01\24

C2BRNE DIARY

Dedicated to Global First Responders

ICI International CBRNE INSTITUTE

December 2023

PART B

Taliban About to Buy A North Korean Nuclear Weapon

An International CBRNE Institute publication

ICI International CBRNE Institute

CBRNE-Terrorism Newsletter

DIRTY R-NEWS

C2BRNE DIARY

Iran Triples Production of Enriched Uranium

Source: https://www.homelandsecuritynewswire.com/dr20231227-iran-triples-production-of-enriched-uranium

Dec 27 – Iran has tripled its production of uranium enriched to 60 percent, after slowing down of production earlier this year, the International Atomic Energy Agency (IAEA) reported on Tuesday.

Iran has "increased its production of highly enriched uranium, reversing a previous output reduction from mid-2023," Reuters reports, quoting a summary of a confidential report – which the news service had obtained — sent to IAEA member states.

The report notes that Iran is using two facilities — the Pilot Fuel Enrichment Plant (PFEP) in Natanz and at the Fordow Fuel Enrichment Plant (FFEP) – to enrich uranium up to 60 percent. The IAEA says that between mid-June and the end of November, the two enrichment plants produced about three kilograms a month of uranium enriched to 60 percent.

The IAEA report says that "The agency confirms that, since the end of November 2023, the rate at which Iran has been producing uranium enriched up to 60 percent U-235 at these two facilities combined has increased to approximately 9 kg per month."

The IAEA says that its inspectors in Iran first noted changes in production at Fordow on 25 November, and that Iran admitted that the increase in production began three days earlier. The inspectors observed the increase in production at Natanz on 27 November. The IAEA says that its inspector's observations from late November were verified in the past week.

Reuters says that diplomats attribute the enrichment slowdown to secret talks held between the United States and Iran over the release of U.S. citizens held in Iran. **Iran's current stockpile of uranium enriched to 60 percent, if enriched to weapon-grade 90 percent, would be sufficient to build three Hiroshima-size bombs.** The 2015 nuclear deal between Iran and the world powers limited Iran to stockpiling no more than 202.8 kilograms of enriched uranium, and limited the enrichment level to 3.67 percent.

President Donald Trump's 2018 unilateral decision to withdraw the United States from the nuclear deal removed the restrictions the deal imposed on Iran's nuclear-weapons program, thus facilitating a significant expansion and acceleration of that program and dramatically shortening Iran's "breakout" time, that is, the time it would take Iran to produce one nuclear bomb if the decision to do so was taken. Between January 2016, when the nuclear deal went into effect, and May 2018, when Trump announced that the United States was withdrawing from the deal, Iran's breakout time was between 12 and 18 months. As a result of the U.S. withdrawal from the deal, Iran's breakout time is now assessed to be between 10 and 14 days.

In August, the IAEA's quarterly report on Iran estimated the size of Iran's stockpile of uranium enriched to various levels at 3,795.5 kilograms (8,367.7 pounds), down by 949 kilograms from May.

The agency's August quarterly report said Iran had 121.6 kilograms (268 pounds) of uranium enriched to 60 percent. In the agency's May report, it estimated Iran's stockpile of 60 percent enriched uranium at a little over 114 kilograms (250 pounds). The agency's February report estimated the amount of 60 percent enriched uranium in Iran's stockpile at 87.5 kilograms (192 pounds).

The IAEA reported that earlier this year, agency's inspectors detected "particles" of uranium enriched to 83.7 percent at Iran's underground nuclear site in Fordow. The withdrawal of the United States from the nuclear deal has allowed Iran to curtail and obstruct meaningful inspection of its nuclear weapons-related activity. Reuters reports that the IAEA's recent reports also note difficulties inspectors have recently faced in trying to monitor's Iran's nuclear-weapons program:

- Iran was trying to stonewall IAEA officials by denying them visas;
- Iran was also engaging in "de-designation of experienced agency inspectors" in an effort to weaken the agency's monitoring capabilities;
- Since February 2022, the IAEA 1 has been unable to access surveillance footage from declared nuclear sites;
- As of June 2022, the only recorded data the agency was able to obtain originated from cameras at a workshop in the Iranian city of Isfahan.

The nuclear year in review: A renewed interest in nuclear weapons—for and against

By François Diaz-Maurin

Source: https://thebulletin.org/2023/12/the-nuclear-year-in-review-a-renewed-interest-in-nuclear-weapons-for-and-against/

Dec 27 – As we wrap up the year, one event—or rather a non-event—stands out: Russia has not used nuclear weapons in Ukraine. This is not a trivial outcome. One year ago, concerns among experts and officials over this possible scenario was at their highest, with repeated, thinly veiled threats to use them and Russia's new policy to deploy nuclear weapons in Belarus. Prospects were so grim that UN Secretary-

General António Guterres highlighted these nuclear concerns in opening his annual remarks to the United Nations General Assembly in New York.

(Credit: Kelly Michals/National Museum of the US Air Force via Flickr; adapted)

That Russian President Vladimir Putin decided not to use nuclear weapons can be subject to different interpretations. His decision may have been based on moral concerns, fear of international backlash, or fear of uncontrollable escalation. But the decision could well also be the result of a sudden realization that nuclear weapons, practically speaking, have no military value on the battlefield.
Nearly two years into the war, however, the risk of nuclear weapon use in Ukraine cannot been dismissed completely: Russia continues to consider part of Ukraine as its own territory, and Russia's nuclear doctrine states that it may use nuclear weapons to defend its territory. No one can know how the Kremlin would react should Ukraine make any breakthrough in these territories after the winter is over or if Russia's economy of war starts to crack. And one fact is obvious: Both countries consider this war to be existential and have no intention of stopping the fight.
On the frontline, the situation at the six-reactor Zaporizhzhia nuclear power plant—Europe's largest—remained critical. The embattled plant's site continued to endure fire, structural damage, temporary losses of external power, and operator stress. Russia allegedly destroyed the Kakhovka dam, the plant's cooling reservoir and a major source of water for drinking and irrigation, and experts feared for intentional sabotage on the plant itself. Meanwhile, analysts still had difficulty articulating clear protection measures against military attacks on nuclear reactors.
Globally, the world experienced renewed interests in nuclear weapons as countries looked for ways to ensure their security in the context of rising global tensions. Fearing that "Ukraine today may be Asia tomorrow," some leaders in South Korea and Japan pressed the United States to reinforce its extended deterrence to Seoul and Tokyo. Pakistan continues to gradually expand its nuclear arsenal with more warheads, more delivery systems, and a growing fissile material production industry. And experts voiced concerns that nuclear-armed countries continue proliferating their nuclear technologies and materials in the Middle East and beyond. In the United States, a congressional commission has called for adding new nuclear capabilities to counter China's growing nuclear arsenal—a strategy critics consider ineffective and potentially leading to a nuclear arms race.

On the diplomatic front, two major arms control treaties were all but scrapped this year, with Russia suspending its participation in New START (the US-Russian treaty that limits their deployed long-range nuclear forces) and revoking its ratification of the Comprehensive Nuclear-Test Ban Treaty (CTBT).
Despite these setbacks, the nuclear arms control and disarmament community has continued to confront nuclear proliferation and press the United States to engage in concrete nuclear arms control negotiations with China.

Here are six *Bulletin* nuclear stories that marked 2023—and that you should read.

The US and Russia must re-assess their strategic relations in a world without New START
By Steven Pifer
Despite Russia's treaty suspension and US countermeasures, strategic arms control can still have a bright future if both sides act now, argues Steven Pifer, a former US negotiator. In this piece, Marshall Brown, a former legal advisor to the US New START delegation, also details the impact of US countermeasures to Russia's treaty violations.

The US and China re-engage on arms control. What may come next
By Daryl G. Kimball
In this piece, the executive director of the Arms Control Association, explains how China's growing nuclear capabilities imply more responsibilities and details strategies for a successful bilateral nuclear arms control dialogue with the United States.

Why the congressional strategic posture report is not about nuclear deterrence, but warfighting
By Tara Drozdenko
The recent report by the Congressional Commission on the Strategic Posture of the United States encourages a new arms race and a nuclear buildup, Tara Drozdenko, the director for the Global Security Program at the Union of Concerned Scientists, writes. The commission paints a bleak picture of the near-term international security environment, but its recommendation to expand the US nuclear arsenal would make a bad situation worse, Drozdenko argues.

Why North Korea may use nuclear weapons first, and why current US policy toward Pyongyang is unsustainable
By Robert E. Kelly
Because it will face an intense "use-it-or-lose-it" dilemma, North Korea will likely employ nuclear weapons early if war erupts on the Korean peninsula, argues Robert Kelly, a professor of political science at Pusan National University in South Korea. At the time of attack, the allies should respond with non-nuclear arms as long as politically feasible. And ahead of any attack, the United States should deconcentrate its northeast Asian footprint, to reduce North Korean opportunities to engage in nuclear blackmail, Kelly argues.

The narrow field of options for safely managing Ukraine's Zaporizhzhia Nuclear Power Plant
By Mark Hibbs
Russian and Ukrainian officials making decisions about the Zaporizhzhia Nuclear Power Plant are challenged by a complex safety and security profile, explains Mark Hibbs, a nuclear expert and senior associate in Carnegie's Nuclear Policy Program. No single reactor-management option will address all hazards as long as the war continues, Hibbs argues.

Nuclear expert Mycle Schneider on the COP28 pledge to triple nuclear energy production: 'Trumpism enters energy policy'
By François Diaz-Maurin
In an interview with the *Bulletin*, nuclear expert Mycle Schneider reviews the status and trends of the world nuclear industry and explains why it's impossible to triple nuclear energy capacity by 2050, as countries pledged at a recent climate conference. "This pledge is completely, utterly unrealistic," Schneider says.

François Diaz-Maurin is the associate editor for nuclear affairs at the *Bulletin of the Atomic Scientists*. Previously, Diaz-Maurin was a MacArthur Foundation Nuclear Security Visiting Scholar at the Center for International Security and Cooperation (CISAC), Stanford University, and a European Commission's Marie Sklodowska-Curie Fellow. He has been a scientific advisor to members of the European Parliament on nuclear issues, and he is a founding member of the Emerging Leaders in Environmental and Energy Policy network (ELEEP) of the Atlantic Council, Washington D.C. and the Ecologic Institute, Berlin. Prior to joining academia, Diaz-Maurin spent four years as a research engineer in the nuclear industry in Paris, France and Boston, MA. There, he worked on the safety design of new reactors and of a treatment plant to vitrify Hanford's tank waste from WWII and Cold War nuclear weapons production. Diaz-Maurin received multi-disciplinary training in civil engineering (B.Sc./M.Sc., University of

Rennes 1, 2004/2007, both with distinction), environmental and sustainability sciences (Ph.D., Universitat Autònoma de Barcelona, 2013, summa cum laude and “Extraordinary Ph.D.” Award), and nuclear materials, geochemistry of radionuclides and nuclear security (postdoctoral training, Stanford University, 2017–2019).

Thriving Otters in North America Linked to Nuclear Weapons Tests. Here's Why.

Source: https://www.sciencealert.com/thriving-otters-in-north-america-linked-to-nuclear-weapons-tests-heres-why

Dec 29 – When a large earthquake shook Alaska's Aleutian Islands in 2014, scientists with the US government hurried to assess the damage on Amchitka Island. They were looking for leaking radiation from underground nuclear tests performed decades before.

During the first half of the 20th century, the remote island had been a wildlife preserve, until the US government converted it into a nuclear test site.

Three atomic weapons went off at Amchitka in the late 1960s and early 1970s, including the largest underground detonation the US has ever set off.

No humans lived on the island, but the biggest blast, in 1971, killed at least 900 sea otters. The Atomic Energy Commission, the government agency in charge of nuclear research, had predicted at most 240 otters would die.

If ecologists and others hadn't pushed to relocate some otters before the detonation, it probably would have been much worse.

"There was pressure from the state of Alaska as well as environmental groups," conservation biologist and author, Joe Roman told Business Insider. "They ended up moving hundreds of otters."

Roman wrote about the otter relocation in his new book "Eat, Poop, Die: How Animals Make Our World."

Why were otters recolated?

By the time the AEC was looking at Amchitka in the 1960s, the island's sea otter population was one of only a handful that had survived the sea mammals' near extinction a century earlier.

Their luscious pelts were prized as "soft gold." In the 1700s and 1800s, hunters killed about one million sea otters to sell their fur.

The drop in population was alarming, from between 150,000 to 300,000 in the early 1700s to around 2,000 just 200 years later. Russia, Japan, Britain, and the US signed a fur treaty to help protect the animals in 1911. Over the next several decades, sea otter numbers rose to around 30,000.

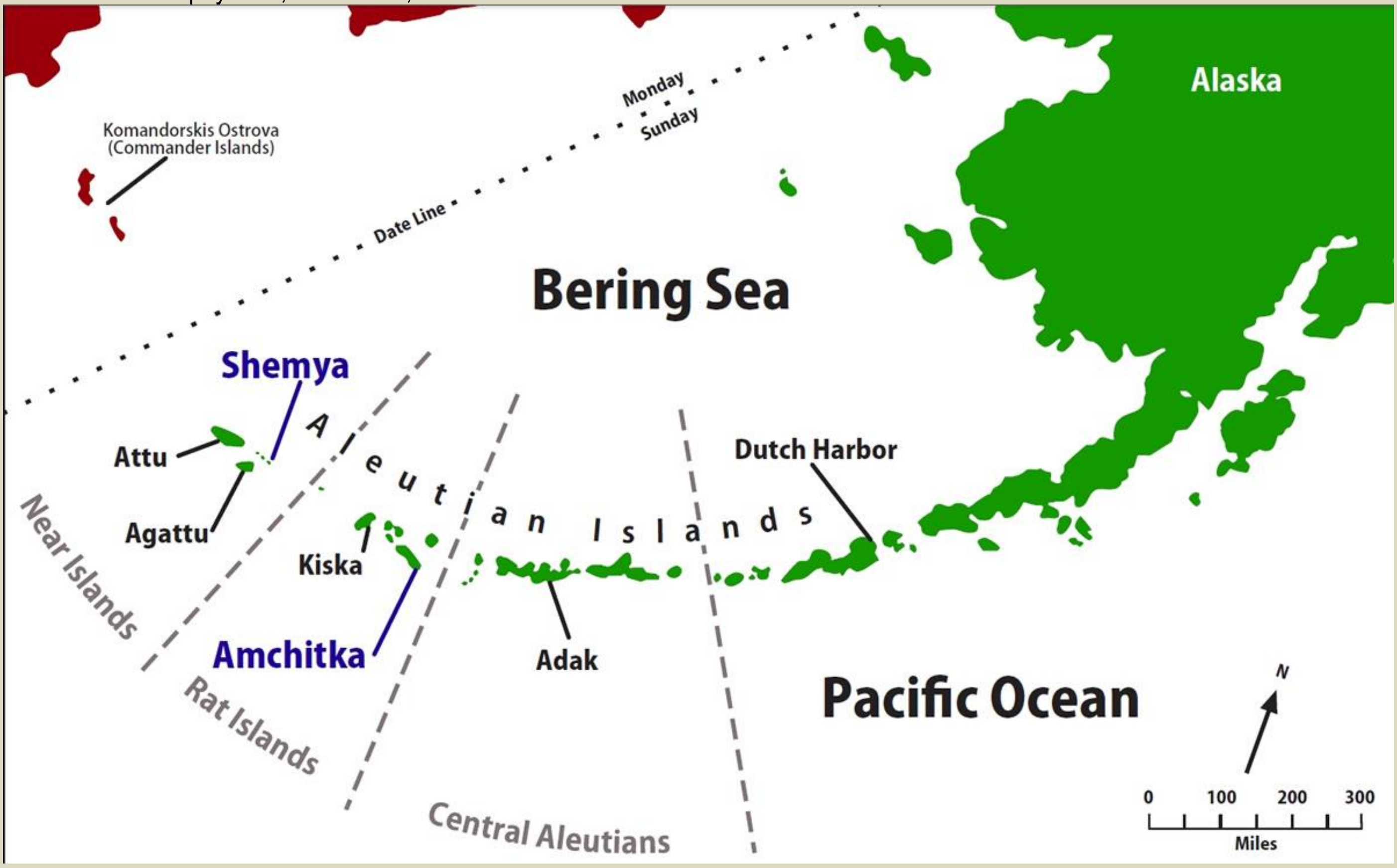
By 1959, the charismatic animals were starring in a nature film, "The Sea Otters of Amchitka." No one wanted to see those adorable otters decimated by an underground explosion, John Vania, an otter specialist with the Alaska Department of Fish and Game, told the AEC.

A confluence of occurrences made many Americans more environmentally conscious in the 1960s, from Ohio's Cuyahoga River continually catching fire to Rachel Carson's exploration of the dangers of pesticides in her book "Silent Spring" to the largest oil spill in US waters at the time, near Santa Barbara, California.

Protestors didn't want a third nuclear test at Amchitka at all. In fact, the conservation group Greenpeace formed out of an organization trying to stop the test.

A US Fish and Wildlife Service biologist, Karl Kenyon, had already worked on relocating some otters to areas they'd lived before the 18th century hunting. The detonations at Amchitka were a good reason to move even more, ecologists and biologists thought.

If the AEC would pay for it, Vania said, the scientists could relocate the otters.



The return of the kelp forests

In addition to funding the relocation, the AEC supplied the scientists with a plane that could hold over 50 otters. Over the next few years, the scientists captured more than 700 otters in nets and carted them to southeast Alaska, Washington, Oregon, and British Columbia.

Over the next 50 years, the sea otter populations in many of these locations, like Sitka, Alaska, would go from several dozen to hundreds or thousands. "All the sea otters — of which there are thousands — in Sitka now are the descendants of these airlifted sea otters," Roman said.

Eighty-nine otters went to British Columbia. Now there are over 7,000. An estimated 125,000 sea otters live in the Pacific Ocean as of 2015. The otters' presence soon changed the landscapes where they live today. Their relocation allowed biologist Jim Estes to study islands with and without otters. As a result, he realized there was a link between otters, sea urchins, and kelp forests.

