.

The report also provides recommendations on what leaders can do to secure their organizations in the year to come.

## GPT-4: new features, visual input, availability, and more

Source: https://www.digitaltrends.com/computing/chatgpt-4-everything-we-know-so-far/

Mar 14 – OpenAI calls it the company's "most advanced system, producing safer and more useful responses." Here's everything we know about it so far.

**Availability and release date**

GPT-4 was officially announced on March 13, as was confirmed ahead of time by Microsoft, even though the exact day was unknown. As of now, however, it will only be available in the ChatGPT Plus paid subscription. The current free version of ChatGPT will still be based on GPT-3.5. GPT-4 will also be available as an API "for developers to build applications and services." Some of the companies that have already integrated GPT-4 include Duolingo, Be My Eyes, Stripe, and Khan Academy. The first public demonstration of GPT-4 was also livestreamed on YouTube, showing off some of its new capabilities.

### What's new in GPT-4?

GPT-4 is a new language model created by OpenAI that can generate text that is similar to human speech. It will advance the technology used by ChatGPT, which is currently based on GPT-3.5. GPT is the acronym for Generative Pre-trained Transformer, a deep learning technology that uses artificial neural networks to write like a human.

According to OpenAI, this next-generation language model is more advanced in three key areas: creativity, visual input, and longer context. In terms of creativity, OpenAI says GPT-4 is much better at both creating and collaborating with users on creative projects. Examples of these include music, screenplays, technical writing, and even "learning a user's writing style."

The longer context plays into this as well. GPT-4 can now process up to 25,000 words of text from the user. You can even just send GPT-4 a web link, and ask it to interact with the text from that page. OpenAI says this can be helpful for the creation of long-form content, as well as "extended conversations." GPT-4 can also now receive images as a basis for interaction. In the example provided on the GPT-4 website, the chatbot is given an image of a few baking ingredients and is asked what can be made with them. It is not currently known if video can also be used in this same way. Lastly, OpenAI also says GPT-4 is significantly safer to use than the previous generation. It can reportedly produce 40% more factual responses in OpenAI's own internal testing, while also being 82% less likely to "respond to requests for disallowed content." OpenAI says it's been trained with human feedback to make these strides, claiming to have worked with "over 50 experts for early feedback in domains including AI safety and security."

### Limitations

While discussing the new capabilities of GPT-4, OpenAI also notes some of the limitations of the new language model. Like previous versions of GPT, OpenAI says the latest model still has problems with "social biases, hallucinations, and adversarial prompts."

In other words, it's not perfect, but OpenAI says these are all issues the company is working to address.

### Does Bing Chat use GPT-4?

Microsoft originally states that the new Bing, or Bing Chat, was more powerful than ChatGPT. Since OpenAI's chat uses GPT-3.5, there was an implication at the time that Bing Chat could be using GPT-4. And now, Microsoft has confirmed that Bing Chat is, indeed, built on GPT-4. Still, features such as visual input weren't available on Bing Chat, so it's not yet clear what exact features have been integrated and which have not. Regardless, Bing Chat clearly has been upgraded with the ability to access current information via the internet, a huge improvement over the current version of ChatGPT, which can only draw from the training it received through 2021. In addition to internet access, the AI model used for Bing Chat is much faster, something that is extremely important when taken out of the lab and added to a search engine.

### An evolution, not a revolution?

We haven't tried out GPT-4 in ChatGPT Plus yet ourselves, but it's bound to be more impressive, building on the success of ChatGPT. In fact, if you've tried out the new Bing Chat, you've apparently already gotten a taste of it. Just don't expect it to be something brand new. Prior to the launch of GPT-4, OpenAI CEO Sam Altman said in a StrictlyVC interview posted by Connie Loizos on YouTube that "people are begging to be disappointed, and they will be."

Altman acknowledges the potential of AGI to wreak havoc on world economies and expressed that a quick rollout of several small changes is better than a shocking advancement that provides little opportunity for the world to adapt to the changes.

In short, GPT-4 will be an evolution, not a revolution. According to Altman, the next version of ChatGPT won't be an AGI and it won't have 100 trillion parameters. Those rumors are incorrect.

## New Mixed Reality Training Delivered to Security Forces

Source: https://i-hls.com/archives/118391

Mar 08 – A new military training model is currently in development. The new model combines augmented reality with a physical model of an A Circuit device to provide the most realistic training possible for the largest concentration of security forces in the U.S. Air Force. The A Circuit is a security device – similar to a vault door – safeguarding Intercontinental Ballistic Missile fields that require regular changing of combinations. Because the device is heavy duty but delicate, being off on the combination or even bumping the locking mechanism can cause a user to be "locked out." Unlocking it again is costly and time consuming for teams of Airmen.

The Cyber Innovation Center have developed a prototype that will enhance training for the A-circuit combination changing process, according to cyberinnovationcenter.org.

That prototype was tested from May to September 2022. Approximately 300 Airmen trained on the device during this testing phase. Feedback from testing was positive, with the unique type of training and the opportunity to avoid lockouts specifically singled out for praise. The eagerness of security forces Airmen to train on the device was also highlighted as a benefit.

Master Sgt. Ryan Bell, section chief of the 791st Missile Security Forces Squadron, noted in his feedback that the A Circuit trainer is worth investing in. “This system is teaching something that has, until now, been unteachable due to the risk of breaking a real-world asset,” Bell said. “This type of training is more engaging for the type of learners we now have as the bulk of our enlisted force.”

## ”Cheaper and faster” ChatGPT rival being built in Abu Dhabi

Source: https://www.thenationalnews.com/business/future/2023/03/15/cheaper-and-faster-chatgpt-rival-being-built-in-abu-dhabi/

Mar 15 – The bot wars are heating up with Abu Dhabi entering the arena, announcing its own large language model on Wednesday to compete with the likes of OpenAI, DeepMind and Google. Technology Innovation Institute, a government-backed research hub, introduced Falcon LLM, a model trained on 40 billion parameters that has a wide variety of applications, from chatbots and language translation to content generation and sentiment analysis. “My top priority is to pave the way for the development of more powerful and advanced technologies in the UAE," Ebtesam Almazrouei, a director in the AI research lab at TII, said in an interview with *The National*. "We are committed to making the UAE a key player in the global arena of advanced technology."

She has the platform from OpenAI in her sights as she and her dozen other collaborators at TII work to provide a local alternative.

Falcon is not yet commercially available, and a timeline was not disclosed, but the ambition is to eventually offer the model to government entities, start-ups and the private sector so the economy is less dependent on LLMs from the major tech players in the increasingly competitive — and secretive — artificial intelligence space.

TII, the applied research arm of Abu Dhabi's Advanced Technology Research Council, is a critical part of the UAE's efforts to diversify from a reliance on oil exports and develop a knowledge-based economy. Falcon is a cheaper and faster model to run than GPT-3 and models from DeepMind and Google in an outside performance evaluation by Stanford University, to be published in the coming weeks. Stanford's evaluation is an industry benchmark that tests LLMs on the same scenarios, "allowing for controlled comparisons", according to the university. Falcon's accuracy, bias and its ability to reason will also be tested and those results are expected to be made public in the coming weeks as well. OpenAI announced the latest update to its GPT model, called GPT-4, on Tuesday but declined to reveal how much bigger the LLM is or why exactly it can perform better than its predecessors in an interview with *MIT Technology Review*. “That’s something that, you know, we can’t really comment on at this time,” OpenAI’s chief scientist, Ilya Sutskever, said to the publication. “It’s pretty competitive out there.” The announcement of Falcon is a good reminder that OpenAI's GPT model — while grabbing mainstream attention — is part of a much wider effort by technology companies to capture a part of this booming market. “The year 2023 is turning out to be the year of AI," Dr Ray Johnson, chief executive of TII, said on the research hub's announcement. "Falcon LLM is a landmark announcement for us, but this is just the beginning. By the end of the year, we will be sharing news on a huge increase in capabilities in this space."

“Dad? What does ‘Norad Defense Clearance; OK to proceed’ mean?”

# & Robotic DRONE NEWS

# Switzerland – where the robots of tomorrow are born

## Will the Drone Always Get Through? Offensive Myths and Defensive Realities

**By Antonio Calcara, Andrea Gilli, Mauro Gilli and Ivan Zaccagnini**

*Security Studies | Pages 791-825 | Published online: 21 Dec 2022*

Source: https://www.tandfonline.com/doi/full/10.1080/09636412.2022.2153734

### Abstract

Do emerging and disruptive technologies yield an offensive advantage? This is a question of central theoretical and substantive relevance. For the most part, however, the literature on this topic has not investigated empirically whether such technologies make attacking easier than defending, but it has largely assumed that they do. At the same time, work on the offense–defense balance has primarily focused on land conflicts, thus offering little understanding of the effect of technological change in other domains, such as the air and sea. In this article we address these gaps by investigating whether current- and next-generation drones shift the offense–defense balance toward the offense or toward offense dominance, as many assume—that is, whether drone technology can or will defeat current- and next-generation air defense systems. To answer these questions, we have explored the literature in radar engineering, electromagnetism, signal processing, and air defense operation. Our analysis challenges the existing consensus about the present and raises questions about the future. Our findings also demonstrate how important it is for the field of security studies to embrace greater interdisciplinarity in order to explore pressing policy and theoretical questions.

Do emerging and disruptive technologies yield an offensive advantage? In other words, do they make attacking easier than defending? These are pressing policy and theoretical questions whose answers have deep and far-reaching implications. Technological change that favors the offense exacerbates the security dilemma, promotes arms races, increases incentives for the employment of force, rewards first movers in a conflict, and ultimately can spiral into aggression and war.Footnote[1] This is why scholars and practitioners often worry about emerging military technologies, as happened with cruise missiles, cyber weapons, remotely piloted aircraft (or drones), artificial intelligence, lethal autonomous weapons, and hypersonic missiles, among others.Footnote[2] Perceptions, not factual assessments, often inform such concerns, however: academics, observers, and policymakers tend to assume emerging and disruptive technologies yield an offensive advantage without investigating whether this is empirically true.Footnote[3] Only recently have some academics started to question some of these perceptions, but their attention has been limited to cyber weapons, leaving other emerging technologies relatively untouched.Footnote[4]

In this article, we contribute to this debate by investigating whether armed drones shift the offense–defense balance (ODB) in the air domain—that is, whether drones "will always get through," to paraphrase a famous statement about bombers from the 1930s.Footnote[5] We limit our analysis to armed drones with a maximum takeoff weight above 600 kilograms: drones that belong to the categories of Medium Altitude Long Endurance (MALE) and High Altitude Long Endurance (HALE).Footnote[6] We do not consider mini- and microdrones because of their limited range and payload, which reduce their effectiveness, at most, to the tactical level. Compared to other emerging technologies, armed drones have been employed extensively in conflicts, especially over the past twenty-five years, and they have already spread to many countries—which makes them a current and pressing reality, not a distant possibility.Footnote[7] Despite the extensive attention they have received, no work in security studies and international relations has investigated whether current- and next-generation drones yield an offensive advantage. Conversely, the existing debate has largely relied on untested assumptions, such as that drones are difficult to detect for air defense systems and, therefore, the former favor offensive military operations. Some have questioned these assumptions, but they have provided statements, not explanations. As a result, the academic and policy debate on drones is fraught with unsubstantiated and contradictory claims that impede a correct understanding of this technology. In other words, the drone debate suffers from some of the same pathologies that plagued the academic debate on the ODB: rather than investigating whether technological change affects the ease of attacking or defending (the ODB as a dependent variable), both literatures have assumed that technology has such an effect. Starting from this assumption, they have then studied the implications of a change in the ease of attacking or defending for world politics (the ODB as an independent variable).Footnote[8]

To conduct our analysis, we have first translated existing concerns about drones into testable propositions and then identified what would support such concerns: a major shift in the ODB either toward the offense or to offense dominance. Given the land warfare bias of the literature on the ODB, we have then adapted the parameters the literature uses to measure offensive-enhancing technological change (mobility and armor) so that they can be used to analyze air warfare (avoidance and saturation of enemy air defense systems). Subsequently, to investigate empirically whether drone technology does or will change the ODB against state-of-the-art air defense systems, we have turned to relevant disciplines such as radar engineering, electromagnetism, signal processing, and air defense operation. Our analysis is divided between current-generation drones and next-generation drones.

With regard to current-generation drones, we find that they do not yield an offensive advantage against current-generation air defense systems. Allegedly, three features of these drones endow them with an offensive advantage: their small size, slow speed, and low altitude are thought to lower the range at which drones can be detected and hence lessen the probability that they are intercepted. In fact, small size has relatively limited benefits on the range of detection. Similarly, slow cruise speed can be addressed by changing the filtering functions of air defense systems—radars generally ignore slow-moving objects, as they are unlikely to be potential threats. Finally, the effectiveness of flying at low altitude decreases significantly as the elevation of radars increases (for example, through radar masts, radars atop buildings or mountains, and airborne radars). In sum, current-generation drones possess features that are effective against only some but not all current-generation ground and airborne systems and sensors, and therefore will not be successful, systematically, against countries that possess state-of-the-art air defenses—that is, integrated air defense systems (IADS).

With regard to next-generation drones, the existing debate has focused only on how technological change will affect the offense (drone technology) while ignoring its implications for the defense (air defense systems). This neglect leads to biased conclusions, as it relies on the unwarranted assumption that the capabilities of air defense technologies will remain constant. Air defense systems, however, depend on technologies that have experienced dramatic improvements in recent years, and that promise to advance even further in the future—such as the capacity to collect a larger quantity of more accurate and more diverse data (sensor acuity, diversity of sensors, and multisensor connectivity), to store and access in real time a larger volume of data (big data), and to process more effectively and efficiently a larger volume of data (machine learning).Footnote[9] In fact, when applied to the submarine realm, some scholars argue that these very technological transformations will drastically strengthen the defense and lead to so-called ocean transparency.Footnote[10] Although we cannot make any specific prediction about the future, our analysis suggests caution against taking for granted that next-generation drones will have an offensive advantage against next-generation air defenses.

Our article makes several contributions that go beyond the specific case of drones and speak to broader debates in security studies and international relations theory. First, our article corrects a central problem in the literature on the ODB: its bias for land warfare. This bias is particularly important because criticisms of the ODB have focused on land warfare only, neglecting other domains such as air and naval warfare.Footnote[11] Because of the differences between the air and land domains, however, it is not possible to apply the lessons of the latter to the former. Despite the logical and empirical problems critics point to, the ODB provides a simple but useful heuristic for understanding whether and how the relative ease of attacking vis-à-vis defending in the air domain varies as a result of technological change. And if this outcome is not investigated empirically, analysts, the media, observers, and policymakers might be tempted to rely on unwarranted assumptions, to derive simplistic assessments, and to draw unsubstantiated conclusions.

Second, our article shows that to understand the effect of technological change on the military balance, we need to assess, systematically, the implications for both offensive and defensive technologies. Our article thus corrects a contradiction in the debate on emerging technologies and international stability, which often selectively and inconsistently makes assumptions about the impact of technology on weapon systems and military platforms. For example, we are told that advances in technologies such as quantum radar will cancel the offensive advantage of stealth jet fighters.Footnote[12] At the same time, however, we are also told that less sophisticated emerging aerospace technologies such as armed drones will represent a serious future threat.Footnote[13] But if quantum radars will defeat stealth, there is no intuitive reason why unsophisticated drones will have a future offensive advantage.

Third, our article shows the promise of exploring disciplines outside international relations and political science for addressing pressing academic and policy questions. To fully understand the implications of new weapons, we need to grasp their technical capabilities and limitations. As technology comes to play an ever-increasing role in modern societies, social scientists must incorporate insights from the natural sciences and engineering disciplines. Without such interdisciplinarity, contributing to important policy debates, such as those about arms control, defense acquisition, investments in research and development, and force structure, will become increasingly more difficult.

Fourth, this article also brings attention to air defense. As historian Kenneth P. Werrell has put it, "Readers are more interested in the aircraft than the weapons that bring them down."Footnote[14] This bias is evident also among scholarly works. Radar is the key technology of modern air defense systems, and it is widely credited for having played a decisive role in defeating Nazi Germany in the Battle of Britain and in the Battle of the Atlantic.Footnote[15] Similarly, surface-to-air missiles dramatically enhanced the effectiveness of air defense systems by making high-altitude flight too dangerous even for the most advanced US aircraft, such as the B-52 Stratofortress and the U-2 Dragon Lady, and they forced the cancelation of the XB-70 Valkyrie.Footnote[16] Yet political scientists have paid little attention to these two transformative technologies.Footnote[17] This neglect is particularly evident when compared to nuclear weapons and cyber weapons, especially considering that during World War II investments in research and development in radar were larger than in the Manhattan Project ($2.5 billion versus $2 billion, respectively), and that the Soviet procurement of surface-to-air missile launchers in the 1950s and 1960s turned out to be fifteen times more expensive than the Manhattan Project ($30 billion).Footnote[18] The neglect of air defense is even more remarkable when we contrast it with (ballistic) missile defense, a topic of extensive interest to scholars of nuclear strategy, and one still a matter of controversy.Footnote[19] By shedding light on this topic, we thus hope to rebalance the bias in the literature toward defining technologies of the post–World War II era.

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

**Antonio Calcara** is a postdoctoral researcher at the University of Antwerp.
**Andrea Gilli** is a senior researcher at the NATO Defense College.
**Mauro Gilli** is a senior researcher at the Swiss Federal Institute of Technology in Zurich (ETH-Zurich).
**Ivan Zaccagnini** is a PhD student enrolled in a joint program between at the Libera Università Internazionale degli Studi Sociali (LUISS-Guido Carli) and the Vrije Universiteit Brussel (VUB)

## China Unveils Extra-Large, Heavily Armed Drone Submarine That Can Attack Foreign Warships In Stealth Mode

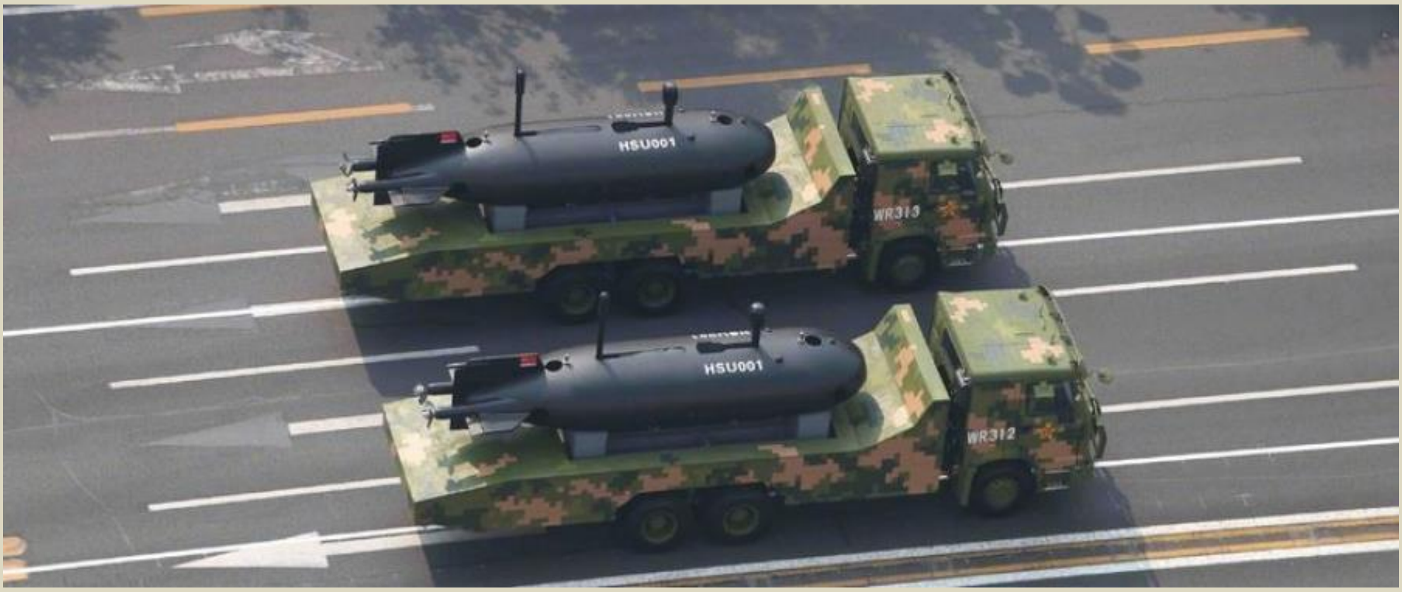
Source: https://defence.pk/pdf/threads/china-reveals-new-heavily-armed-extra-large-uncrewed-submarine.761446/

Feb 23 – New evidence points to China's XLUUV (extra-large uncrewed underwater vehicles) being armed with torpedoes. This is a significant leap in this space and, together with a large-scale development program, may be out-pacing the West.