"In the absence of sea otters, you have a lot of sea urchins," Roman said. "When you have a lot of urchins, they create what's called urchin barrens." The sea urchins eat the kelp holdfasts, which anchor the algae. Roman compares it to sawing down a forest. The kelp eventually disappear.

One of the otters' favorite foods is sea urchin. And they can eat a lot of them. "They have very high metabolisms," Roman said. "They're eating machines." When the sea urchin numbers drop, the kelp return.

In Sitka Sound, the sea otters reduced the sea urchin population by 99%. Kelp forests exploded in return.

"The forests provide food and shelter for more than 800 species, including sea lions, harbor seals, lingcod, gobies, moray eels, octopuses, crabs, sea anemones, and brittle stars," Roman wrote.

The kelp forests are also amazing at capturing carbon, a concern for the warming planet.

The otters can also affect land animals, Roman wrote, either directly, as food for wolves on Alaska's Pleasant Island, or indirectly, with the kelp forests that attracted birds that prey on fish.

Competing with otters

Roman called the sea otter relocation one of the "most successful cases" of its kind. However, he said, "you don't really release animals in that way these days."

For one thing, the US didn't consult indigenous and First Nations people before unleashing the otters. The mammals brought back the kelp forests, but they destroyed a reliable source of food for many people.

"Sea otters don't just eat urchins," Roman said. "They also eat geoducks and other valuable benthic invertebrates in the area." That includes crabs and clams. "And of course that brings them into conflict with fishers in that area," he said.

Suddenly, otters appeared where they hadn't been for generations. "So no one remembers having sea otters in that area," Roman said. "They're used to harvesting these invertebrates, and they're quite abundant in the absence of a predator."

Their voracious appetite is one reason some people call otters the "rats of the sea." For some Alaskans and Canadians, they're seen as a nuisance.

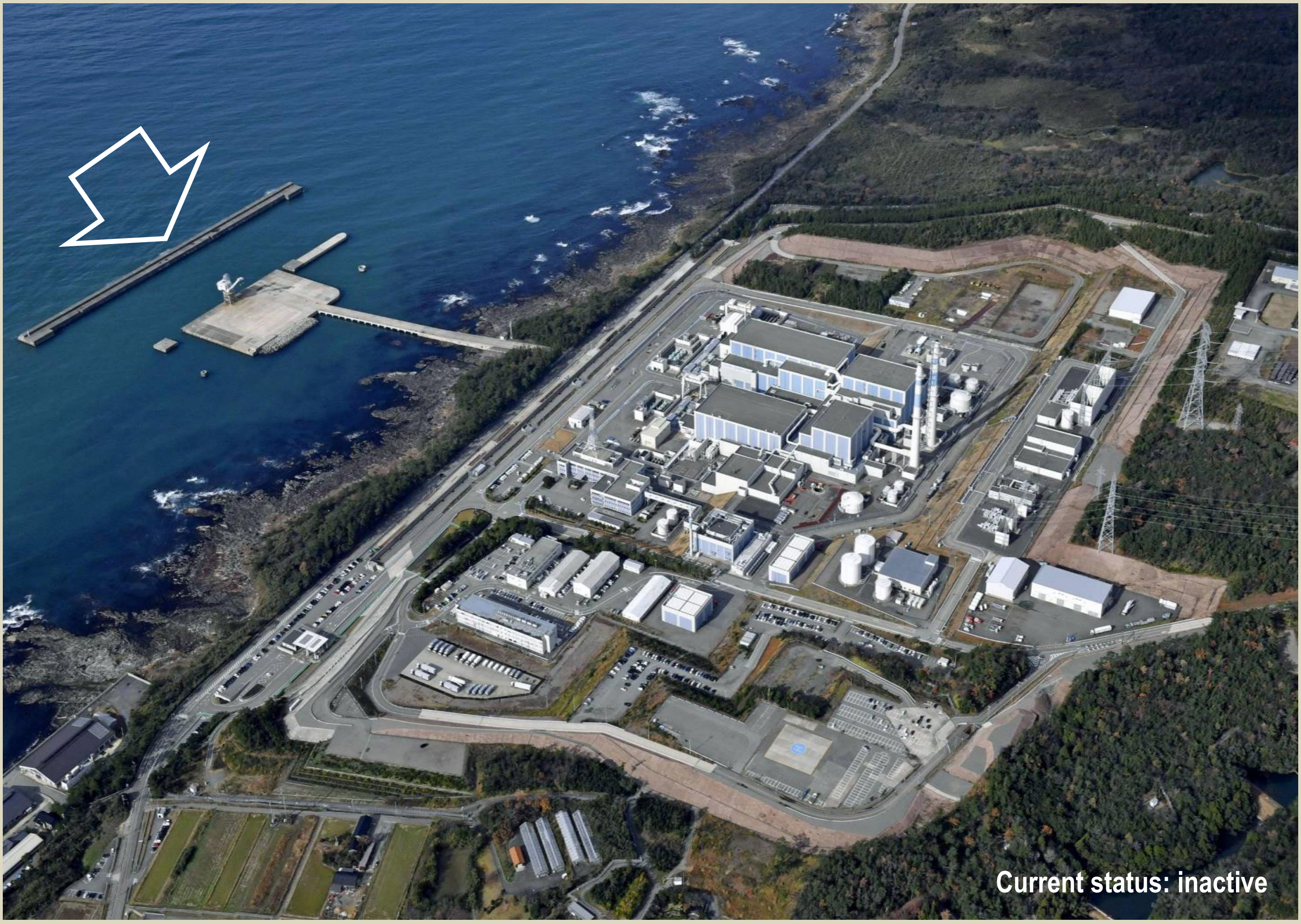
When otters arrived in new regions of Alaska, Washington, and Oregon in the '60s and '70s, it was still legal to hunt them. The Marine Mammal Protection Act of 1973, changed that, though Alaska Natives can still hunt otters, whales, and seals.

"I spoke to Mike Miller, who's a native Sitkan," Roman said. "He promotes this idea of some balance" between the human population and the otters. It's an idea echoed by researchers, too. "We are wondering if there is a sweet spot where you can have it all," ecologist Kristy Kroeker told the BBC.

While sea otter numbers are far greater than they were 100 years ago, the animals are still endangered. They also face challenges due to the climate crisis. And not all the relocated populations survived. They disappeared from Oregon after about a decade.

But sea otters' success elsewhere — especially their impact on kelp forests — has made Oregon want to try reintroducing them again, just with more caution and the input of coastal tribes this time.

7.6-magnitude earthquake in Japan



Hokuriku Electric Power's nuclear plant in Shika, Ishikawa Prefecture | KYODO

EDITOR'S COMMENT: We never learn from previous disasters (Fukushima). Will this sea wall counter a 5m tsunami (arrow)? In Wikipedia I read the following but using Google Earth the numbers mentioned do not seem to be compatible.

Construction of an anti-tsunami-wall
On Wednesday 5 October 2011 a start was made with the construction of a reinforced concrete wall, that should shield the reactors against a possible tsunami. The wall was designed 4 meters high and 700 meters long, 11 meters above sea level. This was done to comply with extra governmental instructions ordered after the Fukushima Daiichi nuclear disaster. Next to this a new drainage gate was to be installed to minimize damage to plant facilities in case seawater would be able to climb over the wall and would submerge the plant. Other emergency safety measures included the installing of an extra pump to cool the reactors with seawater and an extra power source to operate a valve for venting steam out of reactors. Construction should be completed by the end of **March 2013**.

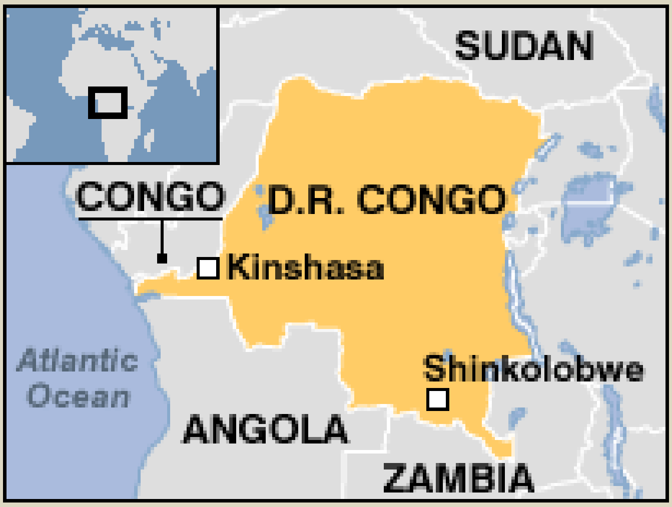
Uranium Security in the DRC

By Daniel Allen
Source: https://nonproliferation.org/uranium-security-in-the-drc/

Jan 02 – The Shinkolobwe mine is located in the southeastern province of Haut-Katanga in the Democratic Republic of Congo. It was a former uranium mine used by the Americans to procure fissile material for the Manhattan Project, with 2/3 of the fissile material i n the Manhattan Project originating from Shinkolobwe. Before the Manhattan Project, the Germans had attempted to use an intercepted shipment of uranium for their (failed) nuclear program. Eventually, the Americans abandoned the mine during the 1960s when domestic uranium production made imports unnecessary; the Belgian company Union Minière subsequently sealed the mine with concrete.

Even though the mine had been sealed following the DRC's independence in 1960, artisanal mining continued throughout the region due to abundant alternative ores including cobalt, silver, and copper. Lack of access to materials, coupled with few means for alternative sources of income, meant that the mining at Shinkolobwe occurred under increasingly hazardous conditions. In 2004, an old section of the mining shaft collapsed killing eight people and injuring a further thirteen. Even though the Shinkolobwe had officially been closed off by presidential decree some months earlier, illegal mining continued in the area.

In 2006, a DRC sanctions committee report found that the "smuggling of radioactive materials […] are far more frequent than previously assumed." These included the confiscation of over 50 containers containing uranium or cesium in or around Kinshasa, as well as the securement of 100 kilograms of uranium ore. While international organizations such as Interpol have attempted closer collaboration with Tanzanian and Congolese authorities, government officials have been reluctant to provide more information. A French documentary in 2017 on the illegal shipments of uranium from the Congo through Tanzania also alleged that government officials had been conspiring with artisanal miners in the smuggling of uranium from Shinkolobwe. Their investigation further highlighted the near-inexistent security infrastructure surrounding the mine, raising doubts about how inactive Shinkolobwe truly was. While these claims have yet to be substantiated by third parties, they ultimately raise more questions than answers.



Most recently, the current governor of Haut-Katanga Jacques Kyabula implemented a project aimed at improving the security of the Shinkolobwe mine in 2019. These included a double-trench perimeter, as well as checkpoints in the larger area. The governor heralded this project by announcing that once it was complete, "no one may say that uranium is mined at Shinkolobwe". Unfortunately, this claim is most likely false. In fact, open-source intelligence techniques paint an alarming picture.

●▶ Continue reading the full paper

Daniel Allen is a fourth-year student at Middlebury College, pursuing two bachelor's degrees in Political Science and Anthropology, respectively. His work has focused primarily on arms control using open-source intelligence techniques with a focus on North Korea and Iran. Having grown up abroad, Allen wishes to use his international perspective and trilingual fluency to help bridge the gap between local and international nonproliferation efforts. The research for this article was conducted during his time at CNS in 2023 as a Summer Undergraduate Fellow.

Doomsday: What could drive Israel and Iran to start launching nuclear weapons?

By Louis Beres

Source: https://thehill.com/opinion/international/4385217-what-could-drive-israel-and-iran-to-start-launching-the-nukes/

Jan 04 – Although Israel's Gaza war is most visibly being waged against Hamas, the ultimate adversary is Iran. If Israel's counter-terrorism efforts should sometime bring it into direct confrontation with Iran, the result could be an immediate escalation between these two adversary states.

In such a plausible scenario, even a still-pre-nuclear Iran could elicit a "limited" Israeli nuclear reprisal. The principal escalation dangers would be an Iranian use of radiation dispersal weapons or an Iranian rocket attack on Israel's Dimona nuclear reactor.

For Israel, a country smaller than Lake Michigan, nuclear weapons and strategy remain essential to national survival. Israel's traditional policy of deliberate nuclear ambiguity, or "the bomb in the basement," goes back to its early days. During the 1950s, Prime Minister David Ben-Gurion understood the need for a dramatic "equalizer" against larger and more populous regional enemies.

Today, facing a recalcitrant and soon-to-be nuclear Iran, Israel needs to update and refine its policy of deliberate nuclear ambiguity. The key objective of such needed changes would be credible nuclear deterrence, a goal that will now require selective nuclear disclosure. Though ironic and counter-intuitive, Iran will need to be convinced that Israel's nuclear arms are not too destructive for actual use.

There will be perplexing nuances. For Israel to fashion reason-based nuclear policies, Iran should be considered rational. But it is conceivable that Iran might act irrationally, perhaps even in alliance with other states (such as Syria or North Korea) or kindred terror groups (such as Hamas, Hezbollah, Palestinian Islamic Jihad or the Houthis).

Unless Jerusalem were to consider Pakistan an authentic enemy, Israel presently has no already-nuclear enemies. Still, as an unstable Islamic state, Pakistan is potentially subject to a coup d'état by assorted Jihadist elements and is closely aligned with Saudi Arabia. The Sunni Saudi kingdom could sometime decide to "go nuclear" itself because of Shiite Iran's steadily accelerating nuclear progress.

For Israel's nuclear deterrence to work longer-term, Iran will need to be told more rather than less about Israel's nuclear targeting doctrine and the invulnerability of Israel's nuclear forces. In concert with such changes, Jerusalem will need to clarify its still-opaque "Samson Option." The point would not be to "die with the Philistines" (per the biblical Book of Judges), but to enhance "high destruction" options of its nuclear deterrence posture.

Though the only gainful purpose of Israel's nuclear weapons should be deterrence at different levels of military destructiveness, there will remain circumstances under which Israeli nuclear deterrence could fail. How might such intolerable circumstances arise? **Four distinct scenarios emerge, with results that range from very destructive to catastrophic.**

First, if Iran were to launch "only" a massive conventional attack on Israel, Jerusalem could respond with a limited nuclear retaliation. If Iranian first-strikes were to involve chemical or biological weapons, Israel might also decide to launch a measured nuclear reprisal. This decision would depend, in large part, on Jerusalem's expectations concerning follow-on Iranian attacks and its calculations of comparative damage-limitation. A nuclear retaliation by Israel could be ruled out conclusively only in circumstances where the Iranian aggression is entirely conventional and "hard-target" oriented — that is, oriented toward Israeli weapons and military infrastructures, not toward Israel's civilian populations.

A **second** scenario would involve Israel feeling compelled to preempt Iranian aggression with conventional weapons. In that case, that enemy state's response would largely determine Israel's next moves. If this response were in any way nuclear, including "mere" radiological weapons, Israel would likely turn to certain controlled forms of nuclear counterretaliation. If Iran's retaliation were to involve other non-nuclear weapons of mass destruction, Israel could still feel pressed to take the escalatory initiative. This decision would depend upon Jerusalem's considered judgment of enemy intent and on its corollary calculations of damage-limitation.

If the Iranian response to Israel's preemption were limited to hard-target conventional strikes, it is unlikely that Israel's decision-makers would go nuclear. If, however, the Iranian conventional retaliation was "all-out" and directed in part toward Israeli civilian populations, an Israeli nuclear counterretaliation could not be excluded. Such a counterretaliation could be ruled out only if Iran's conventional retaliation were proportionate to Israel's preemption; confined to Israeli military targets; circumscribed by legal limits of "proportionality" and "military necessity," and accompanied by verifiable assurances of non-escalatory intent.

A **third** (and highly unlikely) scenario involves Israel launching a preemptive nuclear strike against Iran. Although circumstances could arise wherein such a strike would be rational and permissible under international law, it is improbable that Israel would allow itself to reach such end-of-the-line circumstances. An Israeli nuclear preemption could reasonably be expected only if Iran had already acquired nuclear or other weapons of mass destruction, threatened to use them, began a countdown to launch, and Jerusalem believed that exclusively conventional preemption could not save the Jewish State from destruction.

A **fourth** scenario would be that of nuclear war fighting. This could occur if an Iranian nuclear first-strike or retaliation for an Israeli conventional first strike failed to destroy Israel's second-strike nuclear capability, or vice versa.

For the time being, of course, any Iranian nuclear capacity would be limited to radiation dispersal weapons.

Louis René Beres is professor emeritus of International Law at Purdue University and author of "*Surviving Amid Chaos: Israel's Nuclear Strategy*" (2018).

Are The Taliban About to Buy A North Korean Nuclear Weapon?

By Sam Faddis

Source: https://andmagazine.substack.com/p/are-the-taliban-about-to-buy-a-north

Jan 06 – We reported recently on information coming out of Afghanistan suggesting the very real possibility that **the Taliban and Al-Qaeda were working on a plan to acquire a functioning Pakistani nuclear weapon**. That information came from multiple news sources, and we were able via contacts to verify the reporting independently. That was bad enough, but there is now new reporting suggesting that a Taliban delegation may have traveled to North Korea for discussions about buying a nuclear weapon from that rogue nation.

According to reporting an eight-man Taliban delegation recently made a secret visit to North Korea to discuss cooperation on nuclear weapons technology. Allegedly, several Western intelligence agencies are aware of the contact and are attempting to acquire additional information. One of the individuals reported to have traveled to North Korea is Maulvi Abdul Rasheed Munib, the security chief of Kandahar and head of foreign relations for Afghan Taliban intelligence.

There is nothing fantastic or unbelievable about this reporting. North Korea relies upon illegal weapons sales worldwide to raise much-needed hard currency. The North Koreans make more than $100 billion a year from missile sales alone, and they will deal with anyone. At one point or another, they have sold weapons in violation of international sanctions to Egypt, Syria, Iran, Pakistan, and Libya among others. They are currently pumping munitions including ballistic missiles to Russia, and as we have reported, are rumored to have been given a top-level Russian ICBM capable of hitting the United States in return.

As part of this worldwide enterprise, the North Koreans operate a vast smuggling network. They employ "ghost ships." They carry out black flights. They operate front companies and employ foreign middlemen. We are nowhere close to being able to monitor everything they are moving or where it is going.

There is nothing rudimentary or haphazard about North Korean smuggling operations. They are highly refined and carefully calibrated to escape detection. When oil is smuggled into North Korea for instance – in violation of sanctions – ships often meet at sea under the cover of darkness and move the oil from one vessel to another to throw intelligence and law enforcement agencies off the track. The North Koreans do

not just sell weapons, however. They partner with other dangerous regimes and work with them over time to enhance their capabilities. They have been working with the Iranians since 1979, and a great deal of the progress the Iranians have made in expanding their missile capabilities has been due to North Korean assistance.

"Iran has developed a close working relationship with North Korea on many ballistic missile programs," providing Iran "a qualitative increase in [ballistic missile] capabilities" and advancing Iran toward its "goal of self-sufficiency in the production of medium-range ballistic missiles."

There are no limits apparently on to whom the North Koreans will sell or with whom they will deal. The rogue nations of the planet are in fact the chief clientele of Pyongyang.

"North Korea's history of exporting ballistic missile technology to several countries, including Iran and Syria, and its assistance during Syria's construction of a nuclear reactor— destroyed in 2007—illustrate its willingness to proliferate dangerous technologies."

The international community has long recognized that North Korea would continue to deal with its cash flow problems by expanding the scope of its sales of dangerous technologies. It has also been obvious to experts that the likely "growth market" for the North Koreans would be the Middle East.

"The most likely outgrowth of North Korea's need for cash is an increase in other dangerous behavior. WMD technology represents one of North Korea's few value-added assets."

Let's be clear. If you think somebody is on top of all this, carefully monitoring it and preparing plans to prevent the Taliban and their allies from getting nuclear weapons, you are living in dreamland. **Afghanistan is a terrorist superstate and a denied area in terms of intelligence collection. We have gone blind there, and the policy of this administration is to ignore the issue and hope the American people are too busy trying to figure out how to pay the rent and buy gas under "Bidenomics" to notice**.

Every jihadist group worth its salt has set up shop in Afghanistan under the protection of the Taliban. Al-Qaeda is so tied into the Taliban that many of its senior officials are holding formal positions in the Taliban government. The Pakistani Taliban are waging war on Islamabad and the threat there is so grave the Pakistanis are begging Washington for help.

Against this backdrop the idea that the Taliban are asking the North Koreans to arm them is not only not bizarre it is perfectly reasonable. Are the Taliban about to buy a North Korean nuclear weapon? It is entirely possible.

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

Why a nuclear weapons ban would threaten, not save, humanity

By Zachary Kallenborn

Source: https://thebulletin.org/2024/01/why-a-nuclear-weapons-ban-would-threaten-not-save-humanity/

Jan 10 – On January 22, 2021, the Treaty on the Prohibition of Nuclear Weapons entered into force with 69 state parties. The treaty aims to ban nuclear weapons, bringing global nuclear weapons arsenals down to zero. Treaty states, the International Campaign to Abolish Nuclear Weapons, and other global zero activists that pushed for the treaty frequently highlight the existential harms from nuclear weapons, including in the second meeting of state parties to the treaty. The concern is legitimate. A 2022 study in *Nature* estimated a nuclear war between the United States and Russia would blast massive amounts of soot into the atmosphere, disrupting the global climate, and causing massive food shortages that could kill over five billion people.

But nuclear weapons are not the only threat to humanity. An asteroid over 1 kilometer in diameter striking the Earth, genetically engineered biological weapons, super volcanoes, extreme climate change, nanotechnology, and artificial superintelligence all could generate existential harm, whether defined as the collapse of human civilization or literal human extinction. To address those challenges, humanity needs global cooperation to align policies, pool resources, maintain globally critical supply chains, build useful technologies, and prevent the development of harmful technologies. Nuclear deterrence—alongside robust international organizations, laws, norms, alliances, and economic dependencies—helps make that happen.

Global governments and organizations aiming to reduce existential risks should support nuclear risk-reduction measures but oppose quick, complete abolition of nuclear weapons. Nuclear abolition creates serious risk of returning to an era of great power conflict, which could drastically increase existential risk. A global war between China, Russia, the United States and their respective allies risks the survival of the global cooperative system necessary to combat other existential threats, while threatening infrastructure necessary for risk mitigation measures and accelerating other existential risk scenarios. As Iskander Rehman wrote in his recent in-depth study of great power war: "Protracted great power wars are immensely destructive, whole-of-society affairs, the effects of which typically extend well beyond their point of origin, spilling across multiple regions and siphoning huge amounts of personnel, materiel and resources… Ultimately, protracted great-power wars usually only end when an adversary faces total annihilation, or collapses under the weight of its own exhaustion." If the great powers collapse, the global system may collapse with them. Nuclear deterrence can help prevent that.

An RS-24 Yars intercontinental ballistic missile on display at the Victory Day Parade in May 2023 in Moscow. Source: President of the Russian Federation.

Nuclear weapons place a cap on how bad great power conflict can become and may deter the emergence and escalation of great power war. If China, the United States, or Russia faced a genuine existential threat, the nuclear weapons would emerge, threatening nuclear retaliation. As Chinese General Fu Quanyou, head of the People Liberation's Army General Staff until 2002, once said: "The U.S. and Soviet superpowers both had strong nuclear capabilities able to destroy one another a number of times, so they did not dare to clash with each other directly, war capabilities above a certain point change into war-limiting capabilities." Mutually assured destruction also helps prevent serious great power conflict from breaking out in the first place. During the current war between Ukraine and Russia, Russian President Vladimir Putin has used nuclear threats to deter direct NATO involvement and keep the conflict local. The United States might wish to support Ukraine against Russia, but it's not willing to risk a Russian nuclear strike on New York City or Washington, DC to do more than provide money and material. Removing that deterrence by banning nuclear weapons means a potential return to protracted, global great power war.

To emphasize: Opposing quick, complete abolition does not mean opposing reduction of nuclear arsenals or risk reduction measures like improved crisis management and ensuring human control over nuclear weapons. Massive nuclear war is the most likely scenario for existential harm to humanity in the near term. As the Chinese nuclear arsenal grows, and China potentially aims for nuclear parity with the United States in the coming decades, that problem is going to get worse. Current nuclear weapon strategies depend on targeting adversary nuclear weapons, which means as an adversary builds more nuclear weapons, the United States must build more too. If the United States builds more, so too will Russia and China. Unchecked, nuclear arsenal sizes could quickly spiral upwards, passing the heights of the Cold War when the United States had 23,000 nuclear weapons and the Soviet Union had 39,000.

The risks of great power war

War among great powers increases existential risk in at least four ways. First, the global cooperative system necessary to combat existential threats may be seriously damaged or destroyed. Second, combatants might target and destroy infrastructure and capacity necessary to implement existential risk mitigation measures. Third, military necessity may accelerate the development of technologies like artificial intelligence that create new existential risks. Fourth, a great power war following nuclear abolition could touch off rapid, unstable nuclear rearmament and proliferation. After World War II, the United Nations, NATO, the International Monetary Fund, the International Atomic Energy Agency, and numerous other international organizations were built to stabilize the world and prevent such a global catastrophe from happening again. That cooperative framework allowed for the United Nations Intergovernmental Panel on Climate Change, enabled global partnerships on biosecurity through the G-7, and facilitated high-level discussions on the risks of artificial intelligence. However, a massive global war would undermine the very foundations of this order, because it would show the economic, political, and institutional ties between nations were never enough to prevent global conflict. Plus, World War III might result in the crippling or destruction of the powerful states and institutions that hold up global governance: China, France, Russia, the United States, the United Kingdom, the European Union, NATO, and others. The global community may lose the cooperative institutions necessary for climate change reduction, limiting or controlling risky biological research, prevent the creation and proliferation of artificial superintelligence, and generally defend the planet. Great power war could accelerate a broad range of technologies that generate new and increase other existential risks. Russian President Putin noted in 2017 that, "[w]hoever becomes the leader in [artificial intelligence] will become the ruler of the world." A great power war would almost certainly accelerate research, development, and implementation of artificial intelligence. One can easily imagine a Manhattan Project for artificial superintelligence, bringing together NATO's leading artificial intelligence researchers and organizations to create a superintelligence (or close enough to it) to defend friendly cybernetworks and attack adversarial ones, manipulate adversary decision-making, or create and manage insurgent forces. Although quantum computing is not an existential risk, accelerating development to help break adversary encryption or other military purposes would exacerbate artificial intelligence-related risks, too. Quantum computing offers potentially millions of times more computing power than classical computers, and computing power is a critical resource necessary to train artificial intelligence models. Great power war might also spur massive investment in biotechnologies like genetic engineering to enhance soldier effectiveness. Improvements and proliferation in genetic engineering generate a range of biological warfare concerns from creating new biological warfare agents to making existing agents more harmful.

In a war for survival, infrastructure necessary to mitigate existential risks might be destroyed. Space launch capabilities constitute a prime example: On November 24, 2021, NASA launched the Double Asteroid Redirection Test from Vandenburg Space Force Base near Santa Barbara, California. If China and the United States were at war, Vandenburg Space Force Base would be a viable and desirable target for Chinese attacks. China has long recognized that the United States military depends heavily on space assets for communication, remote sensing, and position, navigation, and timing. And Vandenburg is home to the Combined Space Operations Center, the Space Force center responsible for executing "operational command and control of space forces to achieve theater and global objectives." Damaging or destroying the base, including its space launch capabilities, could help China win the war. At the same time, damaging or destroying the base would make it harder for the United States to carry out asteroid deflection research and, depending on timing, prevent the United States from launching a planetary defense mission when an asteroid is inbound.

General loss of state capacity could also draw resources and policy attention away from existential risk mitigation. Research by, Greg Koblentz of George Mason University and King's College London researcher Filippa Lentzos mapped 69 Biosafety Level 4 laboratories around the world. At these labs, research is conducted on the most dangerous pathogenic material, like the microorganisms that cause smallpox and Ebola. The United States and global community expends significant resources to secure those facilities: President Biden's Fiscal Year 2023 budget provides $1.8 billion to strengthen biosecurity and biosafety. But in a World War III involving the United States and China, biosecurity may fall by the wayside. Even if the United States prevails, rebuilding Tokyo, Los Angelos, Seoul, or other major cities demolished during the fighting would command tremendous resources, and attention. Finally, a World War III breaking out after nuclear abolition could trigger rapid, unstable nuclear rearmament and proliferation. The United States, Russia, China, and other nuclear powers would almost certainly realize that nuclear abolition was a mistake and rearm themselves. A post-abolition World War III would also likely demonstrate to many other states that nuclear weapons are necessary to defend their sovereignty. Rapid nuclear rearmament and proliferation could be highly destabilizing, with significant new risks of nuclear war, because new nuclear arsenals may not be accompanied by the necessary crisis communication, secure second-strike, and general deterrence doctrine necessary to ensure stability. Even if nuclear abolition were achieved, the basic knowledge underlying nuclear weapons would not disappear. Even if all nuclear warheads were dismantled, weapon designs were destroyed, and enrichment facilities closed, the historical and scientific knowledge of nuclear energy and nuclear weapons would not disappear. Nuclear weapons knowledge would need to be retained even in a global zero world to support any monitoring or verification programs aimed at ensuring that a nuclear global zero stays "zero." That knowledge could provide the seeds for rearmament. So, while nuclear abolition might reduce nuclear-related existential risks in the short-term, abolition might counterintuitively increase nuclear existential risk in the long-term.

Navigating the zone of uncertainty

Effectively managing the existential benefits and risks of nuclear weapons requires two questions to be addressed. First, how many nuclear weapons are minimally necessary to deter great power conflict?

Second: At what point does a nuclear war go from just a moral horror and catastrophic loss of life to truly existential harm? Unfortunately, neither answer is clear and requires significantly more modeling and analysis than has been done.

Reducing nuclear arsenals only to the minimum amount necessary to deter great power war requires a nuclear state having sufficient, survivable nuclear weapons to reliably inflict unacceptable harm on an adversary. But how much harm is "unacceptable" will depend on the conflict context, leader personality, domestic and international politics, and other factors. Plus, nuclear forces might be destroyed in an initial nuclear strike; adversary air, missile, and submarine defenses might defeat delivery systems; and nuclear weapons might simply fail to cause expected harm. Finding that right balance will no doubt be hard and change over time, especially with nuclear-relevant emerging and evolving military technologies, but modeling and simulation, red teaming, war games, and similar exercises can all help. Global international organizations, alliances, and complex economic and social interdependence between great powers can also help to ensure nuclear weapons are not the only guarantor of great power peace.

The modeling of global cooling from nuclear war—often called nuclear winter—has been ongoing since Carl Sagan and team raised the concern in October 1983. The results of researchers vary drastically. When looking at the same regional nuclear war scenario, one group of researchers concluded the environmental harms could be globally catastrophic, while the other concluded the climate impact would be minimal. Assumptions regarding how much soot a nuclear war generates, how much soot reaches the upper atmosphere, how food consumption changes, effects on global trade, and the degree to which livestock feed is diverted to human use all affect estimated harm, sometimes drastically.

Unfortunately, political biases and agendas have often colored those assumptions. Fortunately, the National Academies of Sciences, Engineering, and Medicine launched an independent study on potential environmental effects of nuclear war to assess the environmental effects and social consequences of nuclear war, including potential nuclear winter scenarios. The committee's work continues, but the findings should merit significant attention. More generally, the global community should also invest financial, scientific, and computing resources to better assess the climate effects of nuclear detonations, connecting it with ongoing work on modeling climate change. Nuclear war would be a global problem that deserves global attention to understand and mitigate the effects. The United States and global governments can also take action to reduce the risk of nuclear war causing existential harm by strengthening food security. Because the existential harm of a nuclear war that caused nuclear winter would come primarily through massive starvation, the global community can work together to build new and enhance existing long-term food reserves. In addition, the United States and others should think through and develop post-catastrophe plans for a broad range of extreme events, including nuclear war. For example, the United States could develop plans to use the military for emergency food supply, as in the Berlin airlift, when American and British aircraft delivered 2.3 million pounds of food, and other supplies to West Berlin. The United States and global community should also invest in research and development towards synthetic and resilient food sources like methane single cell proteins. These activities would not just be useful for life after nuclear war, but also enhance food security in the near term and be useful for a broad range of ecological and social disasters.

Of course, the best way to reduce the risks of nuclear war is to ensure it never happens in the first place.

The survival of humanity needs to be a global priority, because humanity's survival transcends every social, economic, and political issue. What importance is war in the Ukraine, Taiwanese sovereignty, global poverty reduction, or Icelandic fishing rights, when all of mankind is in danger? For better or worse, ensuring human survival means keeping nuclear weapons for their deterrent effects, accompanied by diligent efforts to ensure that they are never used.

Zachary Kallenborn is an adjunct fellow (non-resident) with the Center for Strategic and International Studies (CSIS), policy fellow at the Schar School of Policy and Government, fellow at the National Institute for Deterrence Studies, Research Affiliate with the Unconventional Weapons and Technology Division of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), an officially proclaimed U.S. Army "mad scientist," and national security consultant. He has published more than 60 articles in a wide range of peer-reviewed, wonky, and popular outlets, including the Brookings Institution, *Foreign Policy*, Slate, DefenseOne, War on the Rocks, the Modern Institute at West Point, Terrorism and Political Violence, and Parameters. Journalists have written about and shared that research in *The New York Times*, the AP, NPR, *The Economist*, *Forbes*, *Popular Mechanics*, Politico, Al Jazeera, The Independent, Blick, *Newsweek, New Scientist*, *MIT Tech Review*, *WIRED*, and the BBC, among others in dozens of languages.

Security Officers at Nuclear Facilities

Source: https://www.homelandsecuritynewswire.com/dr20240112-security-officers-at-nuclear-facilities

Jan 12 – Nuclear plants are sensitive facilities which require strict security measures to ensure the safety of both the plant and the surrounding areas. One of the essential components of this security system is the presence of security officers. These officers play an important role in safeguarding the nuclear plant from potential threats and maintaining a secure environment. **There are nearly 9,000 security officers protecting U.S. nuclear plants.**

The primary responsibility of security officers at nuclear plants is to prevent unauthorized access to the facility. They are trained to monitor and control the entry and exit points, ensuring that only authorized personnel are allowed inside. This includes conducting thorough security checks, such as verifying identification, searching vehicles, and screening individuals for any prohibited items.

In addition to access control, security officers are also responsible for monitoring the premises through surveillance systems. They keep a close eye on the activities within the plant, looking out for any suspicious behavior or potential security breaches. This constant vigilance helps to detect and prevent any threats before they escalate.

Moreover, security officers at nuclear plants are trained in emergency response procedures. They are prepared to handle various situations, such as fires, accidents, or intrusions. They undergo rigorous training to develop the necessary skills and knowledge to respond swiftly and effectively during emergencies, ensuring the safety of the plant and its personnel.

In order to become a security officer at a nuclear plant, individuals must undergo specialized training and obtain the required certifications. This training covers a wide range of topics, including nuclear plant operations, security protocols, emergency response procedures, and the handling of hazardous materials. It is crucial for security guards to have a thorough understanding of these subjects to effectively carry out their duties and ensure the utmost security.

In recent years, there has been a growing trend of unions organizing security officers at nuclear plants to advocate for their rights, improve working conditions, and enhance job security.

Presently the United Federation LEOS-PBA represents many Nuclear Security Officers working at nuclear facilities around the country.

LEOS-PBA notes that it plays an important role in representing the interests of security officers and providing a collective voice for them in negotiations with their employers. By organizing security officers, unions can help address various issues that may arise in the workplace, such as fair wages, benefits, working hours, and safety protocols. Unions also work towards ensuring that security officers have a say in decision-making processes that affect their work and well-being.

Unions also provide support and representation in case of workplace disputes or grievances. Security guards may face challenges, such as unfair treatment, discrimination, or inadequate training. Unions can offer guidance, legal assistance, and representation to security guards, ensuring that their rights are protected and their concerns are addressed.