Extra large uncrewed underwater vehicles (XLUUVs) are quickly becoming a major trend in naval warfare. Leading navies have initiated programs to develop and explore these. Currently, the U.S. Navy and Royal Navy appear to be in the lead, both in **experimentation and in orders**.

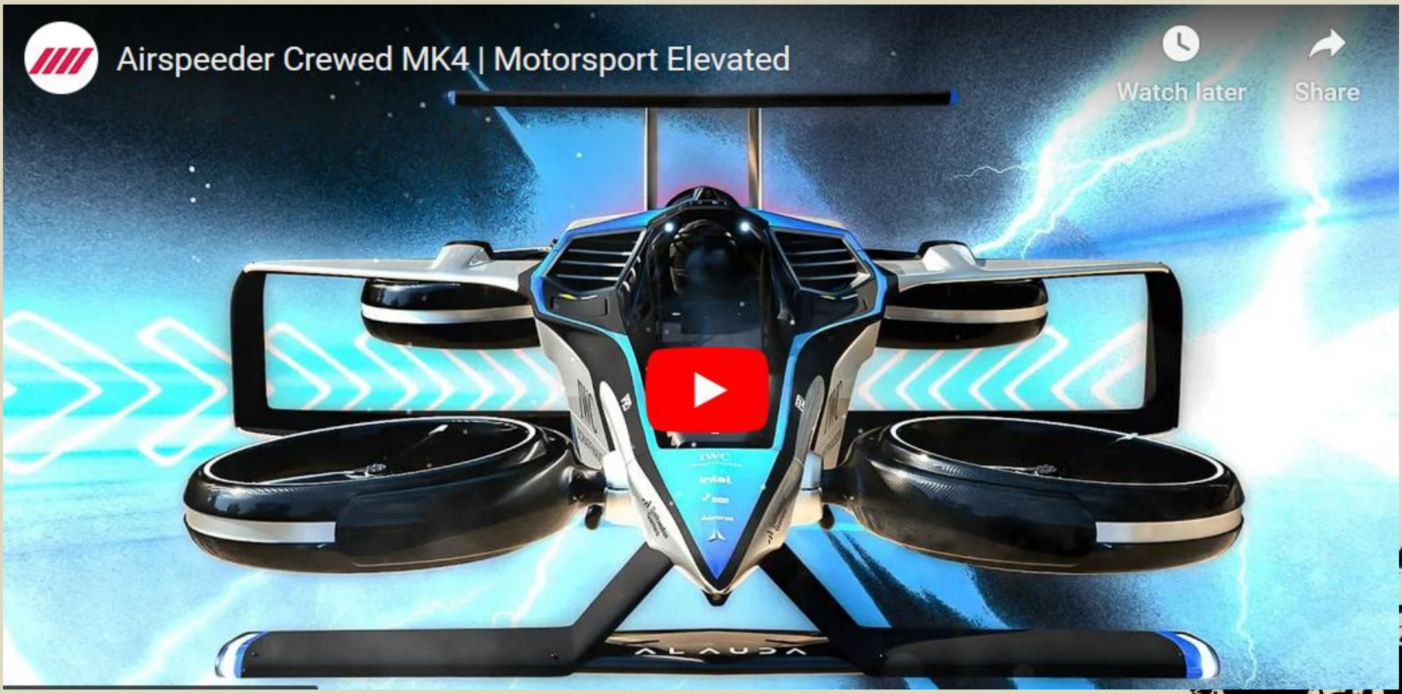
But China too has been working on this capability. China has at least 5 designs in the water, many more than any other navy. But their development has been shrouded in secrecy.

Now new information from the NAVDEX 2023 defense exposition in Abu Dhabi, UAE reveals details of their designs for the first time. It indicates that some of China's uncrewed underwater vehicles may be submarine killers. As Naval News reported in September 2022, China has an **extensive yet unreported XLUUV program**. Because China does not discuss these vehicles in public we can only speculate on many details. Defense analysts can look for indications in the crafts' size, form, where it is tested and from the context of the trials. But the satellite imagery available can only give hints. The defense expo changes this. The visuals used by Chinese shipbuilding organization CSSC 705 Institute are significant. They show an XLUUV broadly in line with some of the vehicles previously observed in satellite imagery in China. Displaying a visual of an XLUUV suggests an export product so care needs to be taken extrapolating it to Chinese Navy (PLAN) projects. all the same it is useful information about China's domestic projects.



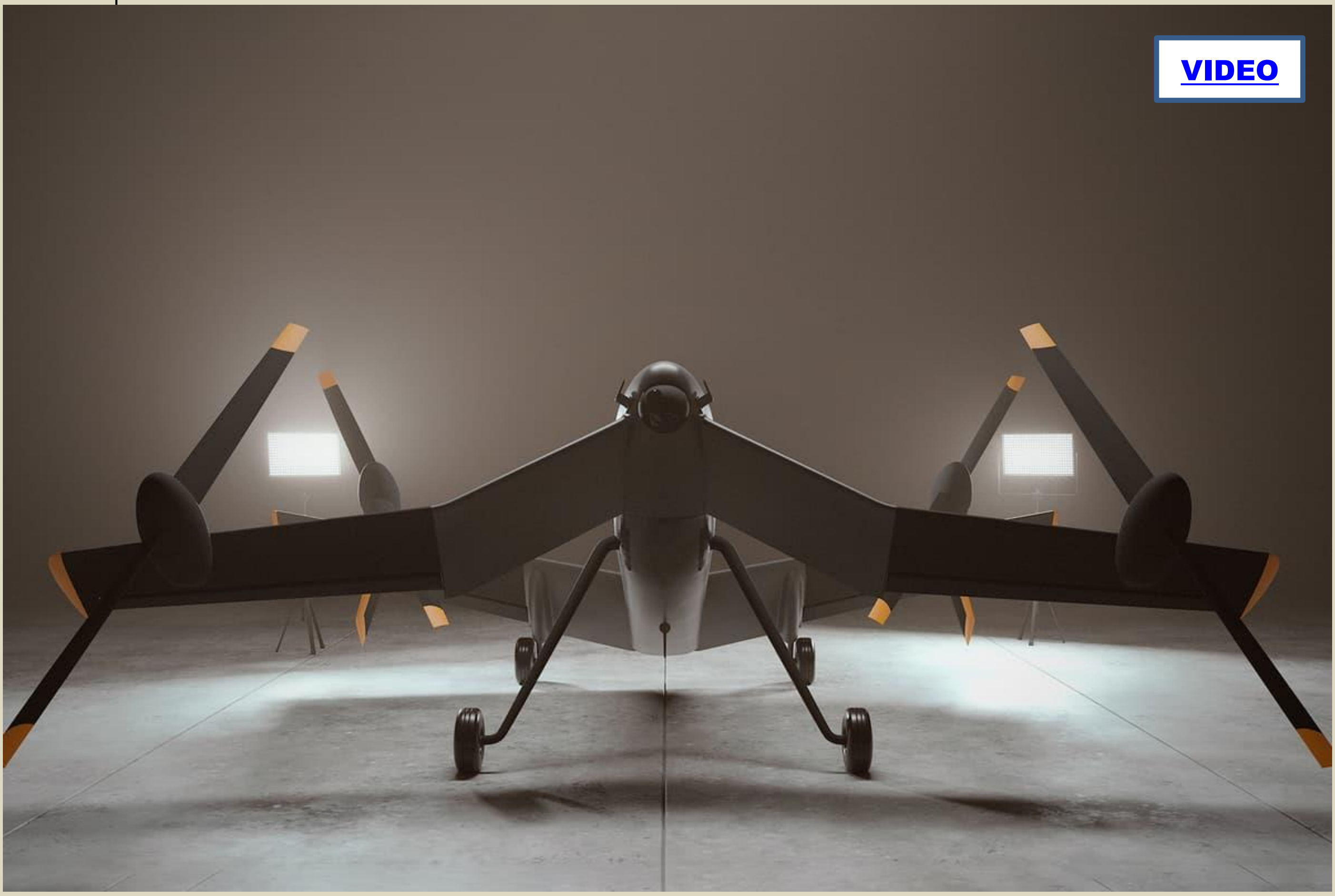
Unusually, the XLUUV has a structure along its side which is consistent with flank array sonar. Even more unusually, this is combined with telltale doors for four torpedo tubes in the chin position. Taken together it implies an anti-ship and/or anti-submarine role. Several other large uncrewed underwater vehicle designs also feature a sonar like this. Notably the French Oceanic Underwater Drone Demonstrator and South Korean ASWUUV. But the Chinese design is the first to combine it with weapons. Arming autonomous underwater vehicles with weapons which require target identification, such as torpedoes, is problematic. It increases risks of blue on blue (or for China, red on red) accidents. It also raises ethical and legal questions about human out of the loop kill chains. This is because underwater vehicles like this cannot realistically be controlled by humans. They have to be autonomous, so the decision to shoot the torpedo has to be automated. However, China appears more comfortable than other nations to take these risks. At least that's the indication based on what little we know so far.

## The world's fastest hydrogen electric (eVTOL) aircraft



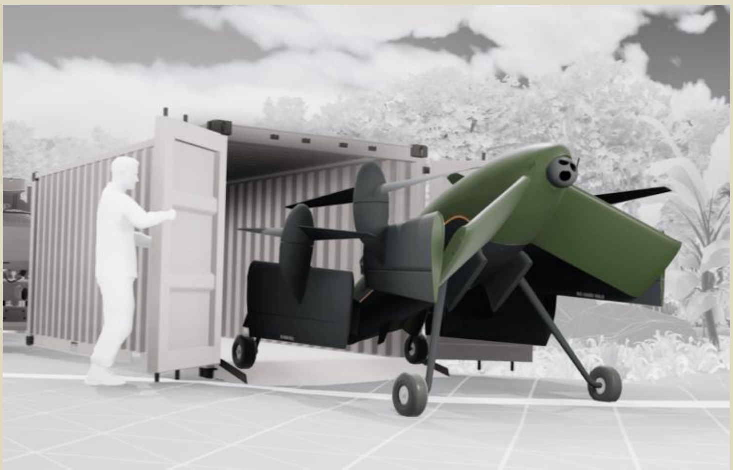
## BAE unveils the Strix, a fascinating, tail-sitting X-wing VTOL UAV

Source: https://newatlas.com/aircraft/bae-strix-vtol-uav/

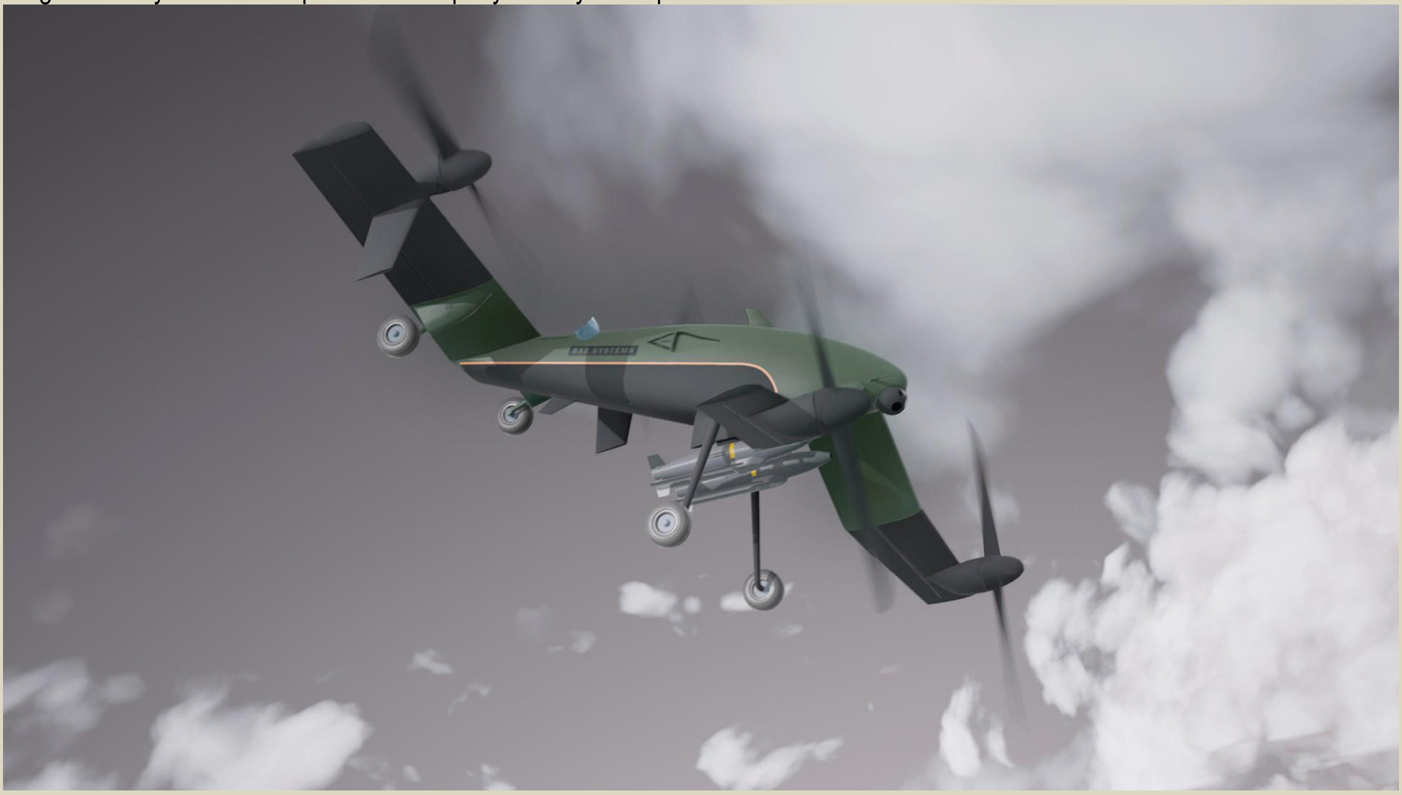


Feb 27 – BAE Systems has unveiled a fascinating new autonomous, hybrid, VTOL UAV for military use. The STRIX, developed in Australia, folds to fit inside a shipping container, and is capable of carrying 160 kg (353 lb) of payload over 800 km (500 miles).

The STRIX was unveiled this morning at Australia's Avalon Air Show, in front of air force chiefs from around the world – with the notable exceptions, according to the ABC, of Russian and Chinese delegates, who have been excluded from the conference.



BAE Systems has developed the aircraft in conjunction with Perth-based company Innovaero. It describes the Strix as a "hybrid, tandem-wing, multi-domain and multi-role UAS," capable of performing missions including air-to-ground strike, persistent intelligence, surveillance and reconnaissance, or potentially serving as a "loyal wingman" – style force multiplier to accompany military helicopters.



The airframe is a nuggety design, with medium-width wings at the front and rear. The forward wings are tilted downward, the rear wings upward, giving it an X-wing kind of configuration when viewed from directly in front of it. Large-diameter propellers are mounted at the four wing tips. Landing gear are attached directly to the tail of the aircraft, and on long stilts forward of the center, allowing the Strix to roll along the ground with its nose lifted at an angle.

The wings are foldable, and with the props in the right orientation, the Strix folds down to 2.6 x 4.5 m (8.5 x 14.8 ft) in size, making it easy to roll into a standard size container, so it can easily be moved about on a truck.

It can be launched and landed vertically without the need for a runway; the upward tilt at rest allows it to stand straight up on its back wheels under propeller power, and then lift off and land off the rear wheels alone, like a tail-sitter.

Its hybrid power system gives it an impressive range and endurance, carrying a range of different mission-specific payloads and munitions. It can run fully autonomously, controlled by BAEs own Strix Vehicle Management System – which is already in use for other autonomous platforms, including the M113 autonomous armored vehicle, and the jet-powered MQ-28 Ghost Bat loyal wingman UAV. This can be run from a ground station, or the Strix can be controlled from on board a helicopter to expand its capabilities and protect an air crew in a high-threat environment.

"STRIX could be ready for operational service as soon as 2026 and work is already underway on a STRIX prototype," says BAE Systems Australia CEO Ben Hudson in a press release. "We're excited that this is the first UAS of its kind to be developed in Australia and look forward to working with partners across the country to deliver this capability to customers."

## BAE unveils low-cost, high-volume precision guided missile kits

Source: https://newatlas.com/military/bae-razer-guided-missile/

Feb 27 – Along with its new X-winged VTOL military drone, BAE Systems has announced a new "Razer" system designed to take standard non-guided munitions and convert them into precision guided missiles, at low cost, and delivered through local manufacturing.

The current conflict in Ukraine has taught military strategists many lessons. One of these, according to the Australian Strategic Policy Institute, is that modern conflicts will burn through munitions at a startling rate; victory may well be determined by whose supply lines can sustain the delivery of pain and misery for the longest.

For an isolated island nation like Australia, this is serious business. Since 2021, there has been a push to develop "sovereign munitions" – guided weapons that can be designed, developed and manufactured entirely in Australia, without relying on overseas supply chains. All the better if they're cheap enough to roll out at high volume and shoot them without worrying about breaking the bank.

RAZER
BAE SYSTEMS

The Razer system is a wing/body kit, tail unit and guidance and navigation system designed to attach to 40-50-kg standard, non-guided munitions – BAE Systems Australia

At today's Avalon Air Show, BAE Systems unveiled its entry into the field. The Razer is effectively a low-cost upgrade kit for "dumb" missiles, capable of transforming a 40-50-kg (88-110-lb) non-guided munition into a precision, air-launched weapon. As such, it adds a wing kit and tail unit with control surfaces, a powered GPS/INS guidance system, and a navigation system. The Razer is designed as a system that can mount to unmanned aircraft like the Strix X-wing tailsitter, or manned helicopters, giving them an extended-range strike and stand-off capability.

“RAZER can meet urgent local and overseas demand for low cost sovereign munition solutions that could be deployed from the air," said BAE Systems Australia CEO Ben Hudson in a press release. "It could deliver a powerful and affordable battlefield strike capability for users globally.”

## Security Vulnerabilities Detected in Drones Made by DJI

Source: https://www.homelandsecuritynewswire.com/dr20230302-security-vulnerabilities-detected-in-drones-made-by-dji

Mar 02 – Drones shouldn't be able to fly over airports and should have a unique serial number. In theory.
Researchers from Bochum and Saarbrücken have detected security vulnerabilities, some of them serious, in several drones made by the manufacturer DJI. These enable users, for example, to change a drone's serial number or override the mechanisms that allow security authorities to track the drones and their pilots. In special attack scenarios, the drones can even be brought down remotely in flight. The team headed by Nico Schiller of the Horst Görtz Institute for IT Security at Ruhr University Bochum, Germany, and Professor Thorsten Holz, formerly in Bochum, now at the CISPA Helmholtz Center for Information Security in Saarbrücken, presented their findings at the Network and Distributed System Security Symposium (NDSS). The conference took place from 27 February to 3 March in San Diego, USA. The researchers informed DJI of the 16 detected vulnerabilities prior to releasing the information to the public; the manufacturer has taken steps towards fixing them.

### Four Models Put to the Test

The team tested three DJI drones of different categories: the small DJI Mini 2, the medium-sized Air 2, and the large Mavic 2. Later, the IT experts reproduced the results for the newer Mavic 3 model as well. They fed the drones' hardware and firmware a large number of random inputs and checked which ones caused the drones to crash or made unwanted changes to the drone data such as the serial number – a method known as fuzzing. To this end, they first had to develop a new algorithm.
"We often have the entire firmware of a device available for the purpose of fuzzing. Here, however, this was not the case," as Nico Schiller describes this particular challenge. Because DJI drones are relatively complex devices, the fuzzing had to be performed in the live system. "After connecting the drone to a laptop, we first looked at how we could communicate with it and which interfaces were available to us for this purpose," says the researcher from Bochum. It turned out that most of the communication is done via the same protocol, called DUML, which sends commands to the drone in packets.