How Quickly Could Iran Make Nuclear Weapons Today?

By David Albright

Source: https://www.homelandsecuritynewswire.com/dr20240112-how-quickly-could-iran-make-nuclear-weapons-today

Jan 12 – Iran's growing nuclear weapons capability is often condemned, most recently in a December 28th joint statement by the United States and its close European allies.[1] The occasion was the Iranian action to expand its output of 60 percent enriched uranium. This level of enrichment is a hair's breadth from 90 percent enriched or weapon-grade uranium, the enrichment level most desired for making nuclear weapons. That is also the enrichment level used in Iran's nuclear weapons designs, which it nearly perfected during its crash nuclear weapons program in the early 2000s, codenamed the Amad Plan. This program was shut down in 2003 and replaced with a smaller, more dispersed nuclear weapons effort, with the decision to make them postponed.[2]

The unfortunate reality is that Iran already knows how to build nuclear weapons, although there are some unfinished tasks related to the actual construction of them. If the regime's leadership decided to build them, how would it proceed? How long would it take?

The long pole in the tent of building nuclear weapons is essentially complete. Iran can quickly make enough weapon-grade uranium for many nuclear weapons, something it could not do in 2003. Today, it would need only about a week to produce enough for its first nuclear weapon.[3] It could have enough weapon-grade uranium for six weapons in one month, and after five months of producing weapon-grade uranium, it could have enough for twelve.

The other major poles in the tent are "nuclear weaponization" and delivery. Iran has a variety of delivery systems, including nuclear-capable missiles: the delivery pole is ready.

Weaponization is the pole that needs more work. It involves theoretical calculations and simulations; development, testing, and construction of the other components of the nuclear weapon; the conversion of weapon-grade uranium into metallic components; the integration of all the components into a nuclear weapon; and the preparation for mounting the weapons on aircraft or missiles or for use in a full-scale underground test. This pole includes the mastery of the high explosive triggering system, the molding and machining of high explosives, and the building of a neutron initiator that starts the chain reaction at just the right moment to create a nuclear explosion.

Iran has multiple pathways to complete its weaponization requirements and build nuclear weapons. The two most prominent pathways are (1) launching an accelerated effort to achieve a few crude nuclear weapons or reconstituting, or (2) completing its earlier Amad nuclear weapons program with the ability to serially produce annually many warheads suitable for delivery by ballistic missiles.

The second path has some notable challenges. It would require Iran maintaining secrecy for an extended period, a few years by most assessments, while rebuilding a range of production-scale facilities able to serially produce warheads for ballistic missiles. This presents a risk for Iran since early discovery could result in a harsh international reaction and plenty of time for Israel, the United States, and its allies to organize a united reaction.

The accelerated program can be accomplished in a matter of six months and would involve activities conducted in far smaller, more disguisable facilities. This path is a more assured way for Iran to establish itself as a nuclear weapons power while leaving little time for the international community to react. It is also the path followed by other programs such as Pakistan's successful effort in the early 1980s and Iraq's in 1990, the latter thwarted by war. After his invasion of Kuwait in 1990, Saddam Hussein ordered a crash, accelerated nuclear weapons program. This program, far less advanced than Iran's, was advancing steadily until the allied bombing campaign in January 1991 ended it, incidentally without the United States and its allies knowing it had done so.

An Iranian accelerated program would not aim to produce warheads for ballistic missiles, a task that could take significantly longer than six months. Nonetheless, a crude nuclear weapon would signal Iran's entry into the nuclear weapons club as the tenth member, either dramatically via an underground nuclear test or stealthily via leaks about its accomplishment. A missile-deliverable warhead would probably be the next goal of Iran's nuclear weapons program. The outside world would be left to ponder how soon it could reach this capability.

While most of the weaponization work has been accomplished for a crude nuclear weapon, such as the high explosive triggering package, an acceptable neutron initiator, and high explosives components, a few significant tasks likely remain.[4] One important step could be a "cold test," a final demonstration test of the complete nuclear device with the weapon-grade uranium in the core replaced by a surrogate material. Iran was preparing to conduct such a test at the end of the Amad Plan in 2003 but may not have conducted it subsequently. Iran may also want to do more development work of its neutron initiator. However, these tasks could be completed in a matter of several months. Much of the work on weaponization could be conducted in utmost secrecy and would use existing or repurposed military facilities or hidden equipment and materials, possibly located underground.

Iran could also immediately start preparatory work on transforming the weapon-grade uranium into nuclear weapon components in anticipation of later receiving weapon-grade uranium. It accomplished a considerable amount of such work during the Amad Plan, and subsequently at civilian nuclear facilities at Esfahan during the last several years as part of Iran's buildup of its nuclear program, including the production of a small amount of 20 percent enriched uranium metal, a material that can stand in for weapon-grade uranium.

Western intelligence agencies may not detect the start of Iran's nuclear weaponization effort. Given all the complexities and conflicts in the Middle East today, Western intelligence agencies, including Israel's, are stretched to the limit. The beginning stages of a quiet, low-level effort to build nuclear weapons could slip through unobserved.

What that means is that Iran may have a six-month timeline, but the United States and its allies may have to react to a much shorter one. Because Iran has achieved very short breakout timelines to produce weapon-grade uranium, it could wait until month four of the six-month timeline to divert its enriched uranium from International Atomic Energy Agency (IAEA) safeguards, a step likely to be detected by inspectors, although Iran may delay the diversion's detection by a few weeks by denying inspectors access to the safeguarded sites storing the enriched uranium and containing the centrifuges to be used to take the enriched uranium up to weapon-grade, falsely declaring a fire, an accident, or a security incident. The result is that instead of a six-month warning, Western intelligence agencies may have less than two months to respond.

Given short warning times and few prospects of a nuclear deal, the United States and its allies have little choice other than focusing on a strategy to deter Iran from deciding to build nuclear weapons in the first place. Iran needs to be made fully aware via concrete demonstrations that building nuclear weapons will trigger quick, drastic actions by the international community, including military strikes. U.S. military cooperation with Israel aimed at destroying Iran's nuclear capabilities should be bolstered, ensuring Israel can decisively strike Iran's nuclear sites on short notice if there are signs that Iran is moving to build nuclear weapons, including the ability of delivering a second strike if Iran reconstitutes those activities. The priority should be assisting and building military capabilities with our allies and regional partners in the Middle East, with a U.S. commitment to prevent Iran from acquiring nuclear weapons and deter Iran from retaliation.

Complementing this strategy is bolstering the IAEA in its efforts to ensure that Iran addresses the inspectors' finding that Iran has undeclared nuclear material and activities in violation of its comprehensive safeguards agreement, a key part of the Nuclear Non-Proliferation Treaty. Beyond stonewalling, Iran has no defense against the IAEA's charges. The IAEA should continue pressing Iran to address its evidence that its nuclear program is not peaceful, publicly raising its alarm, sending a strong signal that Iran's violations are unacceptable, and further isolating Iran internationally.

Accelerating action at the IAEA will also help ensure that the Iran nuclear issue does not slip off the front pages as other pressing security matters dominate. After all, Iran's possession of a nuclear weapon will enormously complicate most of those other issues. The United States and its allies know how to deter Iran from building nuclear weapons. That effort should accelerate and sharpen as the hope of a revived nuclear deal evaporates and the threat of Iran building nuclear weapons increases.

References

1. https://www.state.gov/joint-statement-on-the-latest-iranian-nuclear-steps-reported-by-the-iaea/s. ↩
2. David Albright with Sarah Burkhard and the Good ISIS Team, Iran's Perilous Pursuit of Nuclear Weapons (Washington, D.C.: Institute for Science and International Security Press, 2021). ↩
3. David Albright, Sarah Burkhard, Spencer Faragasso, and Andrea Stricker, "Analysis of IAEA Iran Verification and Monitoring Report — November 2023," *Institute for Science and International Security,* November 20, 2023, https://isis-online.org/isis-reports/detail/analysis-of-iaea-iran-verification-and-monitoring-report-november-2023/8. ↩
4. *Iran's Perilous Pursuit of Nuclear Weapons.* ↩

David Albright is President and Founder of the Institute for Science and International Security.

Israel's nuclear arsenal: what we know

By Dr Kate Hudson
Source: https://cnduk.org/israels-nuclear-arsenal-what-we-know/

Campaign for Nuclear Disarmament

Jan 14 – Last week's attack on Yemen by US, UK and other forces is a dangerous escalation of the war in the Middle East. The attack is intended to halt the Houthi support for the people of Gaza that has taken the form of attacks on Israel-bound shipping. But as the Houthis have made clear, the attacks will not end their support for the Palestinians. The only way to stop this unfolding and escalating conflict in the Middle East, is to stop the war on Gaza: to implement an immediate and permanent ceasefire, and to ensure freedom and sovereignty for Palestine, as enshrined in UN resolutions and international law.

The alternative to this course of action is the further spread of war, to Yemen, Lebanon, and even to Iran. This is the most dangerous time for more than two decades in the Middle East and it clearly raises the spectre of nuclear weapons use. Because not only is Israel heavily armed with the most up to date conventional weaponry, it is also heavily armed with nuclear weapons. Its nuclear arsenal, which it refuses to formally acknowledge – its policy of 'nuclear ambiguity' – comes under no international controls or inspections. Yet it has an enormous killing capacity – and Israel is the only nuclear weapons state in the Middle East. Recent rhetoric from a number of Israeli politicians suggests a willingness to use their nuclear weapons; if the conflict were to extend to Iran, who can say that Israel would not use its nuclear weapons on non-nuclear Iran?

So what does the Israeli nuclear arsenal look like? Israel's lack of transparency means that figures are uncertain, but **the Stockholm International Peace Research Institute (SIPRI) outlines estimates between 90 and 300 nuclear weapons.** SIPRI also reports that since 2021, according to commercial satellite imagery, there has been significant construction taking place at the Negev Nuclear Research Centre near Dimona, in southern Israel. Some may remember that the great Israeli nuclear whistle-blower, Mordechai Vanunu, worked as a technician at Dimona, before revealing details of the secret Israeli nuclear programme to the British press in 1986. The purpose of the recent works isn't known.

SIPRI information indicates that Israel has air, land and sea-based delivery systems for its nuclear arsenal. Bombs can be dropped from planes, either the F-161 or the F-15 aircraft, and are likely to be stored near air force bases such as Tel Nof airbase in central Israel, or Hatzerim airbase in the Negev desert. Reportedly, when Israel sent six F-16s from Tel Nof to Britain for an exercise in 2019, a US official referred to this as Israel's 'nuclear squadron'.

Israel's nuclear weapons can also be launched on land-based Jericho ballistic missiles. The site of these missiles is thought to be the Sdot Micha Airbase near Zekharia, about 25 kilometres west of Jerusalem. And Israel also operates five German-built Dolphin-class diesel-electric submarines which operate from the port of Haifa on the Mediterranean coast. Some or all of these subs may have been equipped to launch a nuclear-armed cruise missile.

By any estimate, this is a formidable array of weapons of mass destruction and it gives Israel the capacity to inflict catastrophic damage on its neighbours. Of course the impact on Israel of any regional use would be considerable too but there is absolutely no guarantee that would deter an Israeli government from nuclear use if it considered its existence was under threat. How such a threat would be defined is also unknown. The fact remains that nuclear-weapons possession allows Israel to act with impunity, in Gaza, and in the wider region. And that possession is also impacting on how others are willing to relate to Israel.

The questions posed in a recent issue of New Left Review, are highly relevant:

"Is the US, blackmailed by the threat of a Middle Eastern Armageddon, now forced to allow Israel to pursue 'victory' at any price? Does Israel's capacity for nuclear war bestow on the Israeli radical right a sense of invincibility, as well as a confidence that they can dictate the terms of peace with or without the Americans, and certainly without the Palestinians?"

And what can be done about this? Both the US and UK helped Israel to develop its nuclear weapons, against all international law. In 2005, it was revealed from Whitehall documents discovered at the Public Records Office, by BBC Newsnight investigators, that **Britain had secretly supplied the 20 tons of heavy water to Israel nearly half a century before, which enabled it to make nuclear weapons**. Britain has known for decades about the Israeli nuclear arsenal, clearly supporting and condoning it, whilst taking an outraged and aggressive approach to the possibility of nuclear proliferation by other countries. The double standards and hypocrisy displayed by successive British governments is deplorable and is absolutely to be condemned.

Britain has supported numerous resolutions from the UN General Assembly and Security Council, calling for a nuclear weapons free Middle East, without owning up to its role in Israeli nuclear proliferation. Israeli nuclear weapons pose a particular risk to peace and security in the Middle East region and internationally; not surprisingly they are seen as a significant threat by neighbouring non-nuclear states, and the ongoing catastrophe in Gaza and the extending war is exactly the situation in which they are likely to be used. There can be few clearer examples of how nuclear weapons are actually weapons of terror and weapons of impunity, as well as being weapons of mass slaughter and destruction. The war on Gaza must end; it must end with a ceasefire, and with peace and justice for the Palestinians. And it must end, to stop the unthinkable risk of a nuclear war in the Middle East.

Kate Hudson has been General Secretary of CND since September 2010. Prior to this she served as the organisation's Chair from 2003. She is a leading anti-nuclear and anti-war campaigner nationally and internationally.

EDITOR'S COMMENT: Disarmament: It is useless for the *sheep* to pass resolutions in favor of vegetarianism, while the *wolf* remains of a different opinion.

Finland soon home to world's first permanent nuclear waste site

Source: https://yle.fi/a/74-20013058

The Onkalo nuclear waste site in Eurajoki has been under construction since 2004. Image: Benjamin Suomela / Yle News

In about two to three years, nuclear waste will no longer be disposed on-site at the Olkiluoto nuclear power plant in Eurajoki. Instead, it will be buried 455 metres deep in an underground cave-like facility in Onkalo.

The site will allow spent nuclear fuel rods to be stored safely for millennia after being encased in boron steel canisters and then into a copper capsule. The encased canisters will then be placed underground in excavated caverns, which will then be backfilled with clay. This method is expected to contain radiation exposure for tens of thousands of years.

maphill
© 2011 Maphill

The facility in Onkalo, on the west coast, is the first of its kind in the world to safely dispose of nuclear waste permanently. Currently, it is standard practice in the industry for spent nuclear fuel to be stored on-site near reactors. A final licence for waste disposal at Onkalo is expected to be issued in 2024.

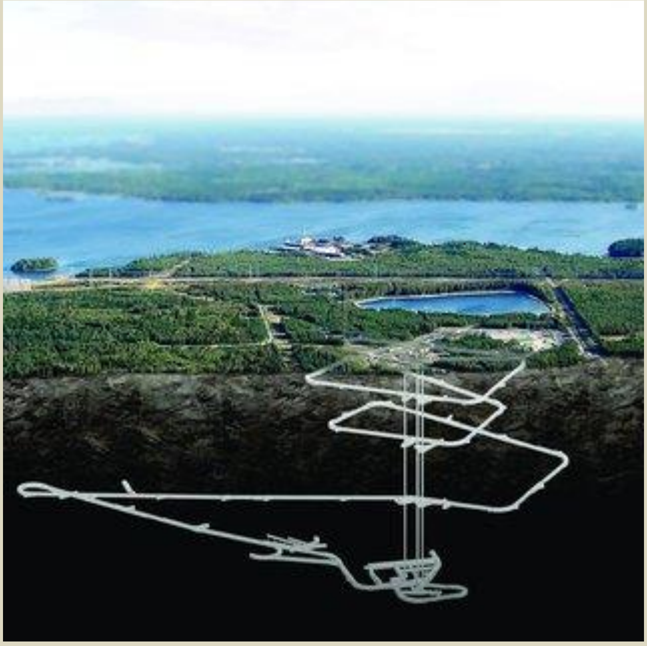
According to **Gareth Law**, a radiochemistry professor at the University of Helsinki, the eyes of the world are on this project.

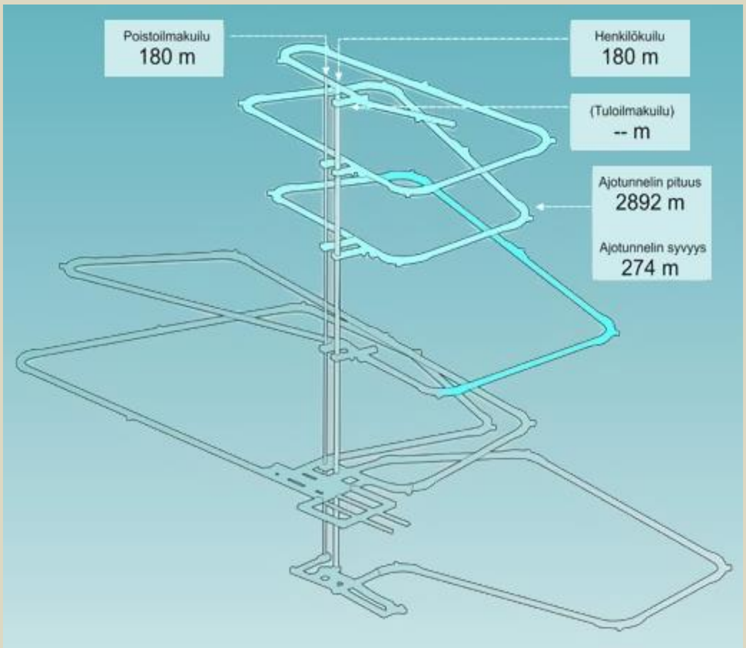
"It's wonderful pragmatism," Law said, describing Finland's decisions on nuclear waste.

International disarray

In Finland, decision-making about the final disposal site has progressed more smoothly than in other countries. **Apart from Finland, waste disposal locations have only been finalised in Sweden, Switzerland and France.**

Law, originally from the UK, pointed to how a similar project fell through in his home country, where the borough of Copeland was willing to host a nuclear waste site, but its county government opposed.