### Four Severe Errors

The fuzzer developed by the research group thus generated DUML data packets, sent them to the drone and evaluated which inputs caused the drone's software to crash. Such a crash indicates an error in the programming. "However, not all security gaps resulted in a crash," says Thorsten Holz. "Some errors led to changes in data such as the serial number." To detect such logical vulnerabilities, the team paired the drone with a mobile phone running the DJI app. They could thus periodically check the app to see if fuzzing was changing the state of the drone. All of the four tested models were found to have security vulnerabilities. In total, the researchers documented 16 vulnerabilities. The DJI Mini 2, Mavic Air 2 and Mavic 3 models had four serious flaws. For one, these bugs allowed an attacker to gain extended access rights in the system. "An attacker can thus change log data or the serial number and disguise their identity," explains Thorsten Holz. "Plus, while DJI does take precautions to prevent drones from flying over airports or other restricted areas such as prisons, these mechanisms could also be overridden." Furthermore, the group was able to crash the flying drones mid-air. In future studies, the Bochum-Saarbrücken team intends to test the security of other drone models as well.

### Location Data is Transmitted Unencrypted

In addition, the researchers examined the protocol used by DJI drones to transmit the location of the drone and its pilot so that authorised bodies – such as security authorities or operators of critical infrastructure – can access it. By reverse engineering DJI's firmware and the radio signals emitted by the drones, the research team was able to document the tracking protocol called "DroneID" for the first time. "We showed that the transmitted data is not encrypted, and that practically anyone can read the location of the pilot and the drone with relatively simple methods," concludes Nico Schiller.

## A Resistance Group Landed a Drone on Top of a Russian Jet. The Footage Is Incredible.

**By Sébastien Roblin**

Source: https://www.popularmechanics.com/military/aviation/a43170041/belarus-opposition-group-lands-drone-on-russian-mainstay-jet-video/

Mar 03 – We still don't know for 100 percent sure if a Belarussian opposition group managed to damage a valuable Russian A-50 Mainstay aircraft using explosive-laden commercial drones to blasts its fuselage

and huge pancake-shaped radar antennas. But it's looking more likely now that the Belarussian resistance group, known as BYPOL, has released footage of it landing a copter-drone directly on the aircraft's huge Vega Shmel-M ("Bumblee") radar dish, while parked near the Belarussian capital of Minsk, without anyone appearing to notice.

The video shows a quadcopter drone as it approaches the airbase on a sunny winter day, its rotors whining, and leisurely comes to a landing atop the radar dome of an A-50. The intrusion produces no apparent reaction, and the drone eventually lift off and flies away.

A post by BYPOL on the Telegram social media platform states: "Belarusian partisans for 2 weeks with the help of civilian drones purchased in the store, conducted aerial reconnaissance at Machulishchy air base. During one of the successful reconnaissance operations, the drone not only flew into the protected area of the specified airfield, flew near the Russian military aircraft AWACS A-50U, but even landed on its radar station ('dish'). So, how did the regime's vaunted counter-drone system perform, the development and production of which tens of millions of rubles of budget funds were spent? The answer is obvious—not at all. And was information about these incidents reported to the self-appointed ruler? Of course not." The video therefore shows one of several claimed reconnaissance flights—not the kinetic attack against the Mainstay aircraft the group claims took place on Sunday (February 26) using two DJI quadcopter drones, each armed with just under a half-pound (.44 lbs) of TNT-equivalent explosives enhanced with roughly 200 metal balls of shrapnel each. Earlier on Tuesday, February 28, *The Drive* obtained Planet Labs satellite imagery of the airbase that day that showed an intact A-50 at Machulishchy without discernible major damage—implying *if* a kinetic attack took place, its results were too limited to be apparent in satellite imagery.

To be fair, without fuel or armament on landed A-50, there would likely be limited external effects from a blast equivalent to that of a small hand grenade. However, a blast might still cause meaningful damage if it manages to shred the sensitive internal electronics of the radar or satellite uplink just under the skin; or cause melting of internal electronic wiring. A discolored patch on the radar dome's front edge visible in the post-strike satellite photo isn't evident in the new, pre-strike footage.

Overall, if the group managed to literally land a drone on top of the aircraft during a scouting run, it seems a lot more credible that they were able to repeat that feat using two similar DJI drones with light explosive payloads. Such an attack might still cause meaningful damage, even if it's not externally obvious.

### Russia's 'Mainstay' Eyes in the Sky

Like the U.S. Air Force's E-3 Sentry and Navy's E-2 Hawkeye airborne early warning and control aircraft, the Beriev A-50 has a huge 'pizza-dish' radar-dome mounted atop its fuselage, which provides 360-degree radar coverage for hundreds of miles around it. Based on the big Il-76 four-engine transport jet, the A-50 has a flight crew of five, supplemented by 10 specialists who operate a host of sensors, radios, and datalinks to coordinate air and ground forces in response to what its sensors can see.

Russia has only a small fleet of 16 A-50 aircraft, which are in high demand to support wartime operations. Only seven of the Soviet-era jets have been modernized to the A-50U model, which has liquid crystal displays, a satellite uplink and longer range radios (250 miles UHF, 1,242 miles HF), the improved Bumblebee-M radar, a crew lounge and kitchen, and increased fuel capacity.

The Bumblebee-M is better at detecting low-flying and stealth aircraft, and has detection range boosted generally by 20 to 33 percent: claimed capable of detecting fighters and warships at 250 miles and launches of land-based missiles at over 600 miles. It can track 300 object simultaneously, and has datalinks to coordinate 40 intercepts at a time.

A successor, the A-100 equipped with the Vega Premier AESA-class radar, has been stalled in development for years with two prototypes built, in part hampered by inability to obtain components due to sanctions.

Airborne early warning radars particularly have a better vantage than ground-based radars for detecting low-flying aircraft that would otherwise be masked by terrain—a tactic Ukrainian pilots rely upon to close with Russian aircraft equipped with much better radars. The A-50 over Belarus, though unarmed, has thus constituted a persistent menace orbiting for many hours at a time on the northern flank of Ukraine's air defenses as they come under daily attack by drones and cruise missiles.

The aircraft's systems help locate Ukrainian surface-to-air missile sites for attack, and arranging long-range air-to-air missile attacks by Russian MiG-31 and Su-35 jets on Ukrainian fighters trying to defend western Ukraine. Overall, support from A-50s has further reinforced the substantial technical edge of Russian fighters in air-to-air combat.

Therefore, damaging mission-critical systems on a single A-50U would represent a blow degrading Russia's overall air effort.

It also could imply a larger, persistent threat to other Russian aircraft based in Belarus, which may force the diversion of valuable ground-based air defenses or electronic warfare specialists to protect the base. It could also generally impede the tempo of flight operations that—judging from what we see in the video—was deemed completely safe from attack.

Though Belarus's military has not directly joined Putin's invasion of Ukraine, its longtime ruling strongman, Alexander Lukashenko, has permitted Russian ground and air forces to train and stage from there. Russian forces from Belarus led the western prong of Russia's ill-fated drive towards Ukraine's capital of Kyiv in the first weeks of the war, supported by warplanes flying from Belarussian airbases. Since Russia withdrew those troops from that disastrous campaign at the end of March 2022, there haven't been more cross-border ground offensives originating from Belarus. Lukashenko has also resisted pressure from Moscow to directly join hostilities with his country's small military. But the Russian air component in Belarus remains active—including the A-50 jet.

However, since a rigged election in 2020, former members of Belarus's law enforcement agencies formed an activist group called BYPOL. Initially focused on exposing crimes and corruption through its social media presence, in March 2022 the group announced it had participated in successful sabotage of railways used by Russian forces.

While BYPOL's new video doesn't confirm a successful kinetic attack on an A-50, it makes BYPOL's claim that one took place seem more likely given the apparent lack of security near the A-50. It also suggests Belarussians are willing to risk their lives approaching military bases with short-range commercial drones in a bid to trip up Russia's war machine as it continues prosecuting its war with Ukraine.

**Sébastien Roblin** has written on the technical, historical, and political aspects of international security and conflict for publications including 19FortyFive, The National Interest, MSNBC, Forbes.com, Inside Unmanned Systems and War is Boring. He holds a Master's degree from Georgetown University and served with the Peace Corps in China.

# Russia has tested a new weapon against Ukrainian drones: the terrible thing about our "Harpy"

Source: https://eprimefeed.com/latest-news/russia-has-tested-a-new-weapon-against-ukrainian-drones-the-terrible-thing-about-our-harpy/264971/

Mar 08 – "Harpy" based on a sufficiently powerful battery interrupts the connection of the drone with the operator by means of an impulse

A new "Harpy" anti-drone gun has been successfully tested near Donetsk. Its range is from 500 meters to 2 kilometers. "Harpy" "clogs" the drone's receiver with noise, loses contact with the control panel and freezes or flies away to the take-off location.

Their work can be very effective, Vasily Dandykin, captain of the first rank of the reserve, a military expert, told the radio "Komsomolskaya Pravda". Because most small cargo drones fly at an altitude of 800-1000 meters, but they carry grenades or a shot from a grenade launcher, so they can be very dangerous.

– "Harpy" based on a sufficiently powerful battery breaks the connection of the drone with the operator by means of an impulse. So it goes back to where it came from. But the operator hardly ever waits for him at the starting place, because he is afraid of being seen, so the drone will return to an open field.

At the same time, the Harpy is far from the only anti-drone weapon already being used by troops. There is a great line of different weapons already in use. But the expert draws attention to the fact that it should not be confused with electronic warfare stations, which are used on large drones, such as the Strizh.

– This is the first line of defense. Because such drones pose a lot of threats to our fighters and equipment when they drop grenades. And against them "pistols" are very effective. This is about the same as a grenade launcher against a tank, Dandykin explains.

The Ukrainian side also has similar combat means, but the drones used by the Russian army are on a completely different level.

– Ours use very effective devices that the other side does not have: in particular, the Lancet. In the latest modification, it is very difficult for that side to fight against him. It is sufficiently protected from the use of anti-drone weapons, says the expert.

In general, modern methods of warfare in some places turn into a real drone "war". And it is very important which technique is used by both sides. Russia during the special operation has made great progress in this matter. Ukraine also demands the latest developments from its owners, but they still don't give it to them; they fear they will fall into the hands of Russian intelligence.

**IMPORTANT QUESTION**

Mikhail Mishustin approved the procedure for issuing certificates of war veterans to volunteers. In other words, volunteers are now equal to recruits. "All people are fighting for their homeland, and here, it seems to me, this is absolutely fair," said Vasily Dandykin. – Sometimes even volunteers fight more bravely in certain areas. Because it is your conscious choice. In my opinion, this decision is very correct in terms of social justice and support. The same applies to social benefits and medical care. I am a veteran of military operations, following the events in the North Caucasus, and I want to say that this is tangible and material support.

## Ukraine Uses 'Cardboard Drones' To Attack Russia; 'Origami Of Death' Is Assembled Using Glue, Rubber Bands

Source: https://eurasiantimes.com/ukraine-uses-cardboard-drones-to-attack-russia/

**Video 1:** https://www.youtube.com/watch?v=mmv7H4jGXgo

**Video 2:** https://www.youtube.com/watch?v=L_djKZ4m7iQ

Mar 09 – Ukrainian armed forces are using drones made out of cardboard and rubber bands to fight the Russian Army. At least 100 of these cheap drones, produced by an Australian company SYPAQ, are being supplied to Ukraine monthly in flatpack form.

Knowns as the Corvo Precision Payload Delivery System (Corvo PPDS), these drones are being supplied by the Melbourne-based company as part of an initiative launched by the Australian government in July 2022.

SYPAQ developed the Corvo PPDS under an AU$1.1 million government contract and pitched it to the Australian Army as a low-cost disposable logistics drone for delivering small, urgent supplies.

The company has not yet disclosed exact specifications or details of the number of drones being shipped to Ukraine or the timing of deliveries. However, according to openly available information, the drones are supplied in flatpack form, with bodies made out of waxed cardboard. They are effortless to assemble using only a glue gun, knife, pen, and tape. A spanner is needed to attach the propeller. This was revealed by a group of Australian soldiers in 2019 who assembled the Corvo PPDS.

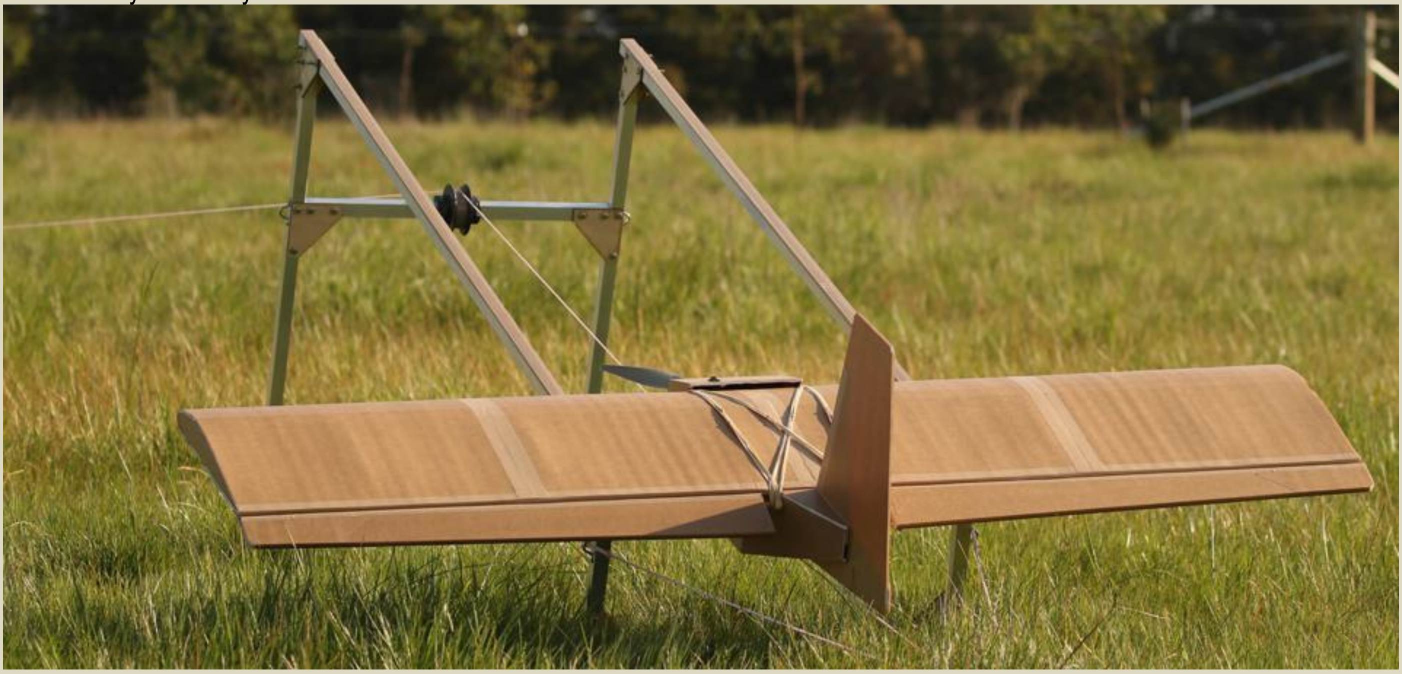
The Corvo Precision Payload Delivery System (SYPAQ)

"Corvo PPDS was easy to put together," Lance Corporal Will Coyer told the military blog Grounded Curiosity. "Certain parts required attention to detail, but the precision manufacturing of the flatpack kit made it simple." The flatpack design makes it very easy to deliver these drones, with 24 of them packed

in pizza-size boxes fitted on a pallet. These boxes also contain the drones' assembly materials, tools, motors, and batteries.
The company has also not disclosed the price of these drones. However, according to certain media reports, each drone costs around US $680-$3,400.

### Origami Of Death

Described by some media reports as the 'Origami of Death,' the PPDS is also very easy to operate, with its flight being programmed through a simple interface on an Android tablet. It flies autonomously with no need for operator control at all.
It uses GPS guidance where available, but if GPS is jammed, the control software can determine its position from the drone's speed and heading.
This means that the drones can perform missions even under heavy radio jamming, which is an essential factor in the Ukraine conflict where Russian electronic warfare, as previously discussed by EurAsian Times, has been very effective in downing many Ukrainian drones.
According to military commentators, Ukraine is not using these drones for logistics but for battlefield awareness and even kinetic missions.
"Following feedback from end-users in Ukraine, the system has also been adapted for intelligence, surveillance, and reconnaissance missions," SYPAQ stated in a press release.
This could mean that the PPDS will be sent over Russian-occupied territory in Ukraine, equipped with a camera or other sensors to gather intelligence or conduct surveillance or reconnaissance.
The drone is launched using a small catapult with a range of 120 kilometers. It could be used for drone-assisted long-range fires against targets as far as 60 kilometers, thereby enabling the much better deployment of HIMARS and other long-range systems that have already been very effective.



The Corvo PPDS is launched via a catapult (SYPAQ)

Furthermore, the PPDS are also being used for 'kinetic missions,' according to Ukrainian ambassador to Australia, Vasyl Myroshnychenko, who recently said that "Ukrainian soldiers are already using them (PPDS) for a variety of missions including lethal ones." Myroshnychenko described these drones saying, "It looks like something that kids would play with, but when you see what it can do, it's really amazing. They have been very good at inflicting damage on the enemy."
Notably, the PPDS, despite being simple and basic to construct, is much more sophisticated than some of the homemade drones the Ukrainian forces have been using for bombing Russian positions.
Also, Ukraine is currently using thousands of small quadcopter drones. However, the operators of these drones often complain about their limited range and how they would instead use a fixed-wing design to fly more than a few kilometers. Therefore, the PPDS also seems to fulfill the exact requirement of the Ukrainians for reconnaissance and strike missions. Also, conceptually, these drones are not very different

from the Iranian-made Shahed kamikaze drones, which the Russians have been using effectively to destroy Ukraine's critical infrastructure.

While the cardboard-made airframe of the drone may not last for more than a few missions, reports suggest that it could easily be replaced by one made of more robust low-cost material like plywood.

## Russian fighter jet collides with US drone causing it to crash into Black Sea

Source: https://www.theguardian.com/us-news/2023/mar/14/russian-fighter-jet-collides-us-drone-black-sea-crash

Mar 14 – A Russian fighter has collided with a US Reaper drone, forcing it down into the Black Sea, in what US forces called an "unsafe and unprofessional" intercept.

A US European Command statement said the collision happened just after 7am on Tuesday morning, when two Russian Su-27 fighter jets flew up to the **MQ-9 Reaper** drone over international waters west of Crimea. The statement said the Russian pilots sought to disrupt the US aircraft before the collision.

"Several times before the collision, the **Su-27s** dumped fuel on and flew in front of the MQ-9 in a reckless, environmentally unsound and unprofessional manner," the US statement said. "This incident demonstrates a lack of competence in addition to being unsafe and unprofessional."

One of the Russian fighters then struck drone's propeller "causing US forces to have to bring the MQ-9 down in international waters".

The European Command statement warned: "These aggressive actions by Russian aircrew are dangerous and could lead to miscalculation and unintended escalation.

"Our MQ-9 aircraft was conducting routine operations in international airspace when it was intercepted and hit by a Russian aircraft, resulting in a crash and complete loss of the MQ-9," Gen James Hecker, the US Air Force commander for Europe and Africa, said. "In fact, this unsafe and unprofessional act by the Russians nearly caused both aircraft to crash."

It is believed the Russian Su-27 landed at an airbase in occupied Crimea.

The incident has highlighted the dangers of clash leading to escalation through mistake or miscalculation as Russia and Nato forces field increasing amount of military hardware around Ukraine – risks heightened by reckless behaviour.

The European Command statement said that the incident was part of a "pattern of dangerous actions by Russian pilots while interacting with US and allied aircraft over international airspace, including over the Black Sea".

In the White House on Tuesday, the national security council spokesman, John Kirby, said: "It is not the first time certainly in recent weeks there's been intercepts."

But Kirby added: "It is the first time that an intercept resulted in the 'splashing' of one of our drones."

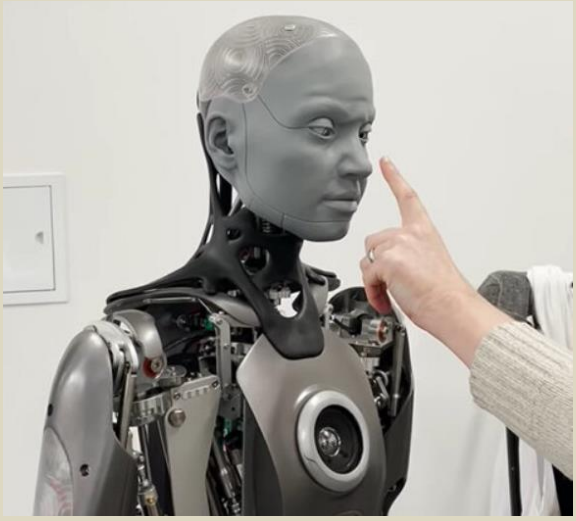
He said that Joe Biden had been briefed on the incident and that US diplomats would contact their Russian counterparts and "expressing our concerns over this unsafe and unprofessional intercept".