"[The county of] Cumbria was afraid that radioactive waste would drive tourists away. The geology of the area also raised concerns," said Law. In many countries, the topic of how to deal with nuclear waste brings up strong emotions, Law noted, further adding that Finland's low population density is more favourable than many other countries, as it is the least densely populated country in the EU. Other countries have also faced obstacles in selecting the location of nuclear waste sites — this past summer Switzerland caused fear across the German border when it excavated test tunnels, and the Yucca Mountain nuclear waste repository in the US has been on hold since the 1980s. "Decision-making is often very, very sticky when it comes to burying nuclear waste in bedrock," Law pointed out.

Smooth sailing in Finland

While Finland has struggled with building nuclear power plants like the long-delayed Olkiluoto 3, the construction of the Onkalo site has gone smoothly.

The excavation site was selected in 2000 and parliament approved it shortly after. By 2004, the firm Posiva began digging out the Onkalo facility.

In comparison, Sweden was prepared to create a permanent spent nuclear fuel depository in the 1990s and was supposedly 'ten years ahead' of Finland.

"Now Finland is ten years ahead of Sweden," **Jessica Palmqvist**, CEO of the Swedish nuclear waste disposal company SKB said in a video call with Yle.

However, Sweden has since chosen a final waste disposal site in Forsmark. In January 2022, the government approved the construction of the facility, but excavation work has yet to start. The firm SKB is waiting for an environmental permit and approval from Sweden's nuclear authorities.

"It is difficult to say anything for sure. But I believe the construction of the tunnels will start in the late 2020s and final waste disposal will be in the mid-2030s," Palmqvist said.

Some concern over canisters

Peter Szakalos, a corrosion researcher at the KTH Royal Institute of Technology in Sweden, said that corrosion and pressure can cause copper capsules to crack much more quickly than modelled, possibly within the span of up to a 1,000 years.

The Finnish and Swedish radiation safety authorities do not consider the corrosion threat to be significant.

Other countries are even further away from Finland and Sweden in terms of a final site.

"In the UK, for example, they are still looking for a site," **Neil Hyatt**, director of research at the NWS nuclear waste facility in the UK, told Yle. Hyatt last visited the Onkalo site a year ago and was impressed by what he saw.

"It was inspiring to see how close Onkalo is to deployment. When final waste disposal actually starts somewhere, the whole spirit of the game changes," Hyatt said.

A response to Kallenborn: Why realism requires that nuclear weapons be abolished

By Ward Hayes Wilson

Source: https://thebulletin.org/2024/01/a-response-to-kallenborn-why-realism-requires-that-nuclear-weapons-be-abolished/

In the 1960s, gentle, pot-smoking hippies believed that a new society could be created, a world filled with peace. The belief that nuclear weapons have changed human nature and made world war impossible, the author writes, is essentially the same claim those hippies made. Photo credit: Wikiwatcher 1 via Wikimedia Commons.

Jan 17 – In a recent piece in the *Bulletin* ("Why a nuclear weapons ban would threaten, not save, humanity"), Zachary Kallenborn argued that a ban on nuclear weapons would create serious risks, including unrestrained great power war and a hindering of global cooperation. He asserted that continuing to maintain small nuclear weapons arsenals for the foreseeable future is sensible.

What is troubling about this assertion is not so much that Mr. Kallenborn is wrong, but that he seems to have strayed from reality. Mistakes in a discussion about nuclear weapons policy matter because roughly 4.2 billion people depend on those policies for their safety and survival. With so much at stake, the discussion about nuclear weapons demands the highest levels of seriousness and an unflinching insistence on realism. Mr. Kallenborn has missed that mark in at least one important regard.

Nuclear weapons prevent all-out war?

Kallenborn writes, "Nuclear weapons place a cap on how bad great power conflict can become and may deter the emergence and escalation of great power war." In the world of nuclear weapons advocates, this is a common claim, viz. that nuclear weapons prevent large-scale existential wars similar to World War II. For example, John Lewis Gaddis a highly regarded historian of the Cold War, puts it this way: "As the means of fighting great wars became exponentially more devastating, the likelihood of such wars diminished, and ultimately disappeared altogether."[1] In other words, "great" wars have disappeared altogether, and nuclear weapons are the reason.

This claim is essential for those who wish to keep nuclear weapons. After all, if nuclear weapons can stop World War II-type wars, then it is safe—even necessary—to keep them. If, on the other hand, they can't, then all-out wars are more likely (because people wrongly think that nothing can go wrong as long as nuclear weapons are present). And when one occurs, the use of nuclear weapons is almost inevitable.

Unfortunately, the faith in the peace-inducing powers of nuclear weapons is wishful thinking. Wars are decided by human beings, and as the history of our civilization demonstrates—Winston Churchill once called it "the dark lamentable catalog of human crime"—human beings have deep-rooted urges to make war. It is not pleasant to insist on this portrayal of human nature, but the stakes require that we be brutally honest with ourselves. We have been fighting wars with dogged persistence for at least 6,000 years. As President John F. Kennedy put it, "[T]he human race's history, unfortunately, has been a good deal more war than peace."[2] Every era of history and region of the world has experienced war with disheartening regularity. There are sometimes pauses and respites—sometimes for even a hundred years—but the lust for war always reemerges.

American philosopher William James explained the persistence of war this way, "Our ancestors have bred pugnacity into our bone and marrow, and thousands of years of peace won't breed it out of us."[3] War is a tenacious part of our behavior. If humans were to suddenly give up fighting wars, it would be a monumental change—a revolution in human behavior. Losing our taste for war would be to surrender something central to our natures—like renouncing our predisposition for religion, our love of beauty, or our tendency to overeat. There's no doubt that the risk of using nuclear weapons can restrain thoughts of war … sometimes. But can the "magic" of nuclear weapons dissuade us forever? Nothing else has. The hopeful (and somewhat naive) belief that nuclear weapons will always prevent all-out wars ignores one important fact: The evidence that supports this claim—the last 78 years—amounts to only 1.3 percent of the evidence. The other 5,928 years tell a different story.

Let's get real

The claim that nuclear weapons have somehow permanently suppressed the heretofore unquenchable desire for war is not a realist position. Typically, it is idealists who optimistically say that we can change the world by simply changing our hearts. Idealists believe that changing human nature overnight is possible. For example, in the 1960s, gentle, pot-smoking hippies believed that a new society could be created, a utopian world where people would live in communes and value love above all other things. And with this new emphasis on love, there would naturally come a world filled with peace. And we could all hold hands and sing.

If you stop and think about it, the belief that nuclear weapons have changed human nature—what Kallenborn asserts—is essentially the same claim those hippies made. Nuclear believers say that the urge to make savage war has at last been overcome. They say we can now live in peace forever. Our darker, primitive natures will never again overwhelm our sensible, rational brains. There will be no more all-out wars. And they say this utopia of peace has already arrived (just without the singing). But rather than the power of love, it is a tool—a piece of technology—that has wrought this magical transformation.

Sadly, nuclear weapons have not transformed our warlike natures into calm and peaceful ones. Unbridled war, fought with savage abandon, is still likely, perhaps even inevitable. If you doubt that anger and violence are stalking the world, read some headlines. Around the world are sudden fires of passion that leap up first here, then there. War is raging in Europe and the Middle East. With so much hatred around as fuel, is there much doubt that a war that engulfs many nations and many peoples is far off? If you don't think so, at least some of your neighbors do. An International Red Cross survey asked millennials in 2019 if they thought a worldwide war similar to World War II would happen in their lifetimes. More than 58 percent of respondents in the United States said yes.[4]

The belief that large-scale war has been banished forever by nuclear weapons is nothing more than a dangerous fantasy. All the evidence of history and everything we know about ourselves tells us that our warlike natures cannot change overnight. (*That* is the sound of genuine realism talking.)

Claims that we can change human nature are unsurprising in the mouths of gentle, pot-smoking hippies. On the lips of nuclear weapons proponents, they are realist heresy. The fact that nuclear weapons advocates can call themselves realists and at the same time claim that nuclear weapons make all-out wars impossible shows that they do not understand the assumptions that underlie their own position. Their “realism” is nothing of the kind. The problem with relying on nuclear deterrence is that if it can’t be perfect—and perfect for all time—then it is too dangerous to rely on. Who’s to say that nuclear deterrence isn’t like a pressure cooker—able to hold off savage wars for a time, but when the top blows off at last, the destruction will be all the more far-reaching because it was held in for so long? Because of our primitive, warlike natures, nuclear weapons have to go. There are no safe hands for nuclear weapons. That is a reality that we all ignore at our own peril.

Notes

[1] John Lewis Gaddis, *The Cold War: A New History* (New York: Penguin Press, 2005), p. 52.

[2] “News conference, President John F. Kennedy,” State Department Auditorium, Washington, D.C., March 21, 1963, https://www.jfklibrary.org/Research/Research-Aids/Ready-Reference/Press-Conferences/News-Conference-52.aspx (accessed May 24, 2023).

[3] William James, “The Moral Equivalent of War,” in *War: Studies from Psychology, Sociology, Anthropology*, ed. Leon Bramson and George Goethals (New York: Basic Books, 1964), p. 23.

[4] https://www.icrc.org/en/document/majority-millennials-see-catastrophic-war-real-possibility

Ward Hayes Wilson is the author of *Five Myths About Nuclear Weapons* and *It Is Possible: A Future Without Nuclear Weapons*.

Chinese nuclear weapons, 2024

By Hans M. Kristensen, Matt Korda, Eliana Johns, and Mackenzie Knight

Source: https://thebulletin.org/premium/2024-01/chinese-nuclear-weapons-2024/

Jan 15 – Within the past five years, China has significantly expanded its ongoing nuclear modernization program by fielding more types and greater numbers of nuclear weapons than ever before. Since our previous edition on China in March 2023, China has continued to develop its three new missile silo fields for solid-fuel intercontinental ballistic missiles (ICBMs), expanded the construction of new silos for its liquid-fuel DF-5 ICBMs, has been developing new variants of ICBMs and advanced strategic delivery systems, and has likely produced excess warheads for eventual upload onto these systems once they are deployed. China has also further expanded its dual-capable DF-26 intermediate-range ballistic missile force, which appears to have completely replaced the medium-range DF-21 in the nuclear role. At sea, China has been refitting its Type 094 ballistic missile submarines with the longer-range JL-3 submarine-launched ballistic missile. In addition, China has recently reassigned an operational nuclear mission to its bombers and is developing an air-launched ballistic missile that might have nuclear capability. In all, China's nuclear expansion is among the largest and most rapid modernization campaigns of the nine nuclear-armed states.

We estimate that China has produced a stockpile of approximately 440 nuclear warheads for delivery by land-based ballistic missiles, sea-based ballistic missiles, and bombers. Roughly 60 more warheads have thought to have been produced, with more in production, to eventually arm additional road-mobile and silo-based missiles and bombers (see Table 1).

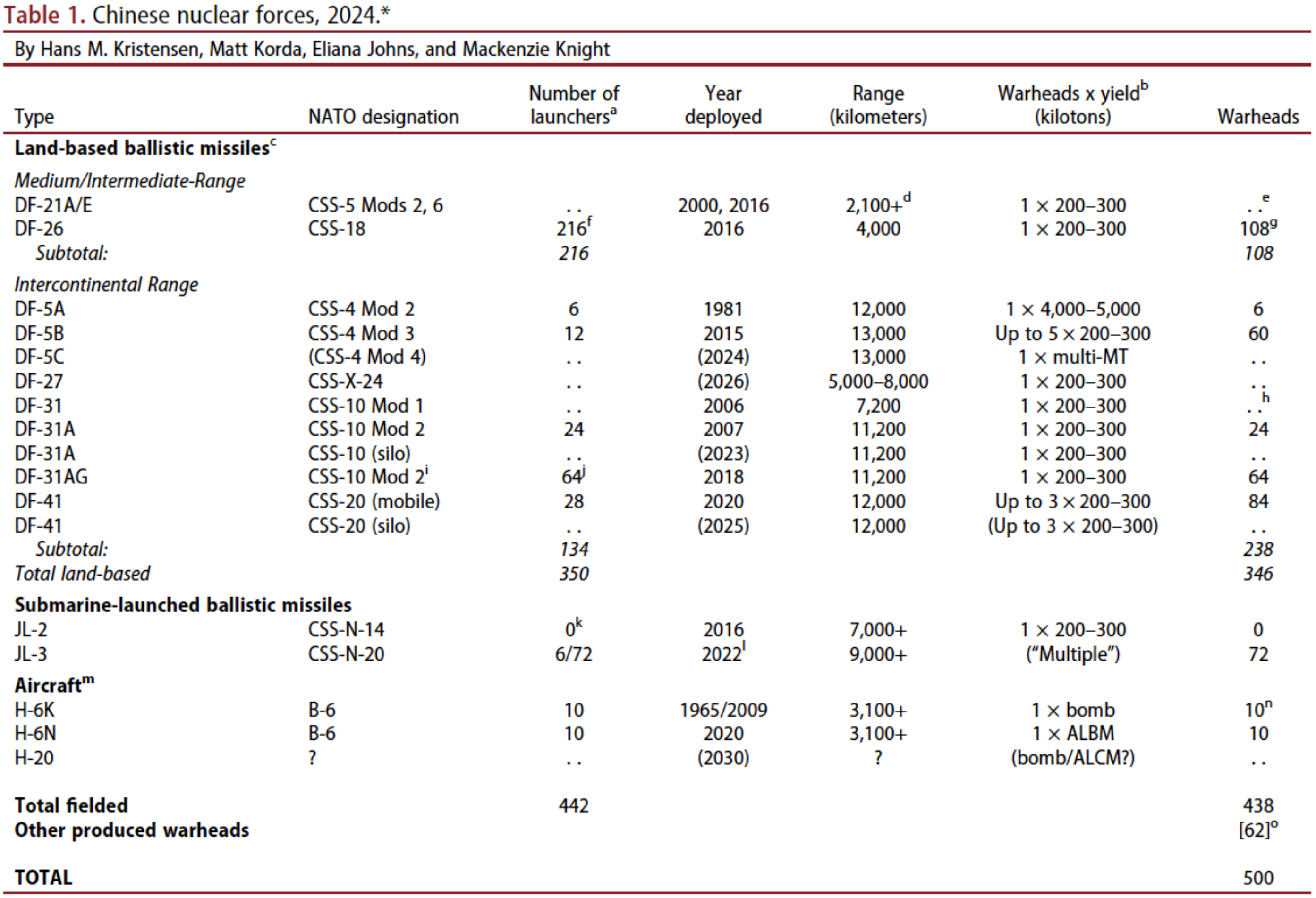


Table 1. Chinese nuclear forces, 2024.*

By Hans M. Kristensen, Matt Korda, Eliana Johns, and Mackenzie Knight

Type	NATO designation	Number of launchers[a]	Year deployed	Range (kilometers)	Warheads x yield[b] (kilotons)	Warheads
Land-based ballistic missiles[c]						
Medium/Intermediate-Range						
DF-21A/E	CSS-5 Mods 2, 6	. .	2000, 2016	2,100+[d]	1 × 200–300	. .[e]
DF-26	CSS-18	216[f]	2016	4,000	1 × 200–300	108[g]
Subtotal:		*216*				*108*
Intercontinental Range						
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	1 × multi-MT	. .
DF-27	CSS-X-24	. .	(2026)	5,000–8,000	1 × 200–300	. .
DF-31	CSS-10 Mod 1	. .	2006	7,200	1 × 200–300	. .[h]
DF-31A	CSS-10 Mod 2	24	2007	11,200	1 × 200–300	24
DF-31A	CSS-10 (silo)	. .	(2023)	11,200	1 × 200–300	. .
DF-31AG	CSS-10 Mod 2[i]	64[j]	2018	11,200	1 × 200–300	64
DF-41	CSS-20 (mobile)	28	2020	12,000	Up to 3 × 200–300	84
DF-41	CSS-20 (silo)	. .	(2025)	12,000	(Up to 3 × 200–300)	. .
Subtotal:		*134*				*238*
Total land-based		*350*				*346*
Submarine-launched ballistic missiles						
JL-2	CSS-N-14	0[k]	2016	7,000+	1 × 200–300	0
JL-3	CSS-N-20	6/72	2022[l]	9,000+	("Multiple")	72
Aircraft[m]						
H-6K	B-6	10	1965/2009	3,100+	1 × bomb	10[n]
H-6N	B-6	10	2020	3,100+	1 × ALBM	10
H-20	?	. .	(2030)	?	(bomb/ALCM?)	. .
Total fielded		442				438
Other produced warheads						[62][o]
TOTAL						500

Table 1. Chinese nuclear forces, 2024.

The Pentagon's 2023 report to Congress assessed that China's nuclear stockpile now includes over 500 warheads, in accordance with our own estimate. The Pentagon also estimates that China's arsenal will increase to about 1,000 warheads by 2030, many of which will probably be "deployed at higher readiness levels" and most "fielded on systems capable of ranging the [continental United States]" (US Department of Defense 2023, viii, 111). If expansion continues at the current rate, the Pentagon's previous projections say that China might field a stockpile of about 1,500 nuclear warheads by 2035 (US Department of Defense 2022b, 94, 98).

These projections depend on many uncertain factors, including:

- How many missile silos China will ultimately build;
- How many silos China will load with missiles;
- How many warheads each missile will carry;
- How many DF-26 intermediate-range ballistic missiles will be deployed and how many of them will have a nuclear mission;
- How many missile submarines China will field and how many warheads each missile will carry;
- How many bombers China will operate and how many weapons each will carry; and
- Assumptions about the future production of fissile materials by China.

Several US government estimates about China's nuclear weapons stockpile growth have previously proven inaccurate. The latest Pentagon projection appears to simply apply the same growth rate of new warheads added to the stockpile between 2019 and 2021 to the subsequent years until 2035. We assess that this projected growth trajectory is feasible but depends significantly upon answers to the above questions (Figure 1).