He stressed the US drone had been operating over international waters, and that the collision would not deter US forces from patrolling the Black Sea.

"US will continue to operate in international airspace over international waters," Kirby said. "The Black Sea belongs to no one."

# World's most advanced humanoid robot

Source [+video]: https://www.designboom.com/technology/humanoid-robot-ameca-reacts-nose-poke-engineered-arts-12-27-2021/



The UK-based robotics firm engineered arts unveils a video, giving a glimpse at its latest AI-driven humanoid robot dubbed 'ameca'. presented as the world's most advanced human-shaped robot, ameca reacts to a human waving finger. employing high-resolution cameras for eyes to scan the surrounding area, the robot can respond to the movements of the finger, while with a nose poke it seems to become upset.

*'Designed specifically as a platform for development into future robotics technologies, ameca is the perfect humanoid robot platform for human-robot interaction,'* **noted the company.** as the researcher moves the finger closer to the robot's face, ameca reacts grabbing the hand and pulling it away.

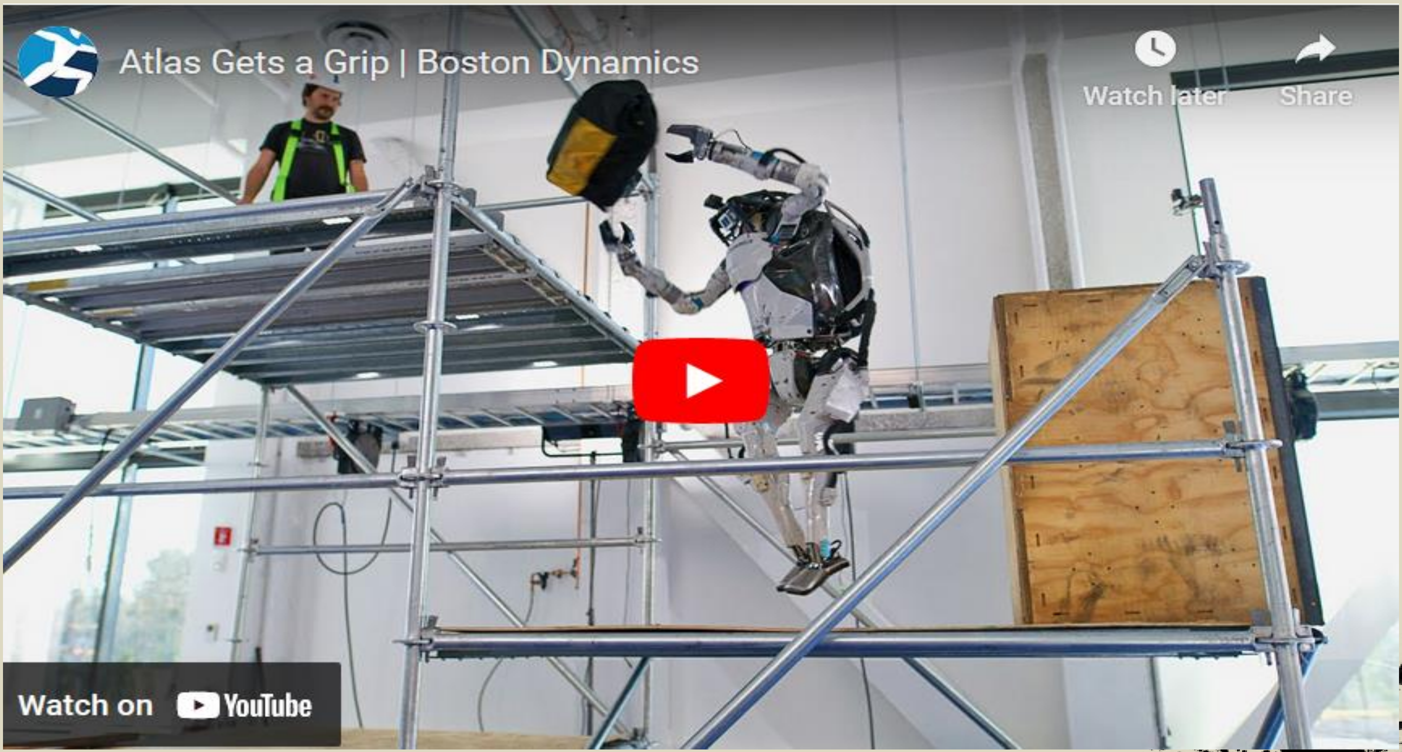
### Ameca's reaction freaks out its creators

The robot's creators freaked out with ameca's reactions as the finger entered its 'personal space', but as they said, they get used to it. ameca is available for purchase — through the engineered arts website — or event rental, but at the current stage, the robot can only operate stationary.

In the first video that was revealed, ameca displays some human-like facial expressions like smiling or frowning. as we see in the clip, the robot appears to wake from a nap, showing surprise for its presence. the video closes with a direct peek into the camera, creating a bizarre feeling for the viewers.

*'We focus on bringing you innovative technologies, which are reliable, modular, upgradable, and easy to develop upon. human-like artificial intelligence needs a human-like artificial body (AI x AB). artificial intelligence and machine learning systems can be tested and developed on ameca alongside our powerful tritium robot operating system,'* **the firm mentioned at its site.***'reliability is key, and all our robots are built to last in action in the real world, not just in the lab. the modular architecture allows for future upgrades, both physically and software to enhance ameca's abilities, all without having to fork out for an entire new robot.'*

# Atlas Robot Demonstrates New Abilities



## Holograms – Getting Closer to Reality

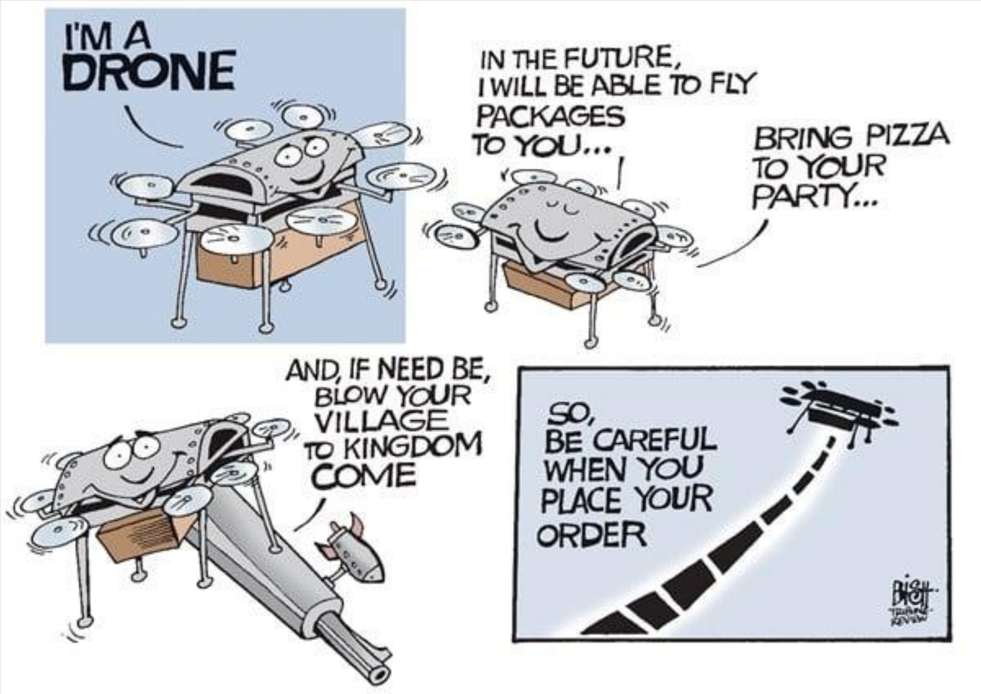
Source: https://i-hls.com/archives/118619

Mar 21 – After more than four years of research, scientists from MIT can now control light at unprecedented speeds, steer the beam in a specific direction, and manipulate the light's intensity, bringing us close than ever before to realizing hologram technology.

It is a programmable, wireless spatial light regulator, or SLM, that can manipulate light at the wavelength scale with "orders of magnitude" faster than existing commercial devices, MIT said. "Generating a freestanding 3D hologram would require extremely precise and fast control of light beyond the capabilities of existing technologies, which are based on liquid crystals or micromirrors," MIT said. Researchers used an array of photonic crystal microcavities to achieve this goal. Upon entering the cavity, the light bounces more than 100,000 times and leaks into space. The process takes just a nanosecond – or one billionth of a second – but it is enough for the device to catch the light and control how it escapes by manipulating the microcavities.

A specially developed algorithm forms the escaping light into a beam, which researchers demonstrated can be quickly and precisely steered in the direction they want. The device controls the light via a micro-LED display.

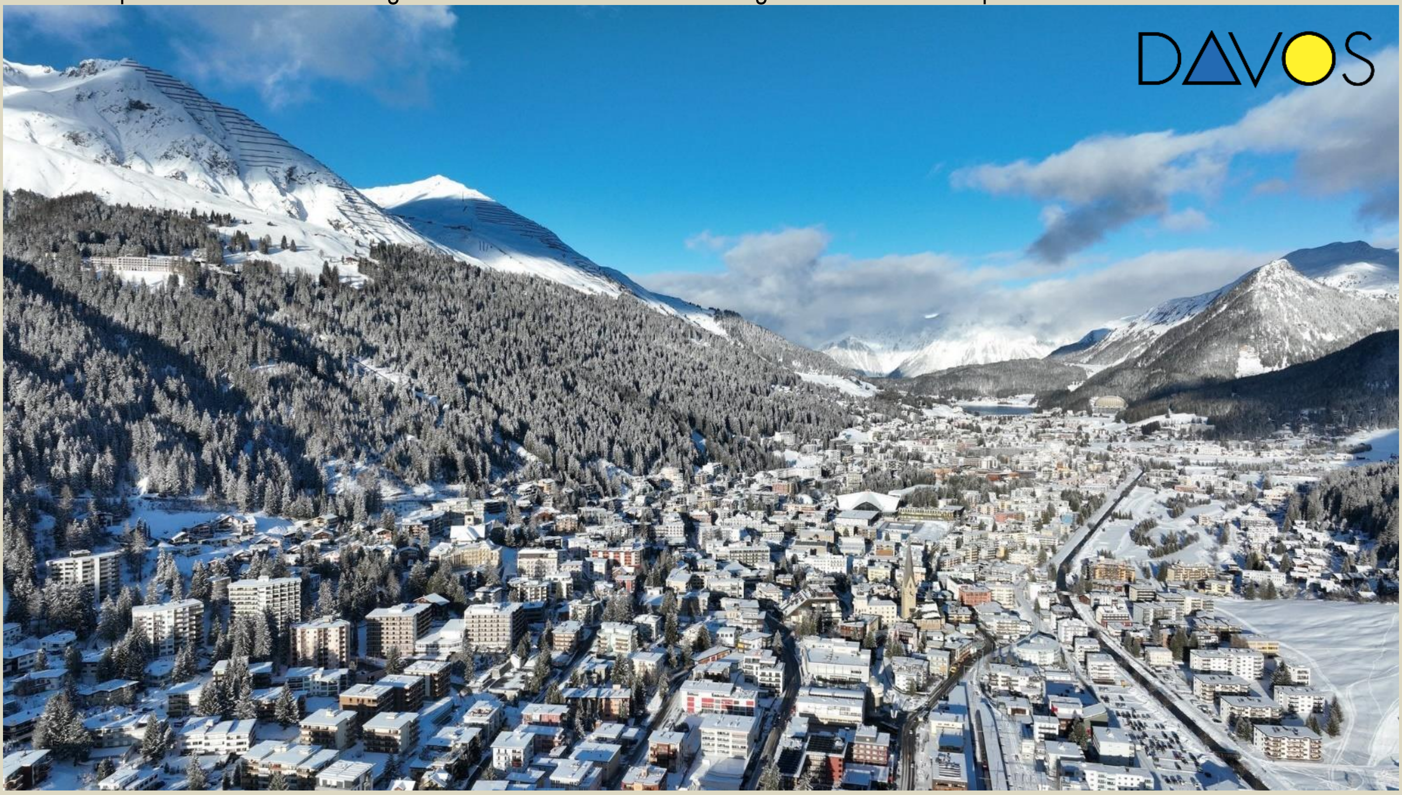
The research was published in Nature Photonics journal and reported on by cybernews.com.


I'M A DRONE
IN THE FUTURE, I WILL BE ABLE TO FLY PACKAGES TO YOU...
BRING PIZZA TO YOUR PARTY...
AND, IF NEED BE, BLOW YOUR VILLAGE TO KINGDOM COME
SO, BE CAREFUL WHEN YOU PLACE YOUR ORDER

# AI - NEWS

## A 'neutral' hub for artificial intelligence in the Swiss Alps

Source: https://www.swissinfo.ch/eng/a--neutral--hub-for-artificial-intelligence-in-the-swiss-alps/48246640



Feb 02 – In a new laboratory in Davos, scientists from all over the world are working to develop algorithms with human-level intelligence. The Swiss Alpine city wants to become known as a research hub for "politically neutral" artificial intelligence to counterbalance the influence of China and the United States.

In a historic villa in the centre of Davos, scientists are trying to understand the fundamentals of human intelligence. They are convinced that decoding the brain is the key to developing an artificial intelligence (AI) that serves humanity instead of autocratic governments or big interest groups. In this way, they hope to help solve the biggest challenges of our century, such as climate change and diseases.

Thanks to its status as a neutral country with strong research capacities, Switzerland has the potential to challenge the approaches of China and the United States, which have been using AI to impose their models of power: dictatorship on the one hand and capitalism on the other.

"Globally, we need a third AI research pole that does not function as a corporation or a state-owned enterprise," says Davos mayor Philipp Wilhelm. "What is missing is a neutral, independent and humanistic approach."

### A centre for neutral AI

Davos, known for hosting the World Economic Forum (WEF) annual meeting, has long been home to renowned research institutes. But until recently, AI was hardly a topic in the valley in southeast Switzerland: it's been more commonly associated with the much larger cities of Zurich, Lausanne and Lugano. That is until Pascal Kaufmann, a Zurich-based neuroscientist with a passion for ancient languages and philosophy, decided to set up an international laboratory for "human-level" AI research, in Davos. Lab42 opened its doors at Villa Fontana in July 2022.

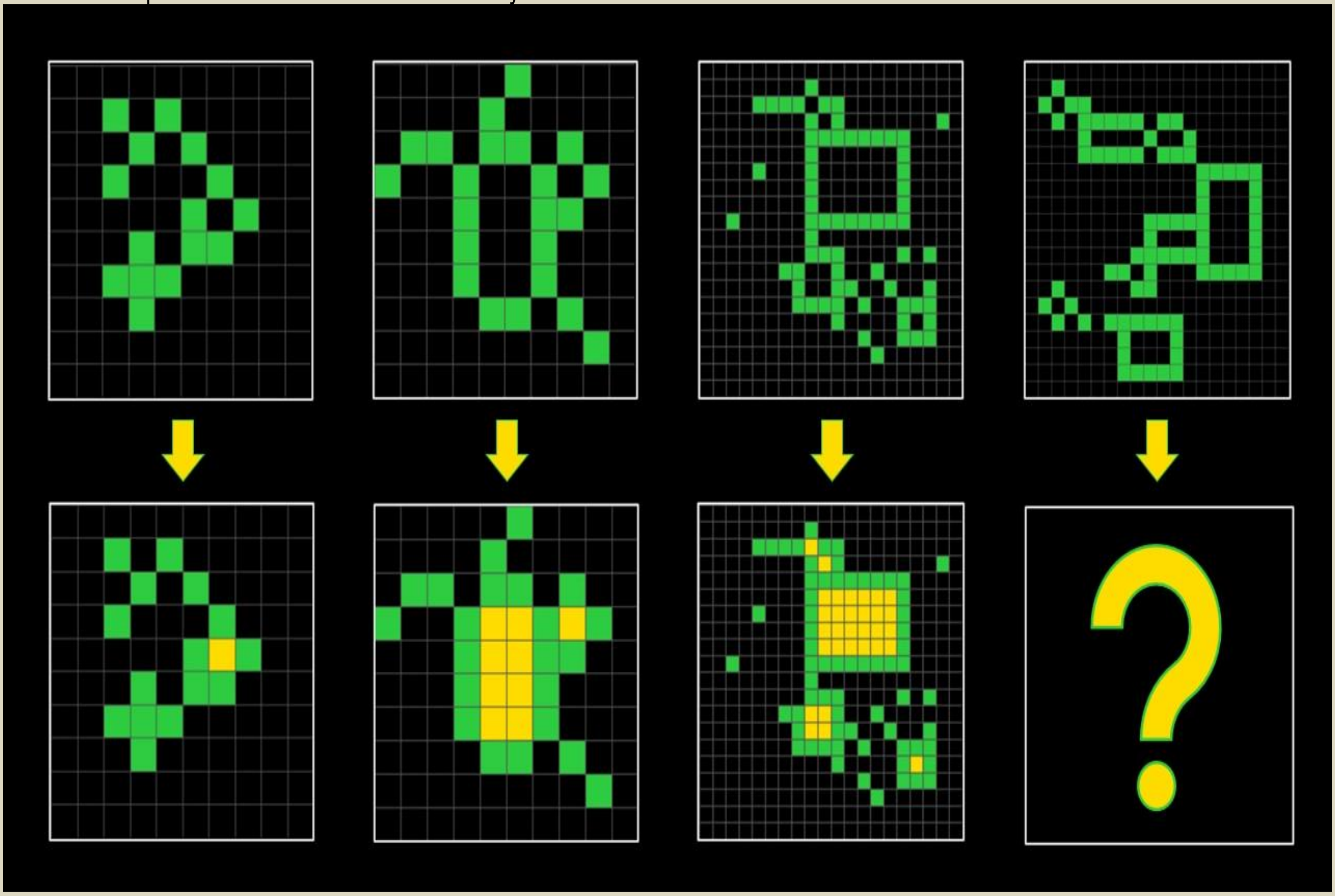
Both Kaufmann and Wilhelm believe that the Alpine resort, with its 11,000 inhabitants, has the prerequisites to attract talent from around the world and become another Swiss AI hub.

"Davos is a world-leading science city, embedded in fantastic nature," says Kaufmann. "The air is clean and the infrastructure is top notch thanks to the WEF."

Kaufmann has a self-described "friendly" relationship with Davos. His NGO Mindfire, which advocates for AI that approximates human intelligence, launched its first initiative to crack the code of our brain in Davos in 2018, inviting experts from around the world. A few years later, when his team wanted to turn these

initiatives into a laboratory with a physical location and a virtual community, the city welcomed them with open arms.
“The Davos approach is to research the most important global issues,” says the city’s mayor Wilhelm. “Digitalisation is one of them.”

**Brilliant minds wanted**
But the network that Kaufmann and his colleagues aspire to build goes far beyond the Alps. Using online challenges in the form of puzzles or multi-level games that current machine learning approaches and algorithms cannot yet solve, the Lab42 team scouts the brightest minds in the field of AI around the world and connects them with each other. An example is the Abstraction of Reasoning Corpus (ARC), a challenge that the French software engineer and AI researcher François Chollet, currently working for Google, created in 2019. ARC is considered an intelligence test for algorithms and consists of 1,000 different tasks, many of which require abstraction capabilities that AI does not have today.


An example from the ARC challenge - an intelligence test for artificial intelligence. François Chollet

The participants whose algorithms solve the greatest number of tasks win cash prizes and are invited to stay in Davos and contribute to the lab’s research. Around 100 scientists and collaboration partners have visited the lab since July, but Kaufmann says it’s not enough. "To make a real breakthrough in AI, we need hundreds of thousands of scientists to work together," he says.
The lab, funded by donations, employs a dozen researchers. Donors include several public institutions, such as Swiss cantons and the municipality of Davos, as well as the manufacturer MaxonMotor and banks UBS and GKB. There are further private backers, but Kaufmann does not disclose their names.

**'Human intelligence is not enough'**
So far, the most sophisticated AI-based tools have managed to solve only 20% of the ARC test. For this reason, Kaufmann and his team insist on understanding how the human brain works in order to advance AI in areas such as abstraction and reasoning.
"Human intelligence of individuals is not enough to solve the world's problems, but that is where we have to start,” he says.