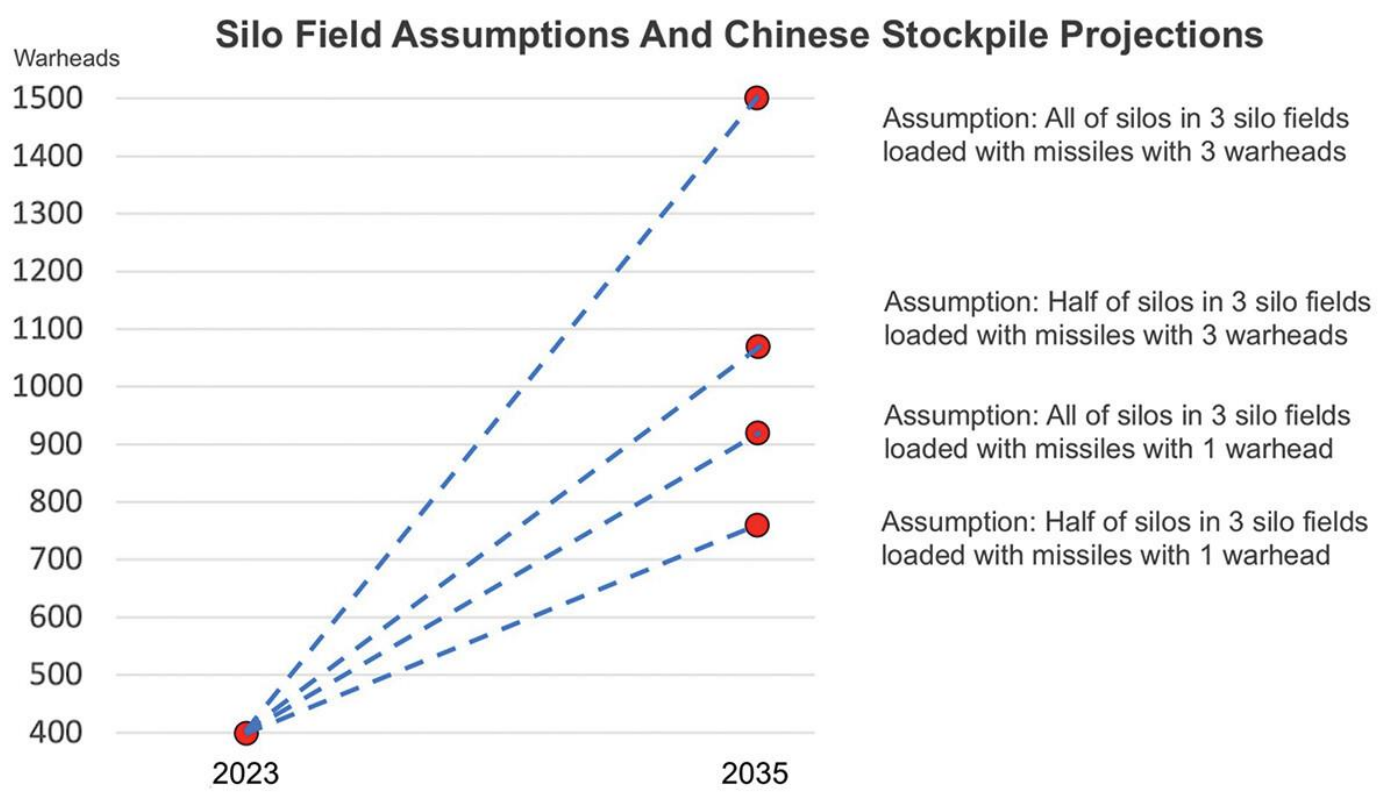


Figure 1. Projections for the growth of China's nuclear weapons stockpile depend significantly on assumptions about how China's three new solid-fuel missile silo fields will be armed. (Credit: Federation of American Scientists)

Research methodology and confidence

The analyses and estimates made in the Nuclear Notebook are derived from a combination of open sources: (1) state-originating data (e.g. government statements, declassified documents, budgetary information, military parades, and treaty disclosure data); (2) non-state-originating data (e.g. media reports, think tank analyses, and industry publications); and (3) commercial satellite imagery. Because each of these sources provides different and limited information that is subject to varying degrees of uncertainty, we crosscheck each data point by using multiple sources and supplementing them with private conversations with officials whenever possible. Analyzing and estimating China's nuclear forces is a challenging endeavor, particularly given the relative lack of state-originating data and the tight control of messaging surrounding the country's nuclear arsenal and doctrine. Like most other nuclear-armed states, China has never publicly disclosed the size of its nuclear arsenal or much of the infrastructure that supports it. This degree of relative opacity makes China's nuclear arsenal difficult to quantify, particularly given that it is likely the fastest-growing arsenal in the world. China may become more transparent about its nuclear forces over the coming decade if it deepens its participation in arms control consultations—the first of which took place in November 2023—although building a culture of nuclear transparency from scratch will take time (Gordon 2023). Despite these blind spots, it is possible to develop a much more comprehensive picture of the Chinese nuclear arsenal today than just a few decades ago by examining videos of China's People's Liberation Army (PLA), military parades, translations of strategic documents, and commercial satellite imagery. The relative degree of structure and standardization within the various PLA services also allows researchers to better understand the structure and mission of missile brigades and individual units. For example, China's missile designations generally indicate the number of stages that the missile contains (e.g., the DF-26 is a two-stage missile, while the DF-31 is a three-stage missile), and each PLA unit's five-digit military unit cover designation offers clues as to where the unit is located, how large it is, and its base and brigade assignment (Eveleth 2023, 7, 26; Xiu 2022, 6–7). In addition, other countries—particularly the United States—regularly produce public assessments or statements about China's nuclear forces. Such statements, however, must be verified as they can be institutionally biased and reflect a mind-set of worst-case thinking rather than the most-likely scenario. Analysis produced by think tanks and non-governmental experts can also be highly useful in informing estimates: The transparency surrounding China's missile forces in particular has been greatly enhanced in recent years by the unique work of Decker Eveleth (Eveleth 2023), Ben Reuter, and the US Air Force's China Aerospace Studies Institute.

It is important to view external analysis with a critical eye, as there is a high risk of citation and confirmation bias, in which governmental or non-governmental reports build on each other's estimates—sometimes without the reader knowing that this is occurring. This practice can inadvertently create a cyclical echo chamber effect, which may not necessarily match the reality on the ground. In the absence of reliable or official data, commercial satellite imagery has become a particularly critical resource for analyzing China's nuclear forces. Satellite imagery makes it possible to identify air, missile, and navy bases, as well as potential underground storage facilities. For instance, satellite imagery was used by non-governmental experts, including some of the authors of this report, to document China's new missile silo fields in 2021 (Korda and Kristensen 2021), and has been instrumental for continuously monitoring construction at those sites and at other bases across the country. The PLA's standardization has also enabled researchers to better understand developments at China's military bases, as layouts and construction dynamics now increasingly follow the same patterns, designs, and dimensions.

Considering all these factors, we maintain a relatively higher degree of confidence in our Chinese nuclear force estimates than in those of other nuclear-armed countries where official and unofficial information is scarce (Pakistan, India, Israel, and North Korea). However, our estimates about Chinese nuclear forces come with relatively more uncertainty than those for countries with greater nuclear transparency (the United States, the United Kingdom, France, and Russia).

Fissile materials production

How much and how fast China's stockpile can grow will depend upon its inventories of plutonium, highly enriched uranium (HEU), and tritium. The International Panel on Fissile Materials assessed that at the end of 2022, China had a stockpile of approximately 14 tonnes (metric tons) of HEU and approximately 2.9 tonnes of separated plutonium in or available for nuclear weapons (Kütt, Mian, and Podvig 2023, 328–329). The existing inventories were sufficient to support a doubling of the stockpile over the past five years. However, producing more than 1,000 additional warheads by 2035, as estimated by the Pentagon, would require additional fissile material production. The Pentagon assesses that China is expanding and diversifying its capability to produce tritium (US Department of Defense 2023, 110). In 2023, China also reportedly began operating two large new centrifuge enrichment plants, and also took a significant step forward with its domestic plutonium production capabilities (Zhang 2023a, 2023b).

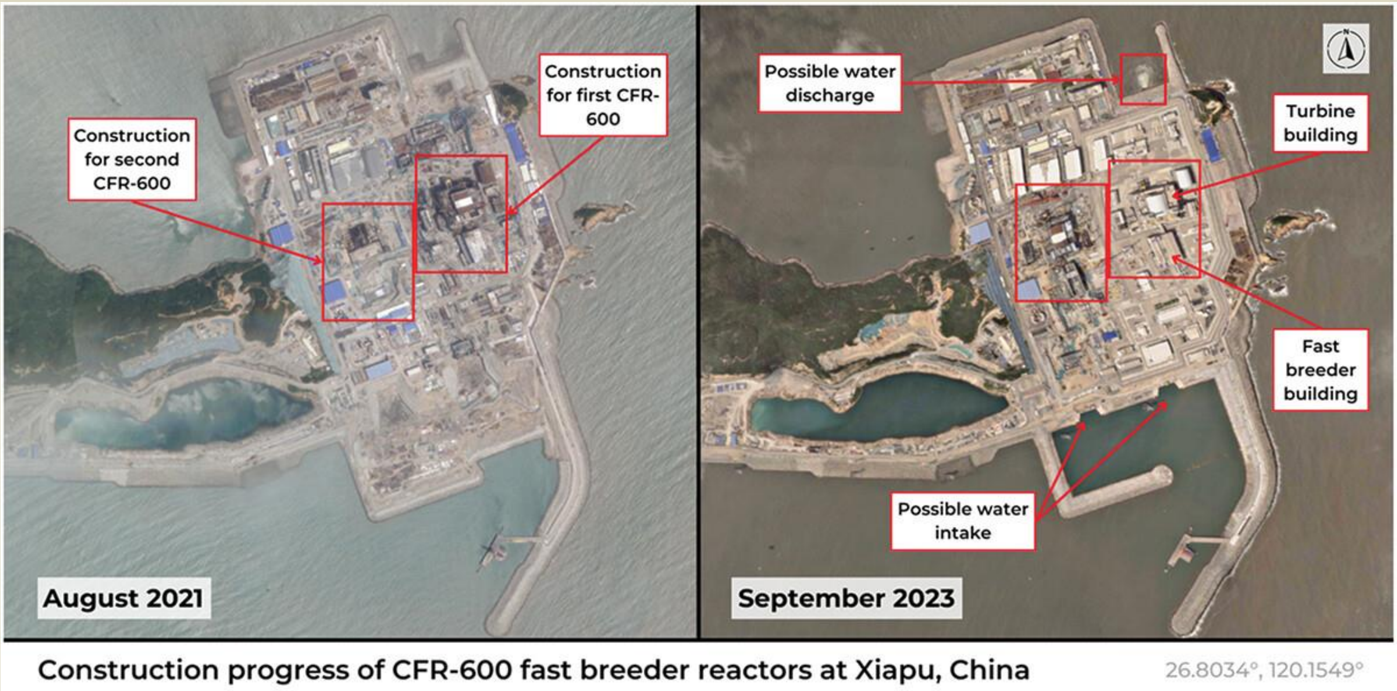

Construction for second CFR-600
Construction for first CFR-600
August 2021
Possible water discharge
Turbine building
Fast breeder building
Possible water intake
September 2023
Construction progress of CFR-600 fast breeder reactors at Xiapu, China
26.8034°, 120.1549°

Figure 2. Satellite imagery showing construction progress of the CFR-600 fast breeder reactors at Xiapu in Fujian province, China. (Credit: Planet Labs/Federation of American Scientists)

Chinese production of weapon-grade plutonium reportedly ceased in the mid-1980s (Zhang 2018). However, Beijing is combining its civilian technology and industrial sector with its defense industrial base to leverage dual-use infrastructure (US Department of Defense 2023, 28). It is believed that China likely intends to acquire significant stocks of plutonium by using its civilian reactors, including two commercial-sized CFR-600 sodium-cooled fast-breeder reactors that are currently under construction at Xiapu in Fujian province (Jones 2021; von Hippel 2021; Zhang 2021b). Rosatom—Russia's state-controlled nuclear energy company—completed the final delivery of fuel to supply the first fuel loading in December 2022 (Rosatom 2022), and steam possibly seen emanating from a cooling tower on satellite imagery in October 2023 suggests the first CFR-600 reactor may have begun operation

(Kobayashi 2023). In December 2023, the International Panel on Fissile Materials reported that the first reactor reportedly began operating at low-power mode in mid-2023, although as of October 2023 it had not yet been connected to the grid and had not yet begun generating electricity (Zhang 2023a). The second reactor is scheduled to come online by 2026 (Figure 2).

To extract plutonium from its spent nuclear fuel, China has nearly completed its first civilian "demonstration" reprocessing plant at the China National Nuclear Corporation (CNNC) Gansu Nuclear Technology Industrial Park in Jinta, Gansu province, which is expected to be operational in 2025. China has started the construction of a second plant at the same location, which should be up and running before the end of the decade (Zhang 2021a). The 200 tonne-per-year fuel reprocessing capacity at Jinta and the 50 tonne-per-year capacity at Jiuquan (Plant 404) could support the plutonium needs of the two CFR-600 reactors, especially since the first of these reactors will begin operation with highly enriched uranium (HEU) rather than mixed oxide (MOX) fuel through a supply agreement with Russia (US Department of Defense 2023, 109; Zhang 2021a).

The ambiguity of Chinese nuclear warhead types and uncertainty on the exact amount of fissile material required for each warhead design make it difficult to estimate how many weapons China could produce from its existing HEU and weapons-grade plutonium stockpiles. Once both fast-breeder reactors come online, they could potentially produce large amounts of plutonium and, by some estimates, could enable China to acquire over 330 kilograms of weapon-grade plutonium annually for new warhead production (Kobayashi 2023)—which would be consistent with the Pentagon's most recent projections.

While China's production and reprocessing of fissile materials is consistent with its nuclear power efforts and its goal of reaching a closed nuclear fuel cycle, the Pentagon suggests that "it is likely that Beijing intends to use this infrastructure to produce nuclear warhead materials for its military in the near term" (US Department of Defense 2023, 109). The degree of transparency surrounding China's nuclear materials production and its suspected expansion of uranium and tritium production has recently decreased as China has not reported its separated plutonium stockpile to the International Atomic Energy Agency since 2017.

US estimates and assumptions about Chinese nuclear forces

Evaluation of current US projections about the future size of China's nuclear weapons stockpile must take earlier projections into account, some of which did not come to pass. During the 1980s and 1990s, US government agencies published several projections for the number of Chinese nuclear warheads. A US Defense Intelligence Agency study from 1984 inaccurately estimated that China had 150 to 360 nuclear warheads and projected it could increase to more than 800 by 1994 (Kristensen 2006). Over a decade later, another Defense Intelligence Agency study published in 1999 projected that China might have over 460 nuclear weapons by 2020 (US Defense Intelligence Agency 1999). While this latter projection ultimately proved to be closer to the warhead estimate the Pentagon published in 2020, it was still more than twice the "low-200s" warhead estimate announced by the Pentagon (US Department of Defense 2020a, ix; Figure 3).

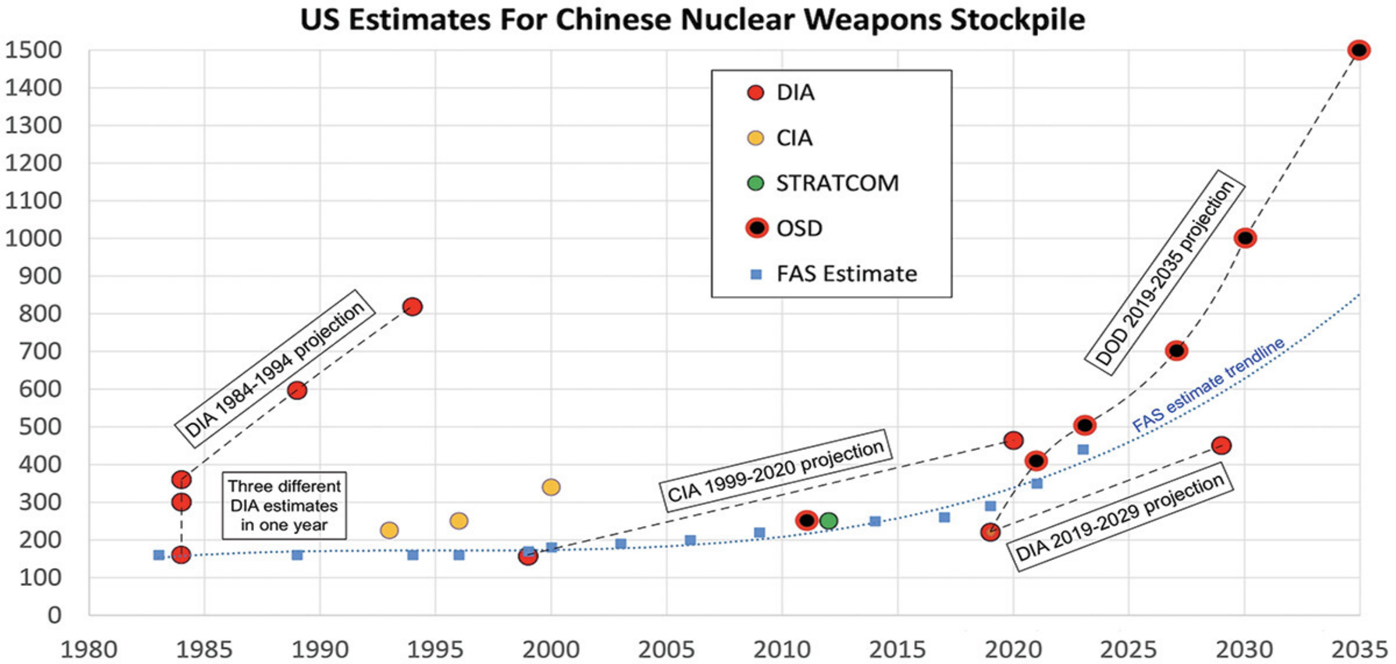


Figure 3. US organizations' estimate of China's nuclear weapons stockpile. Abbreviations used: CIA, Central Intelligence Agency; DIA, Defense Intelligence Agency; DOD, US Department of Defense; FAS, Federation of American Scientists; OSD, Office of the Secretary of Defense; STRATCOM, US Strategic Command. (Credit: Federation of American Scientists)

Current US projections should be read with this record in mind. In November 2021, the Pentagon's annual China Military Power Report (CMPR) to Congress projected that China could have 700 deliverable warheads by 2027, and possibly as many as 1,000 by 2030 (US Department of Defense 2021, 90). The 2022 Pentagon report increased the projection even further, claiming that China's stockpile of "operational" nuclear warheads had surpassed 400 and will likely reach about 1,500 warheads by 2035 (US Department of Defense 2022b, 94). According to the latest 2023 CMPR, China "had more than 500 operational nuclear warheads" as of May 2023 and is on track to have over 1,000 operational warheads by 2030 as previously reported (US Department of Defense 2023, viii). The observable operational force structure, however, does not add up to more than 500 operational warheads (this report estimates approximately 440) unless the Pentagon estimate attributes nuclear warheads to all the DF-26 launchers (which seems excessive), several dozen new missile silos have been loaded with missiles (which is possible, but we have not yet seen indications of widespread loading operations with commercial satellite imagery), or the estimate includes new warheads in production for new missiles. To that effect, this report estimates that China's stockpile numbers approximately 500 warheads; however, we assess that several dozen of these have not yet been fielded and have likely been produced (or are in production) to eventually arm incoming delivery systems. Curiously, the 2023 report does not repeat the 1,500-warhead projection for 2035.

After the release of the 2022 CMPR, the spokesperson for China's Ministry of National Defense, Senior Col. Tan Kefei, reacted saying that the Pentagon was "distorting China's national defense policy and military strategy, groundlessly speculating about China's military development" (Li 2022a). The following year, spokesperson Wu Qian criticized the 2023 CMPR, saying it "exaggerated and sensationalized the non-existent 'Chinese military threat'" (Ministry of National Defense of the People's Republic of China 2023a). None of the two spokespersons acknowledged—nor denied—the expansion of the mobile ICBM force or the construction of three large new missile silo fields.

The projected increase has unsurprisingly triggered a wide range of speculations about China's nuclear intentions. In 2020, Trump administration officials suggested that "China no longer intends to field a minimal deterrent," and instead strives for "a form of nuclear parity with the United States and Russia" (Billingslea 2020). These statements were echoed in August 2021 by the Deputy Commander of US Strategic Command, who stated that: "There's going to be a point, a crossover point, where the number of threats presented by China will exceed the number of threats that currently Russia presents," noting that this point would likely be reached "in the next few years" (Bussiere 2021). In April 2022, the commander of the US Strategic Command, Adm. Charles Richard, referred to China's expansion of its strategic and nuclear forces as "breathtaking," later stating that China was intent on pursuing a "world-class military by 2030, and the military capabilities to seize Taiwan by force, if they choose to, by 2027" (US Strategic Command 2022). He also referred to China's "investments in nuclear command and control" and "nascent launch under warning, launch under attack" capabilities as clear signs that they have improved their readiness and "moved a long way off the historic minimum-deterrence posture" (US Strategic Command 2022). In March 2023, the Commander of the US Strategic Command (STRATCOM), Gen. Anthony Cotton, conveyed a similar perspective, testifying that "China seeks to match, or in some areas surpass, quantitative and qualitative parity with the United States in terms of nuclear weapons. China's nuclear capabilities already exceed those needed for its long-professed policy of 'minimum deterrence,' but China's capabilities continue to grow at an alarming rate" (Cotton 2023).

Even the worst-case projection of 1,500 warheads by 2035 amounts to less than half of the current US nuclear stockpile, so the Chinese government uses the disparity in total warhead numbers to argue it is "unrealistic to expect China to join [the United States and Russia] in a negotiation aimed at nuclear arms reduction" (Ministry of National Defense of the People's Republic of China 2020). While highlighting the increase of Chinese warheads, US defense officials at the same time downplay the importance of numbers when reminded that the United States has many more: "We don't approach it from purely a numbers game," according to the deputy commander of the US Strategic Command, Lt. Gen. Thomas Bussiere. "It is what is operationally fielded, … status of forces, posture of those fielded forces. So, it is not just a stockpile number," he said (Bussiere 2021).

Nuclear testing

The projection for how much the Chinese nuclear stockpile will increase also depends on the size and design of its warheads. China's nuclear testing program of the 1990s partially supported development of the warhead type currently arming the DF-31-class ICBMs. This warhead may also have been used to equip the liquid-fueled DF-5B ICBM with multiple independently targeted reentry vehicle (MIRV) technology, replacing the much larger warhead used on the DF-5A. The large DF-41 and the JL-3 could potentially use the same smaller warhead. The Pentagon believes that China probably seeks a "lower-yield" nuclear warhead for the DF-26 (US Department of Defense 2023, 111), however it is unclear if that implies production of a new warhead or how low a "lower" yield is; the warhead for the DF-31 and DF-41 are also thought to have lower yield than the warhead deployed on the DF-5A.

Recently, the United States has publicly shared its concerns about activity at China's Lop Nur nuclear test site. The (US Department of State's 2022) Compliance Report assessed that some of China's actions at Lop Nur "raise concern" about China's adherence to the United States' "zero-yield" standard (US Department of State 2022, 29). However, the report did not explicitly accuse China of conducting tests that produced a yield, nor did it present any evidence to that effect. The 2023 Compliance Report provided no update on China’s activity at Lop Nur, and the 2023 China Military Posture Report implied again that China is possibly preparing to operate its Lop Nur test site “year-round,” but offered no new information (US Department of State 2023, 18; US Department of Defense 2023, US Department of Defense 2022b, 98).

Open-source satellite imagery analysis indicates that China appears to be expanding the Lop Nur test site with the construction of approximately a dozen concrete buildings near the site’s airfield, as well as at least one new tunnel at the site’s northern testing area (Brumfiel 2021b). Satellite imagery shows what appears to be new drainage areas, drill rigs, roads, spoil piles, and covered entrances to potential underground facilities, as well as new construction at the main administration, support, and storage areas (Brumfiel 2021a; Babiarz 2023; Lewis 2023). Many of these activities remained visible as of the time of writing this report. In addition to new activity at the northern tunnel test area, satellite imagery also indicated activity at a possible new eastern test area at Lop Nur (Babiarz 2023). Although the construction works are significant, they do not necessarily prove that China plans to conduct new nuclear detonations at the test site. If China did conduct low-yield nuclear tests at Lop Nur, it would violate its responsibility under the Comprehensive Test Ban Treaty it has signed but not ratified.

Nuclear doctrine and policy

Since its first nuclear test in 1964, China has maintained a consistent narrative about the purpose of its nuclear weapons. This narrative was recently restated in China’s updated 2023 national defense policy: “China is always committed to a nuclear policy of no first use of nuclear weapons at any time and under any circumstances, and not using or threatening to use nuclear weapons against non-nuclear-weapon states or nuclear-weapon-free zones unconditionally. … China does not engage in any nuclear arms race with any other country and keeps its nuclear capabilities at the minimum level required for national security. China pursues a nuclear strategy of self-defense, the goal of which is to maintain national strategic security by deterring other countries from using or threatening to use nuclear weapons against China” (Ministry of National Defense of the People’s Republic of China 2023b).

Despite its declaratory policy of emphasizing a “defensive” nuclear posture, China has never defined how large a “minimum” capability is or what activities constitute an “arms race,” and the stated policies evidently do not prohibit a massive expansion. The posture apparently seeks to “adapt to the development of the world’s strategic situation,” part of which involves the “organic integration nuclear counterattack capability and conventional strike capability” (China Aerospace Studies Institute 2022, 381–382).

Such capabilities require investing significant resources to ensure the survivability of the nuclear arsenal against a nuclear or conventional first strike, including practicing “nuclear attack survival exercises” to ensure that troops could still launch nuclear counterattacks if China were to be attacked (Global Times 2020). It also involves improving space-based early warning systems and the stealth capabilities of its nuclear forces to be able to elude enemy detection (Kaufman and Waidelich 2023, 42, 45).

The People’s Liberation Army (China’s principal military force) maintains what it refers to as a “moderate” readiness level for its nuclear forces and keeps most of its warheads at its regional storage facilities and its central hardened storage facility in the Qinling mountain range.[1] The 2023 Pentagon report reaffirmed this posture, stating that China maintains “a portion of its units on a heightened state of readiness while leaving the other portion in peacetime status with separated launchers, missiles, and warheads.” But the report also described that the People’s Liberation Army Rocket Force (PLARF) brigades conduct “combat readiness duty” and “high alert duty” drills, which “includes assigning a missile battalion to be ready to rapidly launch” (US Department of Defense 2023, 106).

The readiness of the Chinese nuclear missile force was challenged in early 2024 with disclosure that a US intelligence assessment had found that corruption within the People’s Liberation Army had led to an erosion of confidence in its overall capabilities, particularly when it comes to the Rocket Force (Martin and Jacobs 2024).

Increased readiness and alert drills do not necessarily require nuclear warheads to be installed on the missiles or prove that they are installed at all times, but it cannot be ruled out either. However, recent dismissals of top defense officials and widespread corruption might chill the Chinese leadership’s willingness to arm missiles with warheads in peacetime. A nuclear attack against China is unlikely to come out of the blue and is more likely to follow a period of increasing tension and possibly conventional warfare, allowing the warheads to be mated to the missiles in time. In April 2019, the Chinese delegation to the Preparatory Committee for the 2020 Review Conference of the Parties to the Treaty on the Nonproliferation of Nuclear Weapons provided a generic description of its alert posture and the stages Chinese nuclear forces would go through in a crisis:

In peacetime, the nuclear force is maintained at a moderate state of alert. In accordance with the principles of peacetime-wartime coordination, constant readiness, and being prepared to fight at any time, China strengthens its combat readiness support to ensure effective response to war threats and emergencies. If the country faced a nuclear threat, the alert status would be raised and preparations for nuclear counter-attack undertaken under the orders of the Central Military Commission to deter the enemy from using nuclear weapons against China. If the country were subjected to nuclear attack, it would mount a resolute counter-attack against the enemy. (Ministry of Foreign Affairs of the People’s Republic of China 2019)

In peacetime, the “moderate state of alert” might involve designated units to be deployed in high combat-ready condition with nuclear warheads installed or in nearby storage sites under control of the Central Military Commission that could be released to the unit quickly if necessary. China is building several underground facilities at some of its newer sites, including at its three solid-fuel missile silo complexes, which could potentially be used for warhead storage.

The Pentagon assesses that China’s construction of new silo fields and the expansion of its liquid-propellant ICBM force indicates its intent to move to a launch-on-warning (LOW) posture to increase the peacetime readiness of its nuclear forces (US Department of Defense 2023, viii). The Pentagon elaborates that part of the LOW posture involves implementing an “early warning counterstrike” strategy, relying on space- and ground-based sensors that would warn of an enemy missile strike that would give China time to launch its missiles before they would be destroyed (US Department of Defense 2023, 112).

As part of this effort, the Pentagon says that the PLARF continues to conduct exercises involving “early warning of a nuclear strike and LOW responses” (US Department of Defense 2023, 112). In its 2023 report, the Pentagon assessed that China “likely has at least three early warning satellites in orbit” to support its LOW posture as of mid-2023 (US Department of Defense 2023, 112).

In addition to the technical means for protecting the missiles against a first strike, the PLARF has also emphasized “survival protection” for its land-based nuclear forces (China Aerospace Studies Institute 2022, 386). This involves training soldiers to perform additional tasks beyond their primary roles, including a “role switch” where a transporter erector launcher (TEL) driver would also know how to launch a missile, or a measurement specialist who knows how to command (Baughman 2022). During one “survival protection” training exercise in November 2021, a launch battalion was informed they would be “killed” by an enemy missile strike in five minutes. Rather than attempting to evacuate—the standard “survival protection” procedure—the battalion commander ordered his troops to conduct a surprise “launch on the spot” of their ballistic missile before the enemy missile hit their position (Baughman 2022; Lu and Liu 2021). While the report did not specify whether the battalion had a nuclear or conventional strike role, the results of the exercise suggest that the PLARF is practicing launching missiles in a launch-on-warning scenario.

These data points, however, are not necessarily evidence of a formal shift to a more aggressive nuclear posture (Fravel, Hiim, and Trøan 2023). They could just as likely be intended to allow China to disperse its forces and, if needed, launch rapidly—but not necessarily “on warning”—in the context of a crisis, thereby safeguarding its forces against a surprise conventional or nuclear first strike. For decades, China has deployed silo-based DF-5s and road-mobile ICBMs that, in a crisis, would be armed with the intention to launch them before they are destroyed. China potentially could maintain its current strategy even with many new silos and improved early-warning systems.

Notably, both the United States and Russia operate large numbers of solid-fuel silo-based missiles and early-warning systems to be able to detect nuclear attacks and launch their missiles before they are destroyed. The two countries also insist that such a posture is both necessary and stabilizing. It seems reasonable to assume that China would seek a similar posture to safeguard its own retaliatory capability.

A Chinese early-warning system could potentially also be intended to enable a future advanced missile defense system. The latest Pentagon report on China’s military capabilities notes that China is developing an indigenous HQ-19 (known to the United States as CH-AB-X-02) anti-ballistic missile system as well as a hit-to-kill mid-course interceptor that could engage intermediate-range ballistic missiles and possibly ICBMs, although the latter would still take many years to develop (US Department of Defense 2023, 64). China already maintains several ground-based large phased-array radars that contribute to its nascent early-warning capabilities. The PLA continues to substantially invest in and improve its intelligence, surveillance, and reconnaissance (ISR) infrastructure and is reportedly progressing in its development of a space-based early warning capability (US Department of Defense 2023, 112).

China’s nuclear modernization—particularly the construction of hundreds of silos for solid-fuel missiles and the development of an “early warning counter-strike” strategy—has triggered significant debate about China’s longstanding no-first-use policy. Although there has been considerable discussion in China about the size and readiness of the nuclear arsenal as well as when the no-first-use policy would apply, there is little evidence to suggest that the Chinese government has deviated from it, which is also reiterated in its 2023 national defense strategy (Ministry of National Defense of the People’s Republic of China 2023b; Santoro and Gromoll 2020).

It remains unclear what circumstances could cause the Chinese leadership to order the use of nuclear weapons. In the past, Chinese officials have privately stated that China reserves the right to use nuclear weapons if its nuclear forces were attacked with conventional weapons. In addition, in 2023, the Pentagon’s annual report stated that “China’s nuclear strategy probably includes consideration of a nuclear strike in response to a non-nuclear attack threatening the viability of China’s nuclear forces or C2, or that approximates the strategic effects of a nuclear strike” (US Department of Defense 2023, 105).

The modernization of the nuclear forces could gradually influence Chinese nuclear strategy and declaratory policy in the future by offering more efficient ways of deploying, responding, and coercing with nuclear or dual-capable forces. The 2022 US Nuclear Posture Review suggested that China’s trajectory of expanding and improving its nuclear arsenal could “ … provide [China] with new options before and during a crisis or conflict to leverage nuclear weapons for coercive purposes, including military provocations against US Allies and partners in the region" (US Department of Defense 2022a, 4). Advanced non-nuclear weapons could also provide a strategic strike capability that may achieve effects similar to a first use of nuclear weapons (Kaufman and Waidelich 2023, 21).

This raises the question of whether China will leverage nuclear weapons in its "counter-intervention" strategy that aims to limit the US presence in the East and South China Seas and achieve reunification with Taiwan. China has made clear that it "keeps to the stance that China will not attack unless we are attacked, but China will surely counterattack if attacked. China will firmly defend its national sovereignty and territorial integrity, and resolutely thwart the interference of external forces and the separatist activities for 'Taiwan Independence'" (Li 2022b).

Regardless of what the specific red lines may be, China's no-first-use policy probably has a high threshold. Many experts believe there are very few scenarios in which China would benefit strategically from a first strike even in the case of conventional conflict with a military power such as the United States (Tellis 2022, 27). The Pentagon also assesses that the PLA most likely prioritizes conflict de-escalation when considering nuclear strike targets and would probably seek to avoid an extended series of nuclear exchanges against a superior adversary (US Department of Defense 2023, 105).

Land-based ballistic missiles

China is continuing the long-term modernization of its land-based, nuclear-capable missile force, but the pace and scope of this effort has increased significantly with the construction underway of approximately 350 new missile silos and several new bases for road-mobile missile launchers. Overall, we estimate that the PLARF currently operates approximately 350 launchers for land-based missiles that can deliver nuclear warheads (excluding new silos that are likely not yet fully operational). Of those missiles, nearly half—about 135—can reach the continental United States. Most of China's ballistic missile launchers are for short-, medium-, and intermediate- range missiles intended for regional missions, and most of those do not have nuclear strike missions. We estimate there are about 108 nuclear warheads assigned to regional missiles, although this number comes with significant uncertainty.

The PLARF, which is headquartered in Beijing, has recently undergone several management shakeups: In July 2023, the PLARF commander and political commissar, along with several other senior officers, were removed from their positions following an anti-corruption investigation. Notably, the top two PLARF officials were replaced by generals from outside the PLARF itself: the new commander and political commissar come from the People's Liberation Army Navy (PLAN) and the People's Liberation Army Air Force (PLAAF), respectively (Lendon, McCarthy, and Chang 2023).

The PLARF controls nine individually-numbered bases: six for missile operations distributed across China (Bases 61 through 66), one for overseeing the central nuclear stockpile (Base 67), one for maintaining infrastructure (Base 68), and one that is assumed to be for training and missile tests (Base 69) (Xiu 2022, 2). Each missile operating base controls six to eight missile brigades, with the number of launchers and missiles assigned to each brigade depending on the type of missile (Xiu 2022, 5).

To accommodate the growing missile force, the total number of Chinese missile brigades has increased too. This increase is predominantly caused by the growing inventory of conventional missiles, but it is also a product of China's nuclear modernization program. We estimate that the PLARF currently has approximately 45 brigades with ballistic or cruise missile launchers. Of those brigades, approximately 30 operate ballistic missile launchers with nuclear capability or are upgrading to do so soon (see Table 2). This is close to the 50 nuclear missile brigades operated by Russia—known as regiments in the Russian military (Kristensen, Korda, and Reynolds 2023).