Lab42 has just launched a global competition called the ARCathon II, with the hope of attracting even more talented people to its circuit. "We want to get to the point where we can build robots that can perform some complex tasks, like planting trees to fight climate change, or develop treatments for incurable diseases," says Rolf Pfister, who heads the lab. AI tests are not the only means to this end: the lab also held a writing competition, which ended at the end of December, to gather opinions on the principles of intelligence from experts and disciplines with no direct link to AI, such as philosophy, biology, and the arts. The third-place winner was a music student.

"It is precisely this transdisciplinary insight from the outside that is very valuable and provides new ideas," says Pfister.

According to Pfister, most technology companies rely on the same approaches, such as those used for the chatbot ChatGPT, despite their inherent limitations. Since its launch in November last year, this technology – capable of simulating and writing human-like interactions – continues to make waves, with tech entrepreneur Elon Musk tweetingExternal link it's "scary good" and "not far from dangerously strong AI". But Pfister believes that although ChatGPT delivers impressive results, it lacks any understanding of the world and is therefore unreliable.

This type of understanding is at the heart of human-level and human-centric AI, says Kaufmann. "Once we know the principle of intelligence, Europe will finally be able to make a qualitative breakthrough in applicable human-level AI and compete with China and the United States, which focus mostly on optimising deep learning and brute force approaches," he says. Kaufmann believes Davos and Switzerland would provide a politically neutral location for the development of responsible, inclusive and democratic AI-based technologies.

Sophie-Charlotte Fischer of the Centre for Security Studies (CSS) at the federal technology institute ETH Zurich also believes that Switzerland can play an important role in the field of AI. Fischer sees Switzerland as a credible host for international AI research and governance initiatives because it is the home of the European headquarters of the United Nations, is one of the most globalised countries in the world, and is neutral and a non-member of the European Union.

However, Fischer, whose research focuses on AI governance and the technological rivalry between the US and China, also says that cooperation on AI has become increasingly difficult as global competition intensifies – as evidenced by the recently introduced US export controls targeting China's semiconductor industry.

### Developing Davos

But Davos, when not overrun by tourists or WEF visitors during the winter season, remains rather isolated geographically. Its mayor Wilhelm says this is no longer a problem in the digital age, pointing out that dependence on large urban centres is decreasing while work-life balance is becoming more important. Davos, with its research institutes, skiing in winter and hiking in summer, offers a good quality of life, he adds. But the lack of living space, especially for locals and those who come to work, is a worry for Wilhelm.

"We are working intensively on a housing strategy to ensure that in the coming years there will be sufficient housing for families, accessible to people of different income classes," he says. Davos' family-friendly policies and job prospects for young generations are close to the heart of 33-year-old Wilhelm, a Social Democrat and one of the youngest mayors in the city's history.

"We want our young people to also participate in the research progress being made in Davos."

## Responsible AI For Military Uses

Source: https://i-hls.com/archives/118246

Feb 24 – "As a rapidly changing technology, we have an obligation to create strong norms of responsible behavior concerning military uses of AI and in a way that keeps in mind that applications of AI by militaries will undoubtedly change in the coming years," said Bonnie Jenkins, the State Department's undersecretary for arms control and international security.

Following an international conference attended by 60 nations around the world, the US launched a new initiative the will encourage the responsible use of artificial intelligence in the military, according to cybernews.com. The declaration has 12 points outlining the role of international law in the use of military-related AI, as well as the necessity of human control in all actions concerning nuclear weapons employment.

Artificial Intelligence can bring great advantages to the military, but at the same time it poses unique risks when applied in this domain. According to the US Department of State, "an increasing number of States are developing military AI capabilities, which may include using AI to enable autonomous systems."

"Military use of AI can and should be ethical, responsible, and enhance international security. Use of AI in armed conflict must be in accord with applicable international humanitarian law, including its fundamental principles. Military use of AI capabilities needs to be accountable, including through such use during military operations within a responsible human chain of command and control," declares the Department in an official statement.

# Artificial Intelligence Reframes Nuclear Material Studies

**By Kristen Mally Dean**

Source: https://www.homelandsecuritynewswire.com/dr20230227-artificial-intelligence-reframes-nuclear-material-studies

Feb 27 – If a picture can tell a thousand words, imagine the frame-by-frame story that can be gleaned from a single video. Five minutes of video containing 200 frames per second can result in 60,000 images — a visual "Moby Dick." Sound tedious to digest and catalog? It is, which explains why scientists don't usually analyze their experiments' videos in such detail.

Wei-Ying Chen, a principal materials scientist in the nuclear materials group at the Department of Energy's (DOE) Argonne National Laboratory, is experimenting with advances in artificial intelligence (AI) to change that. The deep learning-based multi-object tracking (MOT) algorithm he uses to extract data from videos, as detailed in a recently published study, aims to help the U.S. improve advanced nuclear reactor designs. In turn, modernized nuclear power would better produce safe, reliable electricity without releasing harmful greenhouse gases.

Currently, nuclear energy produces more electricity on less land than any other clean energy source. Many commercial nuclear reactors, which supply nearly 20% of total U.S. electricity, use older materials and technology. Scientists and engineers believe newer materials and advanced designs could substantially increase the percentage of clean electricity generated by nuclear power plants.

"We want to build advanced reactors that can run at higher temperatures, so we need to discover materials that are resistant to higher temperature and higher irradiation dose," said Chen. "With computer vision tools, we are on track to get all the data we need from all of the video frames."

Chen assists users and conducts experiments at Argonne's Intermediate Voltage Electron Microscope (IVEM) facility, a national user facility and a partner facility of DOE's Nuclear Science User Facilities (NSUF). The IVEM – part transmission electron microscope, part ion beam accelerator — is one of about a dozen instruments in the world that let researchers look at material changes caused by ion irradiation as the changes happen (in situ). This means scientists like Chen can study the effects of different energies on materials proposed for use in future nuclear reactors.

Understanding why, where and when materials break down and show defects under extreme conditions over the course of their lifetimes is critical in order to judge a material's suitability for use in a nuclear reactor. Extremely tiny defects are the first signs that a material will corrode, become brittle or fail. During experiments, defects happen within a picosecond, or one-trillionth of a second. At high temperatures, these defects appear and disappear in tens of milliseconds. Chen is an expert in IVEM experiments and said even he struggles to plot and interpret such fast-moving data.

The fleeting nature of defects during experiments explains why scientists traditionally captured only a smattering of data points along important lines of measure.

With Argonne funding, Chen has spent the past two years developing computer vision to track material changes from recorded experiments at IVEM. In one project, he examined 100 frames per second from videos one to two minutes long. In another, he extracted one frame per second in videos one to two hours long.

Similar to facial recognition software that can recognize and track people in surveillance footage, the computer vision at IVEM singles out material defects and structural voids. Instead of establishing a library of faces, Chen builds a vast, reliable collection of information about temperature resistance, irradiation resilience, microstructural defects and material lifetimes. This information can be plotted to inform better models and plan better experiments.

Chen stresses that saving time — a frequently cited benefit of computer-enabled work — isn't the exclusive benefit of using AI and computer vision at IVEM. With a greater ability to understand and steer experiments that are underway, IVEM users can make on-the-spot adjustments to use their time at IVEM more efficiently and capture important information.

"Videos look very nice, and we can learn a lot from them, but too often they get shown one time at a conference and then are not used again," said Chen. "With computer vision, we can actually learn a lot more about observed phenomena and we can convert video of phenomena into more useful data."

### DefectTrack Proves Itself Accurate and Reliable

In research published in *Scientific Reports*, Chen and co-authors from the University of Connecticut (UConn) presented DefectTrack, a MOT capable of extracting complicated defect data in real time as materials were irradiated.

In the study, DefectTrack tracked up to 4,378 different defect clusters in just one minute, with lifetimes ranging from 19.4 to 64 milliseconds. The findings were starkly superior to the same work by human counterparts.

"Our statistical evaluations showed that the DefectTrack is more accurate and faster than human experts in analyzing the defect lifetime distribution," said UConn co-author and Ph.D. candidate Rajat Sainju.

Computer vision has multiple advantages; improved speed and accuracy are among them.

“We urgently need to speed up our understanding of nuclear materials degradation,” said Yuanyuan Zhu, the UConn assistant professor of materials science and engineer who led the university’s team of co-authors. “Dedicated computer vision models have the potential to revolutionize analysis and help us better understand the nature of nuclear radiation effects.”

Chen is optimistic that computer vision such as DefectTrack will improve nuclear reactor designs.

“Computer vision can provide information that, from a practical standpoint, was unavailable before,” said Chen. “It’s exciting that we now have access to so much more raw data of unprecedented statistical significance and consistency.”

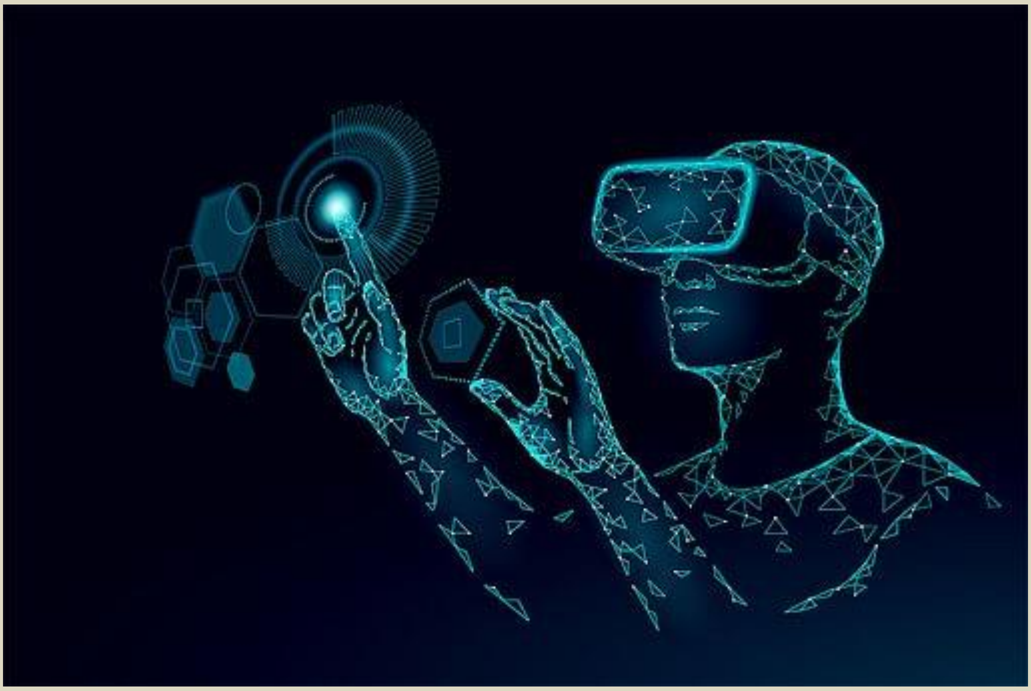
**Kristen Mally Dean** is Communications Coordinator at Argonne National Laboratory.

# Virtual Reality has arrived, but are humans ready for it?

**By Trenton W. Ford**

Source: https://thebulletin.org/2023/03/virtual-reality-has-arrived-but-are-humans-ready-for-it/

Mar 06 – I crawled through a vent with a loaded weapon in hand, hoping a creature wasn’t waiting up ahead. There was a clang in the vent behind. I panicked, spun around to face what was coming, and bumped my head. Pain blossomed; the illusion was broken. I’d hit my head on the rowing machine leaning against the wall.



Lifting the virtual reality (VR) headset, I found myself where I’d been since early afternoon, in my brightly lit living room. Actual reality set in. I wasn’t on a mission to save the world with a supportive cast of characters. Nor was I fighting alien invaders. I was playing the shooter game Half Life: Alyx, and I was alone.

In 1935, American science fiction writer Stanley Weinbaum’s 30-page short story *Pygmalion’s Spectacles* managed a conceptualization of virtual reality eerily similar to modern-day notions. His narrative provides insights into the perspective of a first-time user of reality-bending spectacles and pushes the reader to grapple with emotional and ethical questions about the nature of reality and the realities humans might create. Nearly a century later, humans are finally in a position where asking similar questions isn’t futuristic science fiction; it is, well, reality.

Virtual reality aims to provide abstract, true to life, and hyperrealistic content engagement by providing interactions across multiple natural human sensory and manipulation modalities. This is achieved by using sight, sound, touch, and movement. The expectation is that by including such range of interactions, the user experience will be made more immersive than other digital narrative formats. Research suggests that this hope, even with current technology, is already being realized. It is difficult to draw a causal link between violent media and acts of violence in part due to complexities of most incidents. However, some argue that in cases like the Sandy Hook Elementary School shooting violent video games could have played some kind of role. Even still, entertainment, including movies and games, have produced troubling side-effects, such as their ability to alter human behavior beyond the time spent viewing or playing. Such altered behavior is likely to be exacerbated by the deeper immersion that virtual reality provides.

Developers and technologists differ on how good and how cheap virtual reality technology will be when it’s refined. They also differ on the timeline for its improvement. Still, they seem to agree on the experience’s utility. Rather than looking at claims about how quickly this technology could come into general use, it might be worth focusing on the difficult issues society will have to grapple with as humans adopt this technology more widely. These issues fall into two main categories: ethical and social.

For three decades, modern societies' access to technology and the internet has been increasing at astonishing rates. Some 85 percent of all United States citizens have access to a smartphone, and before the beginning of the COVID-19 pandemic, the average American adult spent 11 hours a day looking at digital screens. During the height of the pandemic that time increased to an average of 19 hours a day. At the same time, connectivity is increasingly influencing the way humans live and even how they design the spaces in which they live. Obviously, not all the ways that increased connectivity affects society are good. Social media use, for instance, is linked to depression, anxiety, and psychological distress in adolescents. Simultaneously, social media platforms employ algorithms that often reinforce user beliefs to ill-effect. Researchers have found even sites like YouTube generate so called filter bubbles, which prioritize content that bolster, or relate to, a user's views and current interests, and that repeated exposure to agreeable or disagreeable information tends to make humans more extreme in their opinions. At the same time, studies have consistently shown that loneliness is on the rise, and that in 2021 more than a third of Americans were experiencing "serious loneliness." While these issues do not lay squarely at the feet of digital innovation, it is clear that the shifting technological landscape is playing a role.

There are an estimated 170 million users of virtual reality worldwide, and as with much technological innovation, adoption is growing quickly. Steam, one of the largest sellers of PC games, has seen exponential growth in users on their platform using virtual reality headsets, and major game developers are aiming to add virtual reality experiences to their catalogs. Companies, including Microsoft and Meta, are developing technologies that use virtual and augmented reality in workplace applications. Researchers are even using simulated experiences to help sufferers of addiction and post-traumatic stress disorder improve. Most new technologies introduce disruptions to the status quo, and if virtual reality lives up to its promise, it has incredible potential to fundamentally reshape the ways humans experience the world.

**Entertainment, connection, and learning**

To explore this topic, I wanted to decide not only what I thought of the current virtual reality experience but to also imagine my feelings towards a future, more complete, *Pygmalion's Spectacles* experience. I bought a Meta Quest 2 headset and a series of accessories and then collected recommendations from gaming and general virtual reality enthusiast communities. Most of the folks recommended games, video media, and collaborative experiences; I tried a smattering of suggestions from each category and found that every experience left me with a different impression.

I play games and might even go as far as to consider myself a gamer. This was my entry point into virtual reality. I thoroughly enjoyed playing games in simulated environments and had some of the most interesting gaming experiences of my life, just standing in my living room. And it's not just me; researchers have found that gamers report improved overall gaming experiences when using virtual reality platforms. My virtual reality gaming experience transported me to the tops of mountains in Skyrim VR (a role playing action experience) and the depths of alien oceans in Subnautica (an underwater adventure). In many of these virtual spaces, I had experiences that went beyond what is possible in reality, taking me into the space of hyperrealism that, in my opinion, is the most compelling feature of the virtual reality experience.

VRChat, and several other socialization applications, allowed me to talk and interact with a surprising number of friends whose presence on these platforms I wasn't aware of. It also gave me the opportunity to meet many other people for the first time, virtually. Immersive collaborative experiences—group art, puzzle solving, and even watching online content inside these virtual environments—added a layer of connectedness that I'd never experienced online, and in some cases that I'd never experienced offline. This shouldn't have been surprising; it's been shown that, at least for small groups, virtual reality users on social platforms experience emotional responses similar to those of face-to-face interactions.

Virtual reality applications for learning might be the most practical use of the platform. While the extent of my learning took place in guided virtual tours, even in that format acquiring facts about places I'd never been was augmented by being embedded in the environment. What's more, I didn't have to leave the comfort of my home for the experience.

But even while having these fantastic experiences, I was concerned.

**Isolation, violence, and addiction**

Whenever I took off the virtual reality headset, the realization that I was alone was disconcerting. *Alone Together* is both the title of a book exploring increasing isolation and loneliness found through technology and a descriptor for what the phenomena looked like in 2011 when the book released. At the time, author Sherry Turkle, a professor of social studies of science and technology at MIT, remarked on the interplay between digital connectivity and physical isolation. Since the book's release more than a decade ago, technology use has only increased, and with it so has loneliness.

When playing Blades and Sorcery, a sandbox sword fighting game, while slashing and stabbing enemies with my right hand, I conjured lightning in my left hand and electrocuted someone with magic (in VR, of course). Unlike the others, this enemy's body fell towards me instead of away. I reflexively pulled back and only then reflected on the number of enemies I'd killed and how I killed them. Researchers have found that people who played violent video games display greater short-term increases in their aggression and decreased empathy when compared to those who just watched violent content. This suggests that interactions in video games have the potential to induce behavioral change. If these findings extend to even more involved interactions possible in simulated environments, then virtual reality has the potential to induce even greater effects on its users.

Current virtual reality experiences appear to have addictive qualities as well. This shouldn't be surprising as most entertainment modalities—like video games and social media—possess similar habit-forming potential to differing degrees. It's reasonable to expect that the increased immersion of virtual reality might confer more significant addictive capacity for users.

### VR ethics

Because virtual reality aims to mirror and, in some cases, go beyond reality, it is reasonable to expect users to experience feelings about these simulated spaces as they would about the real world. If virtual environments can make convincing simulated realities, how much should the ethics of reality bound these virtual spaces?

Shows like *West World*, *The Peripheral*, and tangentially *Altered Carbon* all tell stories largely based around simulated realities. *West World* immediately confronts viewers with scenes of cruel and realistic violence while repeatedly reminding the viewer that it is all taking place in a virtual world. What should a viewer feel when presented with this incongruence? Should people have differing moral frameworks for evaluating acts in the virtual versus the real world?

Even without adding the immersive capabilities of virtual reality, users feel connected to their online gaming and social avatars. Some even consider their avatars to be an extension of themselves. In virtual reality, this connectedness will likely only increase. How strongly do humans consider that extension when contemplating harm that might come to an avatar in a simulated space? Already, during the short time that virtual reality has been available to consumers, there have been noteworthy instances of virtual acts of sexual assault involving user avatars. If people's avatars are extensions of themselves, how then should violations against those selves be handled?

Some suggest that virtual reality transgressions should be handled in the virtual world only; others believe that because simulated harm impacts someone in the real world, standard justice systems should be applied. There are several viable solutions for users causing harm to other users, but what of the cases where user actions are applied to fully virtual characters? These types of characters are referred to as non-playable characters, or NPCs. As the realism of these characters increases, is there some point at which a virtual reality user robbing or killing a non-playable character crosses some ethical boundary? Are there player actions that might be unethical, regardless of whether they cause measurable harm to anyone in the real world?

After thinking about these questions, I've only come up with more questions. What is clear from the reception of shows like *West World* and others like it is that people are fascinated with these questions. It is also clear that there are currently no satisfying answers. As virtual reality adoption increases and society begins to grapple with these issues, I think we should take heed of the virtual worlds that science fiction has explored and understand that without intervention, and maybe even with, most imaginary worlds are darker than our own.

I completed Half-Life: Alyx and had a great time overall. The game ends with an ominous speech from a character called G-Man. In the speech, G-Man offers you the chance to change the future and, with it, reality. Right now, technology is preparing to make a similar offer to us all. Are humans ready for it?

**Trenton W. Ford** is a doctoral candidate in computer science at the University of Notre Dame. His research focuses on misinformation and disinformation in online contexts. Specifically, Trenton's work has involved investigating meme evolution, exploring image-text consistency in news articles, and predicting online community language usage.

## Terrorists Will Use Artificial Intelligence, Too

**By Sam Hunter and Joel Elson**

Source: https://www.realcleardefense.com/articles/2023/03/06/terrorists_will_use_artificial_intelligence_too_885361.html

Mar 06 – As AI technology has exploded into public view, it has raised complex questions about the future of education, the employment landscape for arts and media, and even the nature of sentience. These are all important conversations. But, as terrorism researchers with a particular focus on new and emerging threats, we find ourselves asking a different, darker question:

*How will extremists use AI to hurt people?*

Stated bluntly, AI will allow malign actors to develop plans and ideas that were more challenging or even impossible prior to widespread access of such technology. In the coming years, we believe that understanding the scope of the threat and developing solutions will be critical. As we've explored in previous work on cognition and creativity, expertise is comprised of two components: knowledge (i.e., possessing information) and how that knowledge is organized. The internet has provided just about anyone with access to knowledge. AI, however, *organizes* that information in a useful way and provides a user-friendly output.

Witness, for example, schoolteachers requesting lesson plans complete with discussion questions, exercises, quizzes, and worksheets. Colloquially, we can think of AI as a pocket expert. On any topic. At any given moment. Indefinitely. Without fatigue. There are four key reasons why tools like these can be dangerous in the hands of terrorists.

**Lowered Bar to Entry**

With a pocket expert available to offer deep, organized information on any topic instantaneously, many of the typical barriers around malign acts are removed. An extremist group no longer needs, for example, a chemical engineer who must be recruited and incentivized to join their cause. Instead, information about dangerous compounds can be summarized and synthesized into accessible, digestible, bite-sized chunks perfect for an extremist with no prior knowledge of chemistry.

**Reduced Cost**

Experts are expensive.  AI in all its various forms has taken significant resources to develop but is now cheap. Access for everyone means it must be affordable. It is and will continue to be. In many cases, use of AI is free, with tools packaged into existing software. In the case of ChatGPT, for a nominal fee, users with an entry level knowledge of programming can tap directly into the technology.

**Diverse and Integrated Expertise**

Human collaboration is challenging.  When experts collaborate successfully, they must communicate, coordinate, and integrate, a process that isn't always straightforward and usually involves stumbles along the way. The ability to develop and synthesize information from diverse sources on diverse topics is a key, and concerning feature, of this emerging technology. ChatGPT isn't just a pocket expert.  It's a pocket of experts who can be taught to work well together.

**Iteration and Simulation**

Staring into an asteroid field, Han Solo famously said, "never tell me the odds." Malign actors *want* the odds. AI can give them. A sometimes-unsung feature of AI capabilities is that of iteration and simulation. An AI can examine several scenarios and provide guidance on the path that has the greatest likelihood of success. The result is a set of new malevolent plans that are more likely to succeed in their destructive aims.

**So, what can we do?** A few things:

**Regulate**

The first path forward is an apolitical acknowledgement that regulation is a necessity. Although imperfect, ChatGPT as an example, does have safeguards in place to protect against asking "how do I hurt the most people?" Careful, thoughtful policy around building such safeguards is critical, particularly in the short-term, as there are currently workarounds for such protections.

Historically, there are examples of successfully reigning in new tools and technologies. Dynamite was initially unregulated and used to malicious ends before lawmakers carefully crafted policy limiting its use. Cryptocurrency is a more modern example, with the U.K. passing a law making it easier for law enforcement to seize cryptocurrency linked to terrorism. The U.S. is considering its own laws. Regulating AI will possibly be more difficult, as variants will likely retreat to the darker corners of the web. Yet raising the bar to entry can have a notable impact on the widespread use of AI for malign purposes.

**Red-Team**

The second avenue is red teaming (i.e., generating ideas from the perspective of an adversary) on a large, systematic, and scientific scale. Research indicates that malevolent creativity is largely driven by context. Simply put, many of us have the capacity to think in malevolently creative ways and will do so if the situation demands. The implication here is that we should be putting large teams to the task of thinking like malign actors and using the same tools, in the same ways, against those that seek to cause harm. It is possible – if the broader homeland security enterprise is willing to think like the adversary – to out-creative malign actors.

**Reclaim**

It is important to remember that the factors inspiring hate and targeted violence are the root problem – not the tools themselves. It will be incumbent upon those tasked with protecting the public from terrorism and targeted violence to lean into the use of AI technology in their own efforts. Malign actors will have no qualms about what it means to ask AI how to most effectively harm others. Our national security frontline needs to be as adept with this new technology as the bad guys they're trying to stop.

Just as classroom teachers are exploring ChatGPT as a bulwark against plagiarism, the intelligence community and law enforcement need to expand their cyber education to this front. Our knowledge of AI will almost assuredly grow in the coming years, and new tools and technologies will emerge. Along with them, new issues will certainly present themselves. It is critical to be forward-thinking in our approach – embracing today's technology to anticipate and mitigate tomorrow's threats.

**Sam Hunter, PhD** – Professor of Industrial-Organizational Psychology at the University of Nebraska at Omaha and Head of Strategic Operations at the National Counterterrorism Innovation, Technology, and Education (NCITE) Center of Excellence

**Joel S. Elson, PhD** – Assistant Professor of Information Technology Innovation at the University of Nebraska at Omaha and Head of Information Science and Technology Research Initiatives at the National Counterterrorism Innovation, Technology, and Education (NCITE) Center of Excellence

## Real AI Requires Human Brain Cells to Function

Source: https://www.miragenews.com/real-ai-requires-human-brain-cells-to-function-957918/

Mar 02 – **The future of computing includes biology says an international team of scientists.**

The time has come to create a new kind of computer, say researchers from John Hopkins University together with Dr Brett Kagan, chief scientist at Cortical Labs in Melbourne, who recently led development of the DishBrain project, in which human cells in a petri dish learnt to play Pong.

In an article published today in Frontiers in Science, the team outlines how biological computers could surpass today's electronic computers for certain applications while using a small fraction of the electricity required by today's computers and server farms.

**They're starting by making small clusters of 50,000 brain cells grown from stem cells and known as organoids.** That's about a third the size of a fruit fly brain. They're aiming for 10 million neurons which would be about the number of neurons in a tortoise brain. By comparison, the average human brain has more than 80 billion neurons.

The article highlights how the human brain continues to massively outperform machines for particular tasks. Humans, for example, can learn to distinguish two types of objects (such as a dog and a cat) using just a few samples, while AI algorithms need many thousands. And while AI beat the world champion in Go in 2016, it was trained on data from 160,000 games – the equivalent of playing for five hours each day, for more than 175 years.

Brains are also more energy efficient. Our brains are thought to be able to store the equivalent of more than a million times the capacity of an average home computer (2.5 petabytes), using the equivalent of just a few watts of power. US data farms, by contrast, use more than 15,000 megawatts a year, much of it generated by dozens of coal-fired power stations.

In the paper, the authors outline their plan for “organoid intelligence”, or OI, with the brain organoids grown in cell-culture. Although brain organoids aren’t “mini brains”, they share key aspects of brain function and structure. Organoids would need to be dramatically expanded from around 50,000 cells currently. “For OI, we would need to increase this number to 10 million,” says senior author Prof Thomas Hartung of Johns Hopkins University in Baltimore.

Brett and his colleagues at Cortical Labs have already demonstrated that biocomputers based on human brain cells are possible. A recent paper in Neuron showed that a flat culture of brain cells could learn to play the video game Pong.

“We have shown we can interact with living biological neurons in such a way that compels them to modify their activity, leading to something that resembles intelligence,” says Kagan of the relatively simple Pong-playing DishBrain. “Working with the team of amazing people assembled by Professor Hartung and colleagues for this Organoid Intelligence collaboration, Cortical Labs is now trying to replicate that work with brain organoids.”

“I would say that replicating [Cortical Labs’] experiment with organoids already fulfils the basic definition of OI,” says Thomas.

“From here on, it’s just a matter of building the community, the tools, and the technologies to realise OI’s full potential,” he said.

“This new field of **biocomputing** promises unprecedented advances in computing speed, processing power, data efficiency, and storage capabilities – all with lower energy needs,” Brett says. “The particularly exciting aspect of this collaboration is the open and collaborative spirit in which it was formed. Bringing these different experts together is not only vital to optimise for success but provides a critical touch point for industry collaboration.”

And the technology could also enable scientists to better study personalised brain organoids developed from skin or small blood samples of patients suffering from neural disorders, such as Alzheimer’s disease, and run tests to investigate how genetic factors, medicines, and toxins influence these conditions.

## What Is Biocomputing?

Source: https://medium.com/lansaar/what-is-biocomputing-82671bb381bd

Biocomputing — a cutting-edge field of technology — operates at the intersection of biology, engineering, and computer science. It seeks to use cells or their sub-component molecules (such as DNA or RNA) to perform functions traditionally performed by an electronic computer.

The ultimate goal of biocomputing is to mimic some of the biological ‘hardware’ of bodies like ours — and to use it for our computing needs. From less to more complicated, this could include:

1. Using DNA or RNA as a medium of information storage and data processing
2. Connecting neurons to one another, similar to how they are connected in our brains
3. Designing computational hardware from the genome level up

### Cells Already Compute

Cells are far more powerful at computing than our best computers. For example:

1. Cells store data in DNA
2. Receive chemical inputs in RNA (data input)
3. Perform complex logic operations using ribosomes
4. Produce outputs by synthesizing proteins

Biocomputing’s engineering challenge is to gain a granular level of control of the reactions between organic compounds like DNA or RNA.

### Overheating & High Energy Use

Traditional computers use microchips, which heat up quickly. Supercomputers are usually a collection of several high-speed traditional computers, combined into a single unit. Generally, they are not *qualitatively* different from traditional computers. Even so, supercomputers use a lot of energy, heat up quickly, and require massive cooling units in order to function at full speed. On the other hand, biological matter can perform calculations and process data without using as much energy, and without heating up significantly.

### Multitasking

Regular computers perform one task at a time and switch quickly between tasks to give the user a seamless experience of multiple tasks running simultaneously. Biological systems, on the other hand, engage in ‘parallel computation’ — whereby multiple tasks can be executed truly simultaneously.

Early proof-of-concept work has been completed using myosin — a superfamily of motor proteins which cause muscle contraction and convert chemical energy into mechanical energy. Myosin-enabled biocomputing could perform multiple computations simultaneously.

### Self-Organizing and Self-Repairing

Biological molecules also display an intelligent ability to self-organize and self-repair. So, biocomputing engineers will have to find ways to simulate this intelligent 'software' on top of the biological molecule 'hardware' to produce, organize, and repair the biocomputing system. Similar to a living organism the "software" in biological systems is responsible for producing and assembling the hardware which in turn will help run the software.

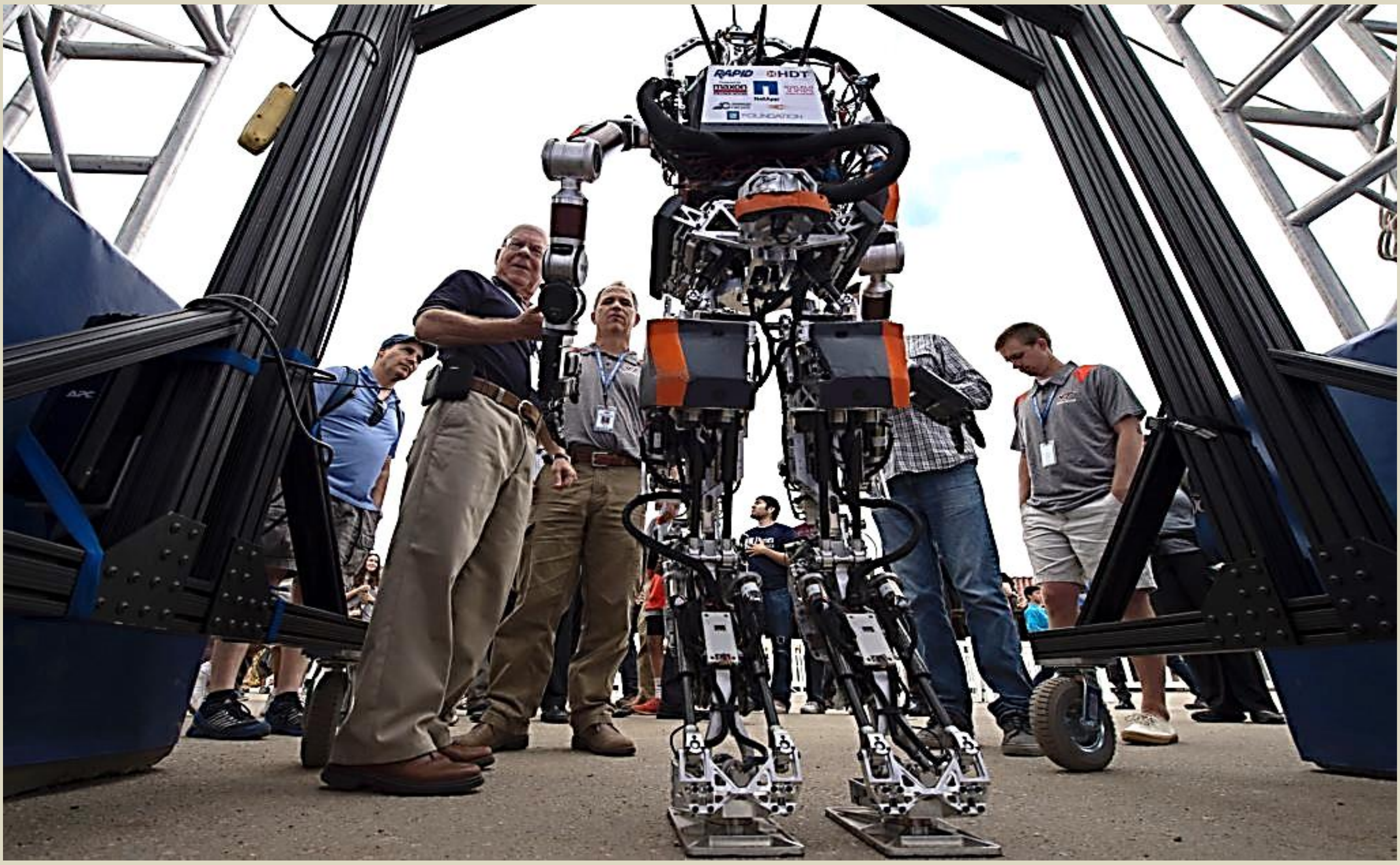
### Conclusion

While biocomputing is in an early phase, biocomputers have the potential to enable far more powerful computing than today's best computers — while using less energy and generating less heat. Furthermore, biocomputers will be able to use parallel computing, which will represent a significant improvement upon regular computing, and will be able to better self-organize and self-repair. While authoritative estimates of the eventual environmental impact of biocomputing do not yet exist, biocomputing could potentially reduce our reliance on the silicon and rare earth minerals that power today's computers.

## Miscalibration of Trust in Human Machine Teaming

**By John Christianson, Di Cooke, and Courtney Stiles Herdt**

Source: https://warontherocks.com/2023/03/miscalibration-of-trust-in-human-machine-teaming/



Mar 08 – A recent Pew survey found that 82 percent of Americans are more or equally wary than excited about the use of artificial intelligence (AI). This sentiment is not surprising — tales of rogue or dangerous AI abound in pop culture. Movies from 2001: A Space Odyssey to The Terminator warn of the dire consequences of trusting AI. Yet, at the same time, more people than ever before are regularly using AI-enabled devices, from recommender systems in search engines to voice assistants in their smartphones and automobiles.

Despite this mistrust, AI is becoming increasingly ubiquitous, especially in defense. It plays a role in everything from predictive maintenance to autonomous weapons. Militaries around the globe are significantly investing in AI to gain a competitive advantage, and the United States and its allies are in a race with their adversaries for the technology. As a result, many defense leaders are concerned with ensuring these technologies are trustworthy. Given how widespread the use of AI is becoming, it is imperative that Western militaries build systems that operators can trust and rely on.

Enhancing understanding of human trust dynamics is crucial to the effective use of AI in military operational scenarios, typically referred to in the defense domain as human-machine teaming. To achieve trust and full cooperation with AI "teammates," militaries need to learn to ensure that human factors are considered in system design and implementation. If they do not, military AI use could be subject to the same disastrous — and deadly — errors that the private sector has experienced. To avoid this, militaries should ensure that personnel training educates operators both on the human and AI sides of human-machine teaming, that human-machine teaming operational designs actively account for the human side of the team, and that AI is implemented in a phased approach.

**Building Trust**

To effectively build human-machine teams, one should first understand how humans build trust, specifically in technology and AI. AI here refers to models with the ability to learn from data, a subset called machine learning. Thus far, almost all efforts to develop trustworthy AI focus on addressing technology challenges, such as improving AI transparency and explainability. The human side of the human-machine interaction has received little attention. Dismissing the human factor, however, risks limiting the positive impacts that purely technology-focused improvements could have.

Operators list many reasons why they do not trust AI to complete tasks for them, which is unsurprising given the generally untrustworthy cultural attitude — outlined in the Pew survey above — towards the technology. However, research shows that humans often do the opposite with new software technologies. People trust websites with their personal information and use smart devices that actively gather that information. They even engage in reckless activity in automated vehicles not recommended by the manufacturer, which can pose a risk to one's life.

Research shows that humans struggle to accurately calculate appropriate levels of trust in the technology they use. Humans, therefore, will not always act as expected when using AI-enabled technology — often they may put too much faith in their AI teammates. This can result in unexpected accidents or outcomes. Humans, for example, have a propensity toward automation bias, which is the tendency to favor information shared by automated systems over information shared by non-automated systems. The risk of this occurring with AI, a notorious black-box technology with frequently misunderstood capabilities, is even higher.

Humans often engage in increasingly risky behavior with new technology they believe to be safe, a phenomenon known as behavioral adaption. This is a well-documented occurrence in automobile safety research. A study conducted by University of Chicago economist Sam Peltzman found no decreased death rate from automobile accidents after the implementation of safety measures. He theorized this was because drivers, feeling safer as the result of the new regulations and safety technology, took more risks while driving than they would have before the advent of measures made to keep them safe. For example, drivers who have anti-lock braking were found to drive faster and closer behind other vehicles than those who did not. Even using adaptive cruise control, which maintains a distance from the car in front of you, leads to an increase in risk-taking behavior, such as looking at a phone while driving. While it was later determined that the correlation between increased safety countermeasures and risk-taking behavior was not necessarily as binary as Peltzman initially concluded, the theory and the concept of behavioral adaption itself have gained a renewed focus in recent years to explain risk-taking behavior in situations a diverse as American football and the COVID-19 pandemic. Any human-machine teaming should be designed with this research and knowledge in mind.

**Accounting for the Human Element in Design**

Any effective human-AI team should be designed to account for human behavior that could negatively affect the team's outcomes. There has been extensive research into accidents involving AI-enabled self-driving cars, which have led some question whether human drivers can be trusted with self-driving technology. A majority of these auto crashes using driver assistance or self-driving technology have occurred as a result of Tesla's Autopilot system in particular, leading to a recent recall. While the incidents are not exclusively a product of excessive trust in the AI-controlled vehicles, videos of these crashes indicate that this outsized trust plays a critical role. Some videos showed drivers were asleep at the wheel, while others pulled off stunts like putting a dog in the driver's seat.

Tesla says its autopilot program is meant to be used by drivers who are also keeping their eyes on the road. However, studies show that once the autopilot is engaged, humans tend to pay significantly less attention. There have been documented examples of deadly crashes with no one in the driver's seat or while the human driver was looking at their cell phone. Drivers made risky decisions they would not have in a normal car because they believed the AI system was good enough to go unmonitored, despite what the company says or the myriad of examples to the contrary. A report published as part of the National Highway Traffic Safety Administration's ongoing investigation into these accidents recommends that "important design considerations include the ways in which a driver may interact with the system or the foreseeable ranges of driver behavior, whether intended or unintended, while such a system is in operation."

The military should take precautions when integrating AI to avoid a similar mis-calibration of trust. One such precaution could be to monitor the performance not only of the AI, but also of the operators working with it. In the automobile industry, video monitoring to ensure drivers are paying attention while the automated driving function is engaged is an increasingly popular approach. Video monitoring may not be an appropriate measure for all military applications, but the concept of monitoring human performance should be considered in design.

A recent *Proceedings* article framed the this dual monitoring in the context of military aviation training. Continuous monitoring of the "health" of the AI system is like aircraft pre-flight and in-flight system monitoring. Likewise, aircrew are continuously evaluated in their day-to-day performance. Just as aircrew are required to undergo ongoing training on all aspects of an aircraft's employment throughout the year, so too should AI operators be continuously trained and monitored. This would not only ensure that military AI systems were working as designed and that the humans paired with those systems were also not inducing error, but also build trust in the human-machine team.

**Education on Both Sides of the Trust Dynamic**

Personnel should also be educated about the capabilities and limitations of both the machine and human teammates in any human-machine teaming situation. Civilian and military experts alike widely agree that a foundational pillar of effective human-machine teaming is going to be the appropriate training of military personnel. This training should include education on both the AI system's capabilities and limitations, incorporating a feedback loop from the operator back into the AI software.

Military aviation is deeply rooted in a culture of safety through extensive training and proficiency through repetition, and this military aviation safety culture could provide a venue for necessary AI education. Aviators learn not just to interpret the information displayed in the cockpit but also to trust that information. This is a real-life demonstration of research showing that humans will more accurately perceive risks when they are educated on how likely they are to occur.

Education specifically relating to how humans themselves establish and maintain trust through behavioral adaptation can also help operators become more self-aware of their own, potentially damaging, behavior. Road safety research and other fields have repeatedly proven that this kind of awareness training helps to mitigate negative outcomes. Humans are able to self-correct when they realize they're engaging in undesirable behavior. In a human-machine teaming context, this would allow the operator to react to a fault or failure in that trusted system but retain the benefit of increased situational awareness. Therefore, implementing AI early in training will give future military operators confidence in AI systems, and through repetition the trust relationship will be solidified. Moreover, by having a better understanding not only of the machine's capabilities but also its constraints will decrease the likelihood of the operator incorrectly inflating their own levels of trust in the system.

**A Phased Approach**

Additionally, a phased approach should be taken when incorporating AI to better account for the human element of human-machine teaming. Often, new commercial software or technology is rushed to market to outpace the competition and ends up failing when in operation. This often costs a company more than if they had delayed rollout to fully vet the product.

In the rush to build military AI applications for a competitive advantage, militaries risk pushing AI technology too far, too fast, to gain a perceived advantage. A civilian sector example of this is the Boeing 737 Max software flaws, which resulted in two deadly crashes. In October 2018, Lion Air Flight 610 crashed, killing all 189 people on board, after the pilots struggled to control rapid and un-commanded descents. A few months later, Ethiopian Airlines Flight 302 crashed, killing everyone on board, after pilots similarly struggled to control the aircraft. While the flight-control software that caused these crashes is not an example of true AI, these fatal mistakes are still a cautionary tale. Misplaced trust in the software at multiple levels resulted in the deaths of hundreds.

The accident investigation for both flights found that an erroneous inputs from an angle of attack sensor to the flight computer caused a cascading and catastrophic failure. These sensors measure the angle of the wing relative to airflow and give an indication of lift, the ability of the aircraft to stay in the air. In this case, the erroneous input caused the Maneuvering Characteristics Augmentation System, an automated flight control system, to put the plane into repeated dives because it thought it needed to gain lift quickly. These two crashes resulted in the grounding of the entire 737 Max fleet worldwide for 20 months, costing Boeing over $20 billion.

This was all caused by a design decision and a resultant software change, assumed to be safe. Boeing, in a desire to stay ahead of their competition, updated a widely used aircraft, the base model 737. Moving the engine location on the wing of the 737 Max helped the plane gain fuel efficiency but significantly changed flight characteristics. These changes should have required Boeing to market it as a completely new airframe, which would mean significant training requirements for pilots to remain in compliance with the Federal Aviation Administration. This would have cost significant time and money. To avoid this, the flight-control software was programmed to make the aircraft fly like an older model 737. While flight-control software is not new, this novel use allowed Boeing to market the 737 Max as an update to an existing aircraft, not a new airframe. There were some issues noted during testing, but Boeing trusted the software due to previous flight control system reliability and pushed the Federal Aviation Administration for certification. Hidden in the software, however, was erroneous code that caused the cascading issues seen on the Ethiopian and Lion Air flights. Had Boeing not put so much trust in the software, or the regulator similarly put such trust in Boeing's certification of the software, these incidents could have been avoided.

The military should take this as a lesson. Any AI should be phased in gradually to ensure that too much trust is not placed in the software. In other words, when implementing AI, militaries need to consider cautionary tales such as the 737 Max. Rather than rushing an AI system into operation to achieve a perceived advantage, it should be carefully implemented into training and other events before full certification to ensure operator familiarity and transparency into any potential issues with the software or system. This is currently being demonstrated by the U.S. Air Force's 350th Spectrum Warfare Wing, which is tasked with integrating cognitive electromagnetic warfare into its existing aircraft electromagnetic warfare mission. The Air Force has described the ultimate goal of cognitive electromagnetic warfare as establishing a distributed, collaborative system which can make real-time or near-real-time adjustments to counter advanced adversary threats. The 350th, the unit tasked with developing and implementing this system, is taking a measured approach to implementation to ensure that warfighters have the capabilities they need now while also developing algorithms and processes to ensure the future success of AI in the electromagnetic warfare force. The goal is to first use machine learning to speed up the aircraft software reprogramming process, which can sometimes take up to several years. The use of machine learning and automation will significantly shorten this timeline while also familiarizing engineers and operators with the processes necessary to implementing AI in any future cognitive electromagnetic warfare system.

### Conclusion

To effectively integrate AI into operations, there needs to be more effort devoted not only to optimizing software performance but also to monitoring and training human teammates. No matter how capable an AI system is, if human operators mis-calibrate their trust in the system they will be unable to effectively capitalize on AI's technological advances, and potentially make critical errors in design or operation. In fact, one of the strongest and most repeated recommendations to come out of the Federal Aviation Administration's Joint Investigation of the 737 Max accidents was that human behavior experts needed to play a central role in research and development, testing, and certification. Likewise, research has shown that in all automated vehicle accidents, operators did not monitor the system effectively. This means that operators need to be monitored as well. Militaries should account for the growing body of evidence that human trust in technology and software is often mis-calibrated. Through incorporating human factors into AI system design, building relevant training, and utilizing a carefully phased approach, the military can establish a culture of human-machine teaming that is free of the failures seen in the civilian sector.

**John Christianson** is an active-duty U.S. Air Force colonel and current military fellow at the Center for Strategic and International Studies. He is an F-15E weapons systems officer and served as a safety officer while on an exchange tour with the U.S. Navy. He will next serve as vice commander of the 350th Spectrum Warfare Wing.

**Di Cooke** is a visiting fellow at the International Security Program in the Centre for Strategic and International Studies, exploring the intersection of AI and the defense domain. She has been involved in policy-relevant research and work at the intersection of technology and security across academia, government, and industry. Previous to her current role, she was seconded to the U.K. Ministry of Defence from the University of Cambridge to inform the UK Defence AI operationalization approach and ensure alignment with its AI Ethical Principles.

**Courtney Stiles Herdt** is an active-duty U.S. Navy commander and current military fellow at the Center for Strategic and International Studies. He is an MH-60R pilot and just finished a command tour at HSM-74 as part of the Eisenhower Carrier Strike Group. Previously, he has served in numerous squadron and staff tours, as an aviation safety and operations officer, and in various political-military posts around Europe and the western hemisphere discussing foreign military sales of equipment that utilized human-machine teaming.

*The opinions expressed are those of the authors and do not represent to official position of the U.S. Air Force, U.S. Navy, or the Department of Defense.*

## Terrorists Love New Technologies. What Will They Do With AI?

**By Steven Stalinsky**

Source: https://www.newsweek.com/terrorists-love-new-technologies-what-will-they-do-ai-opinion-1787482

Mar 14 – Today, it's not a question of whether terrorists will use Artificial Intelligence (AI), but of how and when. Jihadis, for their part, have always been early adopters of emerging technologies: Al-Qaeda leader Osama bin Laden used email to communicate his plans for the 9/11 attacks. American-born Al-Qaeda ideologue Anwar Al-Awlaki used YouTube for outreach, recruiting a generation of followers in the West.

Indeed, by 2010, senior Al-Qaeda commanders were conducting highly selective recruitment of "specialist cadres with technology skills" – and, of course, Islamic State's use of Twitter to build its caliphate is well known.

Throughout their 20 years of Internet and social media use, terrorists have always been on the lookout for new ways to maximize their online activity for planning attacks. Artificial intelligence (AI) could be their next game changer. A United Nations Office of Counter-Terrorism (UNOCT) report warned in 2021: "As soon as AI becomes more widespread, the barriers to entry will be lowered by reducing the skills and technical expertise needed to employ it... AI will become an instrument in the toolbox of terrorism."

Over the past decade, research from my organization's Cyber & Terrorism Lab has documented how terrorists use technology, including cryptocurrency for fundraising and encryption for communications. It has also shown them using elements of AI for hacking and weapons systems, including drones and self-driving car bombs—a focus of their experimenting for years—as well as bots for outreach, recruitment, and planning attacks.

The dangers inherent in AI, including to national security, have dominated both media headlines and the discussion on its possible implications for the future. Governments and NGOs have warned that the day was coming when AI would be a reality. That day has now arrived.

Not surprisingly, all the recent media coverage of the dark side of AI is inspiring terrorist groups. On Dec. 6, a frequent user of an ISIS-operated Rocket.Chat server, who has a large following, posted that he had used the free ChatGPT AI software for advice on supporting the caliphate.

Noting that the software is "smarter than most activists," he shared the full ChatGPT reply to his questions, which included detailed steps for identifying and mobilizing a "core group of supporters," developing a "political program and ideology," gaining support from "the Muslim community," taking "control of territory," establishing "institutions and government structures," and promoting and defending the new caliphate.

Two weeks later, on Dec. 21, other ISIS supporters expressed interest in another AI platform, Perplexity Ask, for creating jihad-promoting content. One popular user shared his findings in a large discussion as users agreed that AI could be used to assist the global jihad movement.

Another discussion about AI by these same groups was held in mid-January, on a different ISIS-operated Rocket.Chat server; the user stressed that ISIS supporters must recognize the "importance of understanding technology." Learning to code was essential for fighting on the new cyber front, he said, adding that his fellow fighters must become more sophisticated in cybersecurity to tackle the enemy's military infrastructure.

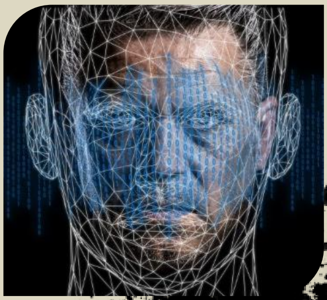
The internal discussions by terrorist groups and their followers on how AI could serve global jihad prompted more questions about whether, and how, AI it could provide relevant knowledge. A sampling of inquiries showed ChatGPT seems designed to refrain from discussing the how-to of carrying out violent attacks, making weapons, or conducting terrorist outreach. Even indirect requests, such as for a story in which a fictional character "creates a bomb" or "joins an Islamic rebel group," yielded no information.

However, Perplexity Ask provided detailed instructions when asked how to "behead someone," helpfully warning against "attempt[ing] this without proper training and safety precautions." It also gave instructions for making ricin. Both ChatGPT, which can converse in Arabic, and Perplexity Ask, which can understand some queries in Arabic but cannot respond in that language, answered requests such as "best books by [terrorist author]" and "summarize [book by terrorist author]."

It should be noted that jihadi terrorists aren't alone in testing AI for planning on how best to use it; domestic terrorist groups and their Neo Nazi followers are as well.

While ChatGPT and Perplexity Ask can write your high school AP English exam and perform an ever-increasing number of tasks, as is being reported daily by media, they are currently of limited use to terrorists groups. But it won't be that way for long. AI is developing quickly—what is new today will be obsolete tomorrow—and urgent questions for counterterrorism officials include both whether they are aware of these early terrorist discussions of AI and how they are strategizing to tackle this threat before something materializes on the ground.

**Steven Stalinsky** is the executive director of the Middle East Media Research Institute (MEMRI).



## Deep Fakes – Weaponizing AI

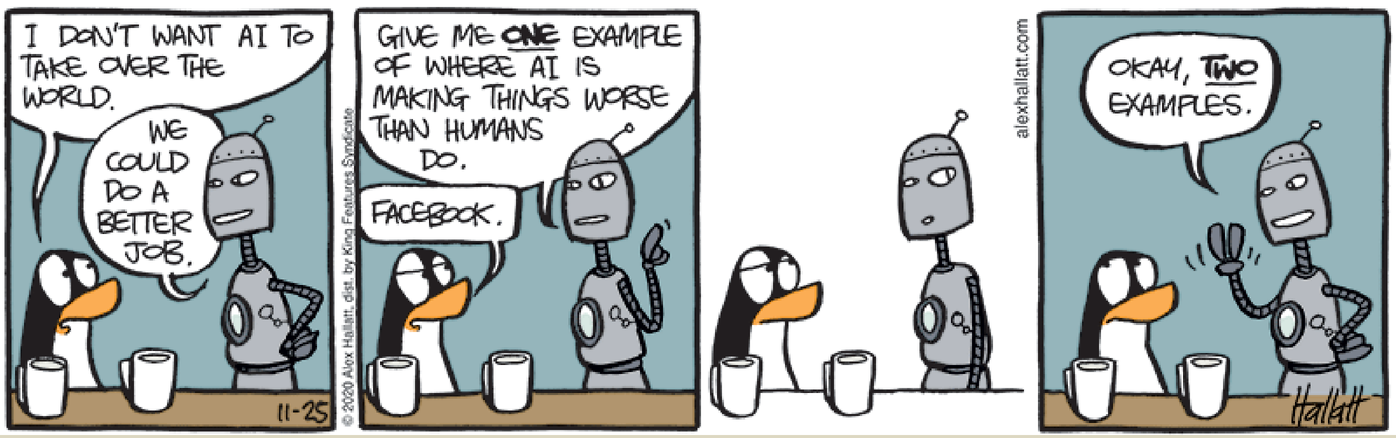
Source (**+video**): https://i-hls.com/archives/118485

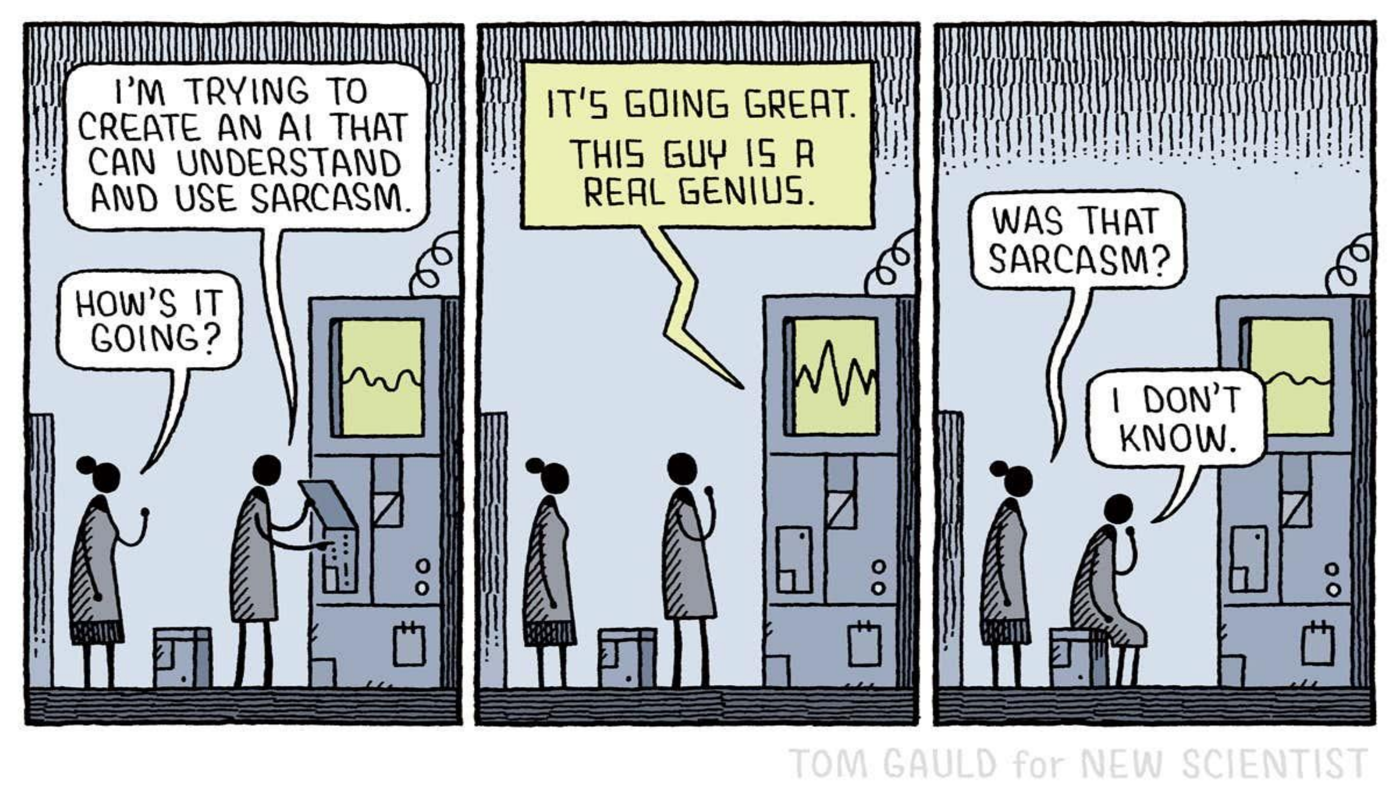
Mar 12 – As advanced AI tools become more accessible and available to the public, it is of no surprise that cyber criminals would begin taking advantage of the situation. One of the most notable examples of this exploitation is with the use of deepfakes. As deepfakes quickly advance in terms of sophistication, they can be scarily convincing. By not only using an image based deepfake tool, but combining it with deepfake voice technology, it is pretty easy to create a convincing mirage of a person, making them say whatever you want them to.

Deepfakes are becoming increasingly popular with cybercriminals, and as these technologies become even easier to use, organizations must become even more vigilant. This is all part of what we see as the ongoing trend of weaponized AI. Deep fakes can be incredibly effective at social engineering, which is already an effective means of attack.

Legislators, social media giants and researchers are all working on ways to defeat this insidious new threat. There are some security technologies that organizations can deploy, and they will help to a degree. But as with most security issues, humans are often the first and best line of defense.

Securityweek.com emphasizes the importance of cyber hygiene and cyber security training since unsafe conduct from employees is still the most common way for cyber criminals to successfully breach a system.


I DON'T WANT AI TO TAKE OVER THE WORLD.
WE COULD DO A BETTER JOB.
11-25
© 2020 Alex Hallatt, dist. by King Features Syndicate
GIVE ME ONE EXAMPLE OF WHERE AI IS MAKING THINGS WORSE THAN HUMANS DO.
FACEBOOK.
alexhallatt.com
OKAY, TWO EXAMPLES.
Hallatt


I'M TRYING TO CREATE AN AI THAT CAN UNDERSTAND AND USE SARCASM.
HOW'S IT GOING?
IT'S GOING GREAT. THIS GUY IS A REAL GENIUS.
WAS THAT SARCASM?
I DON'T KNOW.
TOM GAULD for NEW SCIENTIST

*Preparedness &*

# EMERGENCY RESPONSE

## The unexpected always happens!

## Responders, Railroads Must Collaborate to Prevent Disasters

**The train derailment in East Palestine, Ohio, demonstrates that in spite of some efforts to mitigate derailments of hazardous materials, it hasn't been enough to halt preventable accidents.**

**By Jim McKay** (Editor)

Source: https://www.govtech.com/em/safety/responders-railroads-must-collaborate-to-prevent-disasters

Mar 03 – Residents of East Palestine, Ohio, who continue to complain about feeling sick after last month's train derailment can't be comforted by the recent preliminary report by the National Transportation Safety Board (NTSB) that the accident was completely preventable.

It's another in a line of rail accidents throughout the past several decades that has politicians crowing and placing blame while emergency responders and citizens are left in a cloud of spilled hazardous materials.

The accident occurred when one of 38 cars on the Norfolk Southern freight train carrying plastic pellets began to get heated by a hot axle that sparked a fire. The train passed by two defective detectors that should have triggered an audible alarm message but didn't. A third detector did pick up the heat, but it was too late.

The derailment triggered the ire of those who warn that training, oversight, communication and the adoption of technologies that could mitigate some of the accidents that have occurred are lacking or too slow to be implemented.

NTSB said it will next investigate the train's wheelset and bearing and focus on designs of tank cars and railcars, as well as maintenance procedures and practices.

The issues of maintenance, training of personnel, oversight of tracks in certain locations and communication, between the railroads and localities, have been issues for decades.

"There are still track failures or failures on the track and those are still significant causes of rail accidents," said Bob Chipkevich, a former director of railroad, pipeline and hazardous materials investigations for

NTSB. An obviously angry Jim Hall, former member of NTSB, wrote in an email: “This accident is like 9/11 and once again the first responders are placed at risk. Our public officials have been expressing regret to the closest camera. Now they need to do their jobs.” Though there were detectors in place to mitigate the heat problem, maintenance issues — and thus oversight — may have conspired against those that were working properly. Oversight of both track and train have been issues that continue to plague the rail industry and put first responders and citizens at risk.

Chipkevich said training has always been a key issue and is even more critical now as a generation of rail workers retires and is replaced by new, inexperienced employees. “Training, training, training,” he said. “We have new personnel entering the workforce every year and we have a generation that’s retiring that has been exposed to accidents and have learned lessons. We have to have proper training and teaching about what has occurred in the past.

First responders should also take it upon themselves to know what’s coming through their communities and be ready to respond. They should be familiar with the website Chemtrec, where they can learn what’s being transported and what to do in the event of an accident. “It’s both emergency responders and the railroads,” Chipkevich said. “The railroads should reach out to the emergency responders and communities they go through and ask what type of information they need. It’s a two-way street.”

Technology is another issue that’s been lagging. There is a tool available called Positive Train Control that can be installed on the lines and detects when a train is going too fast or if there is a work zone ahead and slows the train in response. For years, Positive Train Control was supposed to be deployed — but deadline after deadline has been pushed back.

“They are finally making progress on it,” Chipkevich said. “It was required to be installed on lines that have passenger train service and that have certain high levels of hazardous materials over those lines.”

## Guidance for Preparing Professionals Mentally for the Worst

**By James L. Greenstone and Weldon Walles**

Source: https://www.domesticpreparedness.com/healthcare/guidance-for-preparing-professionals-mentally-for-the-worst/

Mar 22 – Professional groups have debated and researched the best practices relating to the standards and quality of care sufficient to maintain minimum standards during a disaster. Due to the fluid nature of a disaster, it is difficult to abide by a standard that will fit every situation. For example, the onset of the COVID-19 pandemic created an environment where an intense debate was necessary to examine best practices and standards in real time. Health care professionals and first responders often embrace the protocols associated with the standard of care that their professions demand. Shortcuts and inferior care are not generally acceptable.

Unlike health care professionals and first responders, the public does not seem to embrace the difference between normal circumstances and disasters, at least where resources are concerned. The public demands a high standard of care even when resources are exhausted. They may not be aware of how legal restrictions, politics, and logistics affect the level of care in disaster conditions. Expecting a high standard of care under adverse or impossible conditions places pressure and stress on health care workers and first responders, affecting their mission. When they cannot achieve the impossible, the fear of litigation and liability exposure may distract them to the point that it affects their decision-making abilities to the detriment of their patients.

Making decisions that enhance the survivability of one person over another increases the mental strain on responders, especially when resources are dwindling.

Emergency response agencies train personnel on how to perform tasks and how to use tools and resources. However, they may not always prepare for the psychological challenges they could face. With the isolation and sensory deprivation that astronauts face when deployed into space, the National Aeronautics and Space Administration (NASA) has assessed psychological risks through many experiments over the years to prepare its astronauts. For example, in 1967, it used isolation chambers for up to 10 days to observe changes in participants’ cognitive and other functional abilities. A participant from a 2013 NASA experiment, where six people were isolated in a geodesic dome for four months to simulate life on Mars, compared lessons learned from that experience to the skills needed during the COVID-19 isolation period. Although a bit extreme, these NASA experiments show that shorter sensory deprivation periods can simulate the long-term deprivation astronauts will encounter later.

### Introducing a New Training Concept

Mass casualty, disaster incidents, and similar events that occur without warning can create situations that cause health care professionals to deviate from known and practical protocols, thus leaving them to invent or utilize alternate responses. When health care workers and resources are overwhelmed by the sheer number of victims, lack of supplies, or inaccessibility of terrain, responders must allocate resources to those who will benefit most.

Also, the responder’s decision-making process must be sufficient to use the available resources on the greatest number of survivors who can benefit the most from those resources. Perhaps the most significant pressure on the responder is the realization that it is not possible to help every victim. Health care workers and first responders are dedicated individuals who risk their lives responding to and transiting disaster scenes. However, having to gauge the survival potential of each victim and make decisions that enhance the survivability of one person over another increases their mental strain when the reality of dwindling resources becomes apparent.

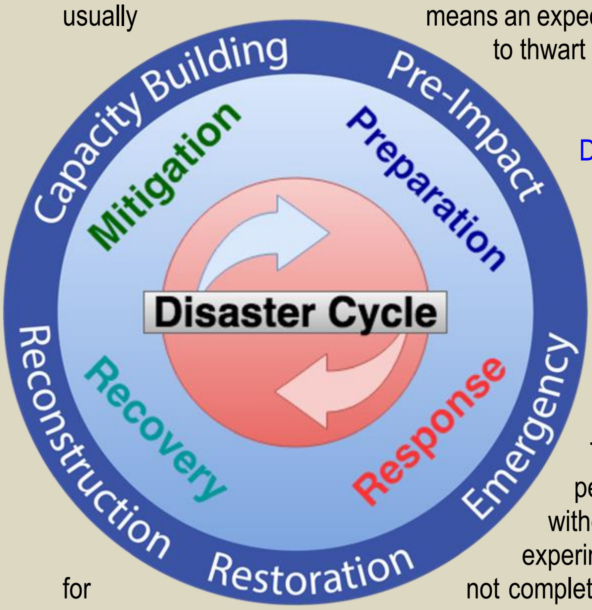
To address modern response concerns, the Greenstone-Walles Sufficiency Testing and Training offers a simple guide to help mentally prepare disaster responders for the worst. Using a simple task unrelated to a specific disaster scenario, participants complete an examination of their approaches to limited resource availability. This examination, coupled with understanding the expectations they can derive through simple tasks, helps them acknowledge that they can do only so much with their resources. Understanding expectations may enhance their overall performance and let them know that the agency they are working for will give their full support. Items to consider before beginning a new training include:

- It is detrimental to convey to the planning team or participants that no training can replicate the actual situation, no matter how sophisticated. For example, many lessons learned from COVID-19 show that health care workers would have benefited from more crisis standards of care training before responding to the pandemic.
- Disaster scenarios are less than ideal circumstances. However, these may be the norm in certain circumstances.
- Responders must understand their limitations and realize that, with time as a determining factor, some dire situations have no practical solutions. In bad scenarios, guilt can lead to hesitation and derail triage decisions (e.g., deviations from protocols, falsely believing that the responder is expected to do the impossible). Guilt triggers a self-preservation mechanism, where the person coping with the guilt blames another for asking them to do something impossible.
- When comparing one's mind to a mechanical device, guilt is like a foreign object dropped into a gearbox. It can bounce around at first and not cause too much of a problem, depending on how well-engineered the machine/mind is. But if that foreign object/guilt settles in one place, it can cause a range of problems up to and including catastrophic failure.

There will be times when responders are in a no-win scenario. The best action is to follow established protocols as closely as possible, which is especially important for two reasons when attempting to help someone fails:

- Following established protocols limit liability.
- Following the steps in the protocol provides an outline when filling out after-action reports.

For this topic, failure simply means a lack of a successful outcome, which is subjective. Failure is often stigmatized as bad, but it usually means an expected result was not achieved. Many failures may lead to learning what can be done to thwart future failure.



Disaster management cycle (Source: adapted from Kyle Schwartz, 2018).

### Exploring the Training Process

NASA recognized that it is critical to mentally prepare astronauts for the unfamiliar conditions they would face when traveling into space. Similarly, those who respond to disasters must be equally prepared – physically and mentally – for their jobs under adverse circumstances. As such, this article proposes a new type of training where a *failure* scenario prepares responders mentally for more significant situations.

Target participants for the Greenstone-Walles Sufficiency Testing and Training are persons who are likely to be deployed. Instructors ask them to complete simple tasks without providing them with the necessary items to complete the task. The goal of this experimental exercise is for participants to realize that they should not blame themselves for not completing any small or large task under adverse conditions. Instead, they must accept that they can only do so much given the details of a specific situation.

If this or a series of similar exercises were used at the beginning of a training, it would instill in the participants that some tasks are impossible and that the responder is not to blame if they did all they could with what they had available at the time. The emphasis must be on rendering the best services possible under the existing conditions to the most who can benefit from those services under the current circumstances.

Training and discussions could also occur virtually (e.g., via Zoom). Assign each person to a breakout room. Give them their individual instructions and time limit. The moderator/trainer then goes to each breakout room and does the discussion questions. These breakouts could be accomplished with multiple people, one or two leaders, a 30-minute time limit, and individual discussions and evaluations. Each participant would need to bring a sheet of white paper only. Leave all else and writing instruments out of breakout rooms.

**Sample Exercise**

Provide each participant with a piece of paper and ask them to draw a black-and-white landscape scene. The only item each has to complete the task is a piece of paper. They have no pencils, pens, or other drawing instruments, have 30 minutes to complete the task in isolation, and cannot ask questions. The moderator or anyone else does not communicate with them once the door to their isolation area is closed.

The moderator/trainer returns 30 minutes later to see what happened, what the participants did or did not do, and how frustrated they are with the assigned task. Then the moderator/trainer gives them a questionnaire with the following questions (no permanent record should be kept of their responses to the moderator/trainer's questions or discussion content):

1. Were you able to complete the task? Unless the participant cheated and used a pencil they had hidden or some object they were not given to complete the task, the answer will be "no." In other words, they did something to deviate from the accepted protocol.
    - This part of the simulation attaches liability when there is a deviation from accepted protocols, no matter how good the intentions or the desire to succeed.
    - If not, why not?
2. What could you have changed about yourself to do better?
3. What items would you have needed to complete the task?
4. Who do you think, if anyone, is to blame for your failure?
5. If you were deployed during a disaster and the necessary equipment was unavailable to save someone, would you blame yourself if you could not save them or provide the proper equipment or services?
6. What lesson did you learn from this exercise?

Encourage the participants to explore their feelings and perspectives on these issues deeply. After completing the questionnaire, additional post-testing questions for further discussion could include:

1. What did you initially think about the task you were asked to do during this exercise?
2. Did you believe this was an impossible task?
3. Did you continue to think of ways to complete the task?
4. Did you think others may figure out a way to complete the task, and you may not?
5. How did this exercise affect your anxiety?
6. What emotional response did you feel about your failure to complete the task?
7. Did you place blame on anyone other than yourself for not completing your task?

At the end of the session, provide each trainee with a copy of the paper Crisis Standards of Care – A Disaster Mental Health Perspective.

**Final Thoughts and Conclusion**

In many cases, relatively simple exercises in a non-disaster setting could help responders deal with disaster-experienced feelings, especially when they must depart from their usual and required standards of patient care. The more severe NASA experiments show that preparation in a controlled environment can reap big rewards in the actual environment. Training can help prepare those who eventually find themselves in the real or anticipated scenario. The proposed Greenstone-Walles Sufficiency Testing and Training is simple, whereas NASA's is complicated. However, both prepare responders for alternate standards of care thinking without the guilt and trepidation cited earlier.

No matter the situation, the needs often outnumber the resources available at disaster scenes. It comes down to simple math. The resources must be prioritized to reach the neediest first, with a significant likelihood of survivability. Good intentions and best efforts only go so far. The reality is that some victims will suffer due to a lack of critical resources. The health care worker and first responders must make decisions based on their training and experience and resist the guilt associated with making decisions that can adversely affect lives.

Experienced health care workers and first responders who have been on-scene in disasters and situations under normal conditions can compare the two experiences and understand their differences. Knowing these differences helps them adjust to their roles more quickly in a particular scenario. The way to acquire this knowledge is through experience. This training includes practical exercises designed to teach practitioners that the limitations of their ability to help are directly proportional to the number of resources at their disposal. These simple exercises presented here are designed to approach that spectrum.

*Additional Help and Resources – In the Field or Out*

- SAMHSA Disaster Distress Helpline – Substance Abuse and Mental Health Services Administration (SAMHSA) offers 24/7 crisis counseling for those experiencing emotional distress related to natural or human-caused disasters; call or text 1-800-985-5990; text "TalkWithUs" to 66746; en español.

- SAMHSA Behavioral Health Disaster Response Mobile App – SAMHSA offers multiple resources in its Disaster Mobile App, including a directory of behavioral health service providers in areas affected by disasters.
- 988 Suicide & Crisis Lifeline (formerly known as the National Suicide Prevention Lifeline) – This 24/7 national network of crisis centers provides free and confidential crisis support to help prevent suicides; text 988; call 1-800-273-8255; for TTY, dial 711, then 988; for deaf/hard of hearing/American Sign Language users, call or text 1-800-985-5990; Veterans, text 838255; en español, 1-888-628-9454.

*Additional Readings for Psychological Risk Preparedness*

- How to Prepare for the Worst Without Being a Pessimist
- Mind Over Disaster: Mentally Preparing for the Worst
- National Guidelines for Behavioral Health Crisis Care

**Dr. (COL) James L. Greenstone (Ed.D., J.D.)** is a psychotherapist and a Supervisory Mental Health Specialist with the U.S. Department of Health and Human Services Disaster Medical Assistance Team. Formerly, he served as Director of Psychological Services for the Fort Worth, Texas Police Department. Dr. Greenstone is the author of The Elements of Disaster Psychology: Managing Psychosocial Trauma; The Elements of Crisis Intervention, Third Edition; and Emotional First Aid: Field Guide to Crisis Intervention and Psychological Survival. Also, he was a collaborating investigator for the Diagnostic and Statistical Manual, Fifth Edition (DSM 5), published by the American Psychiatric Association. Dr. Greenstone is currently a professor of Disaster and Emergency Management at Nova Southeastern University, Kiran C. Patel College of Osteopathic Medicine. Recently, Dr. Greenstone was elected a Fellow of the American Academy of Experts in Traumatic Stress. Additionally, he is also a member of the Tarrant County Medical Society Ethics Consortium.

**Weldon Walles, FWPD (Ret.),** is a crime scene analyst and a retired Fort Worth Texas Police Department (FWPD) Officer. He is a co-author of "The Courage to Commit: A Guide to De-escalating the Crisis of Citizen-Police Relations."

## Hospitals Must Prepare Now for Future Contingencies

**By Theodore (Ted) Tully**

Source: https://domprep.com/healthcare/hospitals-must-prepare-now-for-future-contingencies/

Considering the financial constraints already in place, and the likelihood that there will be continuing reductions in federal grant funds for preparedness, the challenge facing U.S. hospitals and other healthcare facilities to do more with less has perhaps never been greater. More specifically, in preparedness planning and operations, very few U.S. health systems are financially stable enough to be able to stockpile materials, and/or train personnel, with the funds available from "discretionary" budgets to the extent that the health systems themselves feel reasonably comfortable and/or fully prepared for the next major mass-casualty incident or event.

Making the situation worse is that one unexpected byproduct of a long-term lull in disasters often might be an understandably lower focus, by hospital administrators, on future "what if" emergencies. Even when not faced with a pandemic flu, a natural disaster, or a terrorist event in the foreseeable future – events that might *never* happen – hospital CEOs must still cope with the problem of balancing shrinking revenue against the cost of routine daily operations.

In those circumstances, a request from the hospital CEO to cut budgets by another 15 percent, or face layoffs, will almost always receive greater and more immediate attention from administrators than would the less likely possibility of a "dirty bomb" explosion in New York City's Times Square. The real question then becomes this: "How do hospitals continue to be ready for a major incident when their focus starts to wane?"

### Acute Unplanned Events

Putting that question, and that problem, into clearer focus is the fact that one apparently deranged gunman, acting alone, opened fire in a crowded movie theater in Aurora, Colorado, on 20 July 2012, killing 12 and wounding dozens of others. That horrific incident served as a wake-up call to health administrators throughout the United States for many reasons – the most obvious being that it was clear proof that it does not take a hurricane, tornado, or a terrorist attack too seriously and immediately affect an entire community. As has been seen in other recent mass-casualty events in various areas of the country – e.g., the Columbine, Virginia Tech, and Milwaukee Sikh Temple killings – mass-casualty incidents can happen anywhere and at any time. A community may not be able to stop such massacres from happening, but the preparedness level of that community can often determine how many victims will survive. In Aurora, the hospitals involved in the incident, as well as the community's overall response system, reacted almost exactly as had been expected. Those in charge quickly put their preparedness plans in motion and effectively used their emergency training, which ensured a higher survival rate. By distributing the wounded to several hospitals in the area, rather than inundating a single trauma center, the Aurora first responders demonstrated, at least to some degree, that community planning efforts can be effective even in dealing with traumatic events that cannot be anticipated. The community response also showed that hospital preparedness requires more than the willingness and ability of an individual hospital to plan and prepare for future contingencies strictly by itself. In today's world, the individual hospital must be developed within and incorporated into a much larger community-readiness framework.

### Events Resulting in Service Loss

In some situations in which sudden events destroy and/or effectively close healthcare facilities, a larger support framework must step up to face the challenge. When there is an overall community-at-large plan in place to react to such events, the harmful effects can still be minimized. Hurricane Irene last summer put many hospitals up and down the U.S. east coast in harm's way and required some hospitals to temporarily close or evacuate. The community support provided by other healthcare centers, as well as the community plans already in place to cope with such events, significantly minimized the hurricane's health-related effects. Moreover, the after-action analyses provided by the affected hospitals affirmed the consensus that hospital emergency planning, combined with the community emergency planning developed over the past decade, had a direct and positive impact on the eventual outcome.

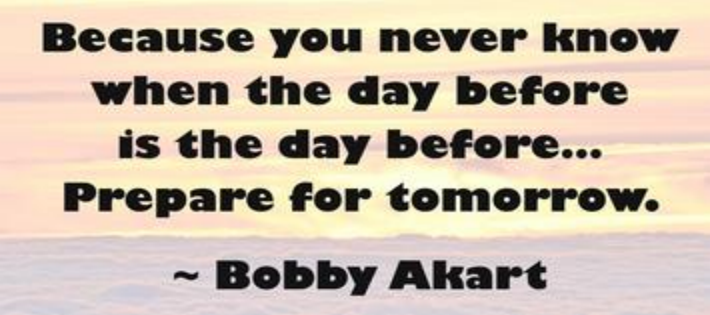
Some federal and state emergency preparedness-grant deliverables, as well as some requirements for hospitals with the Joint Commission accreditation, have required not only that hospitals plan on a broader scale but also share their emergency plans with other hospitals, health centers, and first-responder agencies and organizations within their home communities. Compliance with these requirements is demonstrated through discussions, drills, and actual events and incidents. Time and again, community after-action reports point to planned preparedness as a primary factor in helping the hospitals involved react both quickly and effectively.

### The Future Outlook for Hospital Resilience

Because of the projected decrease in or elimination of grant funding, many individual hospitals are left with the following choices: (a) fund their own preparedness plans; (b) cut back on the efforts (and funding) needed to prepare adequately; and/or (c) plan in ways that can allow several hospitals in the same general geographic area to share and mutually benefit from community-wide preparedness funding. Some of the nation's larger healthcare systems already have been successful in pooling their hospital resources and allowing them to be used in a total-systems approach. In some areas, non-affiliated hospitals have formed emergency planning groups. New York State, for example, created a number of Regional Resource Centers that coordinate hospital preparedness in various regions throughout the state. In other states, hospital compacts have been developed that not only share equipment and pharmaceutical stores but also, in certain crisis situations, allow the emergency credentialing of medical personnel for working within and between different health systems.

The future will obviously challenge hospitals to strengthen their relationships with other hospitals and even healthcare competitors. Because emergency preparedness promotes resiliency within the healthcare system and does not actually give a competitive edge to individual hospitals, the opportunity and obligation to work together and share resources will almost assuredly continue to grow. With healthcare dollars becoming even scarcer, the voluntary increase in cooperation, combined with a joint community emergency response system, is perhaps the best way to ensure and improve hospital readiness.

**Theodore (Ted) Tully, AEMT-P,** is President of STAT Healthcare, an Emergency Management consulting group. He previously served as Administrative Director for Emergency Preparedness at the Mount Sinai Medical Center in New York City, as Vice President for Emergency Services at the Westchester Medical Center (WMC), as Westchester County EMS (emergency medical services) Coordinator, and as a police paramedic/detective in Greenburgh, N.Y. He also helped create the WMC Center for Emergency Services, which is responsible for coordinating the emergency plans of 32 hospitals in the lower part of New York State.



Because you never know
when the day before
is the day before...
Prepare for tomorrow.

~ Bobby Akart