Intercontinental ballistic missiles

We estimate that China currently operates approximately 134 ICBMs that can deliver nearly 240 warheads. The most significant recent development in China's nuclear arsenal is the construction of what appears to be approximately 320 new missile silos in three desert areas across northern China (excluding the training silos at Jilantai) and the construction of 30 new silos in three mountainous areas of central-eastern China (Eveleth 2023; Korda and Kristensen 2021; Lee 2021; Lewis and Eveleth 2021; Reuter 2023).

Throughout the extensive construction period, each silo across the three new northern Chinese complexes was covered with an inflatable air dome to protect the site from environmental damage as well as from the prying eyes of satellite imagery analysts. These air domes were removed from all silos in the three new solid-fuel missile fields by the end of 2022, indicating that the most sensitive stages of construction had been completed by that point. The Department of Defense first declared them completed in late 2022 (Kristensen, Johns, and Korda 2023).

At each one of the three missile silo fields—as well as the training site at Jilantai—the silos are positioned roughly three kilometers apart in an almost perfect triangular grid pattern. The silo fields are located deeper inside China than any other known ICBM base, and beyond the reach of the United States' conventional and nuclear cruise missiles. These facilities consist of the Yumen, Hami, and Yulin silo fields; details for which are rendered below:

Table 2. Chinese missile brigades, 2024. (Click to display full size with notes.)

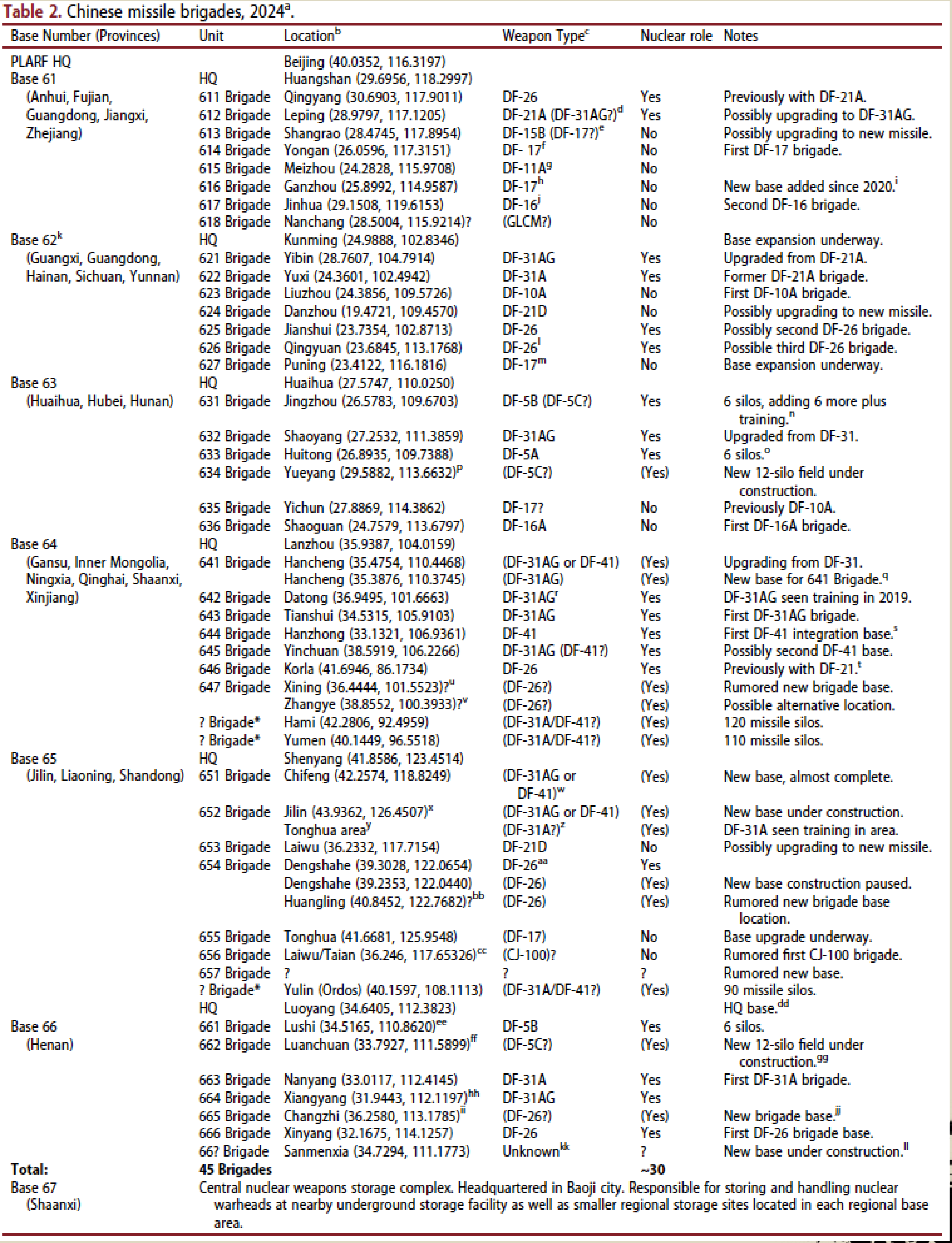


Table 2. Chinese missile brigades, 2024[a].

Base Number (Provinces)	Unit	Location[b]	Weapon Type[c]	Nuclear role	Notes
PLARF HQ		Beijing (40.0352, 116.3197)			
Base 61	HQ	Huangshan (29.6956, 118.2997)			
(Anhui, Fujian, Guangdong, Jiangxi, Zhejiang)	611 Brigade	Qingyang (30.6903, 117.9011)	DF-26	Yes	Previously with DF-21A.
	612 Brigade	Leping (28.9797, 117.1205)	DF-21A (DF-31AG?)[d]	Yes	Possibly upgrading to DF-31AG.
	613 Brigade	Shangrao (28.4745, 117.8954)	DF-15B (DF-17?)[e]	No	Possibly upgrading to new missile.
	614 Brigade	Yongan (26.0596, 117.3151)	DF- 17[f]	No	First DF-17 brigade.
	615 Brigade	Meizhou (24.2828, 115.9708)	DF-11A[g]	No	
	616 Brigade	Ganzhou (25.8992, 114.9587)	DF-17[h]	No	New base added since 2020.[i]
	617 Brigade	Jinhua (29.1508, 119.6153)	DF-16[j]	No	Second DF-16 brigade.
	618 Brigade	Nanchang (28.5004, 115.9214)?	(GLCM?)	No	
Base 62[k]	HQ	Kunming (24.9888, 102.8346)			Base expansion underway.
(Guangxi, Guangdong, Hainan, Sichuan, Yunnan)	621 Brigade	Yibin (28.7607, 104.7914)	DF-31AG	Yes	Upgraded from DF-21A.
	622 Brigade	Yuxi (24.3601, 102.4942)	DF-31A	Yes	Former DF-21A brigade.
	623 Brigade	Liuzhou (24.3856, 109.5726)	DF-10A	No	First DF-10A brigade.
	624 Brigade	Danzhou (19.4721, 109.4570)	DF-21D	No	Possibly upgrading to new missile.
	625 Brigade	Jianshui (23.7354, 102.8713)	DF-26	Yes	Possibly second DF-26 brigade.
	626 Brigade	Qingyuan (23.6845, 113.1768)	DF-26[l]	Yes	Possible third DF-26 brigade.
	627 Brigade	Puning (23.4122, 116.1816)	DF-17[m]	No	Base expansion underway.
Base 63	HQ	Huaihua (27.5747, 110.0250)			
(Huaihua, Hubei, Hunan)	631 Brigade	Jingzhou (26.5783, 109.6703)	DF-5B (DF-5C?)	Yes	6 silos, adding 6 more plus training.[n]
	632 Brigade	Shaoyang (27.2532, 111.3859)	DF-31AG	Yes	Upgraded from DF-31.
	633 Brigade	Huitong (26.8935, 109.7388)	DF-5A	Yes	6 silos.[o]
	634 Brigade	Yueyang (29.5882, 113.6632)[p]	(DF-5C?)	(Yes)	New 12-silo field under construction.
	635 Brigade	Yichun (27.8869, 114.3862)	DF-17?	No	Previously DF-10A.
	636 Brigade	Shaoguan (24.7579, 113.6797)	DF-16A	No	First DF-16A brigade.
Base 64	HQ	Lanzhou (35.9387, 104.0159)			
(Gansu, Inner Mongolia, Ningxia, Qinghai, Shaanxi, Xinjiang)	641 Brigade	Hancheng (35.4754, 110.4468)	(DF-31AG or DF-41)	(Yes)	Upgrading from DF-31.
		Hancheng (35.3876, 110.3745)	(DF-31AG)	(Yes)	New base for 641 Brigade.[q]
	642 Brigade	Datong (36.9495, 101.6663)	DF-31AG[r]	Yes	DF-31AG seen training in 2019.
	643 Brigade	Tianshui (34.5315, 105.9103)	DF-31AG	Yes	First DF-31AG brigade.
	644 Brigade	Hanzhong (33.1321, 106.9361)	DF-41	Yes	First DF-41 integration base.[s]
	645 Brigade	Yinchuan (38.5919, 106.2266)	DF-31AG (DF-41?)	Yes	Possibly second DF-41 base.
	646 Brigade	Korla (41.6946, 86.1734)	DF-26	Yes	Previously with DF-21.[t]
	647 Brigade	Xining (36.4444, 101.5523)?[u]	(DF-26?)	(Yes)	Rumored new brigade base.
		Zhangye (38.8552, 100.3933)?[v]	(DF-26?)	(Yes)	Possible alternative location.
	? Brigade*	Hami (42.2806, 92.4959)	(DF-31A/DF-41?)	(Yes)	120 missile silos.
	? Brigade*	Yumen (40.1449, 96.5518)	(DF-31A/DF-41?)	(Yes)	110 missile silos.
Base 65	HQ	Shenyang (41.8586, 123.4514)			
(Jilin, Liaoning, Shandong)	651 Brigade	Chifeng (42.2574, 118.8249)	(DF-31AG or DF-41)[w]	(Yes)	New base, almost complete.
	652 Brigade	Jilin (43.9362, 126.4507)[x]	(DF-31AG or DF-41)	(Yes)	New base under construction.
		Tonghua area[y]	(DF-31A?)[z]	(Yes)	DF-31A seen training in area.
	653 Brigade	Laiwu (36.2332, 117.7154)	DF-21D	No	Possibly upgrading to new missile.
	654 Brigade	Dengshahe (39.3028, 122.0654)	DF-26[aa]	Yes	
		Dengshahe (39.2353, 122.0440)	(DF-26)	(Yes)	New base construction paused.
		Huangling (40.8452, 122.7682)?[bb]	(DF-26)	(Yes)	Rumored new brigade base location.
	655 Brigade	Tonghua (41.6681, 125.9548)	(DF-17)	No	Base upgrade underway.
	656 Brigade	Laiwu/Taian (36.246, 117.65326)[cc]	(CJ-100)?	No	Rumored first CJ-100 brigade.
	657 Brigade	?	?	?	Rumored new base.
	? Brigade*	Yulin (Ordos) (40.1597, 108.1113)	(DF-31A/DF-41?)	(Yes)	90 missile silos.
	HQ	Luoyang (34.6405, 112.3823)			HQ base.[dd]
Base 66	661 Brigade	Lushi (34.5165, 110.8620)[ee]	DF-5B	Yes	6 silos.
(Henan)	662 Brigade	Luanchuan (33.7927, 111.5899)[ff]	(DF-5C?)	(Yes)	New 12-silo field under construction.[gg]
	663 Brigade	Nanyang (33.0117, 112.4145)	DF-31A	Yes	First DF-31A brigade.
	664 Brigade	Xiangyang (31.9443, 112.1197)[hh]	DF-31AG	Yes	
	665 Brigade	Changzhi (36.2580, 113.1785)[ii]	(DF-26?)	(Yes)	New brigade base.[jj]
	666 Brigade	Xinyang (32.1675, 114.1257)	DF-26	Yes	First DF-26 brigade base.
	66? Brigade	Sanmenxia (34.7294, 111.1773)	Unknown[kk]	?	New base under construction.[ll]
Total:	**45 Brigades**			**~30**	
Base 67 (Shaanxi)	Central nuclear weapons storage complex. Headquartered in Baoji city. Responsible for storing and handling nuclear warheads at nearby underground storage facility as well as smaller regional storage sites located in each regional base area.				

Yumen silo field

The Yumen silo field, located in Gansu province in the western military district, covers an area of approximately 1,110 square kilometers with a perimeter fence surrounding the entire complex. The field includes 120 individual silos. There also appear to be at least five launch control centers scattered throughout the field, which are connected to the silos through underground cables.

In addition to the 120 silos, the Yumen field also includes dozens of supporting and defensive structures. These include multiple security gates in the north (40.38722° N, 96.52416° E) and south (40.03437° N, 96.69658° E), at least 23 support facilities, and approximately 20 surveillance or radio towers. Additionally, the Yumen field includes at least five raised square platforms around the perimeter of the complex, which could possibly be used for air and missile defense.

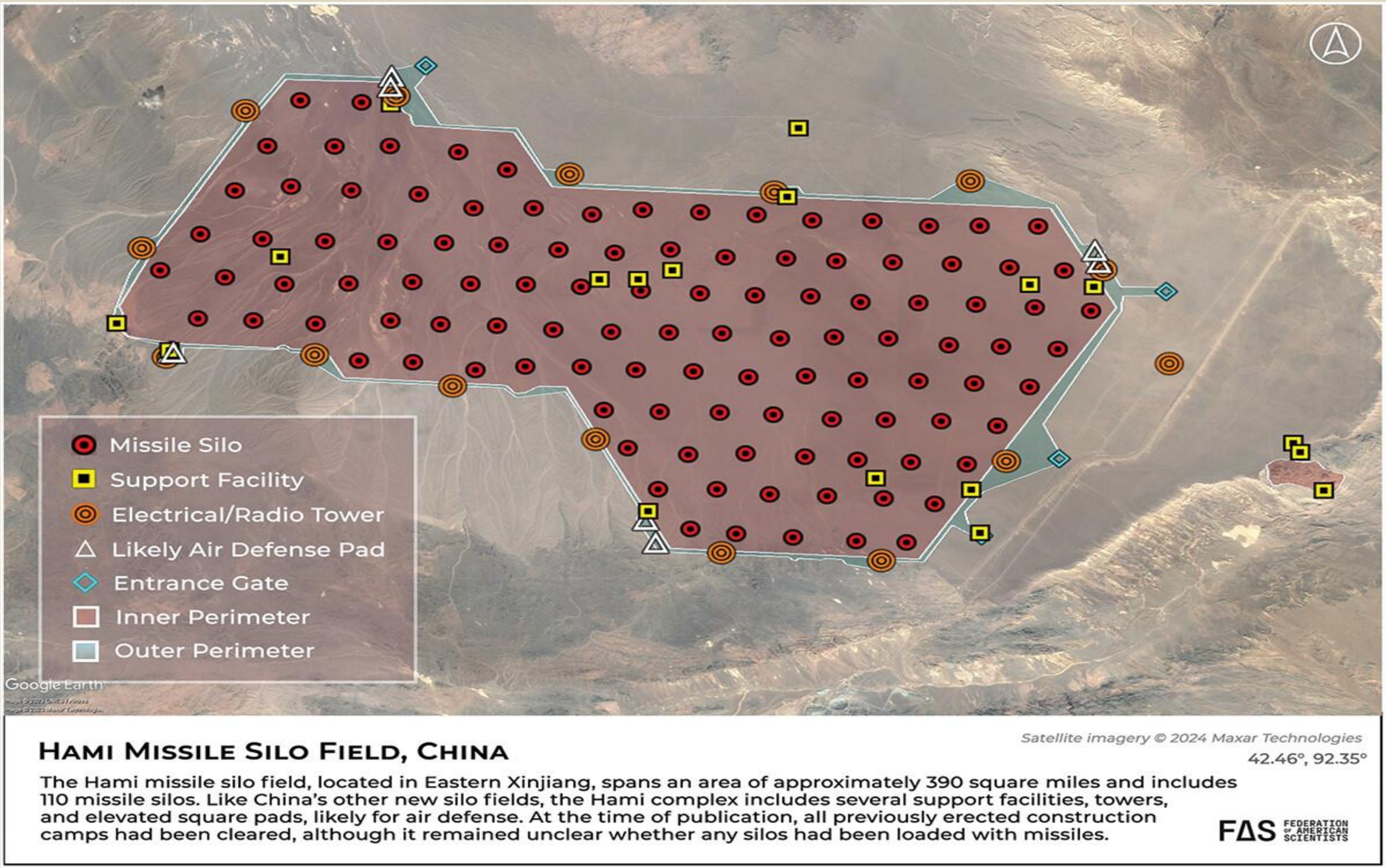
Construction of the field began in March 2020 and the last inflatable shelter was removed in February 2022, indicating that the most sensitive construction on each silo has now been completed. Construction at the Yumen field, which was first discovered by Decker Eveleth (Warrick 2021), is the furthest along out of the three silo complexes, and it is likely that the other two fields will likely follow a similar pattern and timeline.

Hami silo field

The Hami field, located in Eastern Xinjiang in the western military district, spans an area of approximately 1,028 square kilometers, roughly the same size as the Yumen field, and has also a perimeter fence around the entire complex.

The Hami silo field, which includes 110 missile silos, is at a less advanced stage of development compared to the Yumen field, with construction thought to have begun at the start of March 2021—roughly one year after Yumen. First discovered by Matt Korda (Korda and Kristensen 2021), the last of the Hami field's inflatable domes were removed in August 2022.

Like Yumen, the Hami field includes at least three security gates-one in the north (42.46306º N, 92.34831º E) and two in the east (42.34269º N, 92.79957º E and 42.25023º N, 92.73585º E)—and at least 15 surveillance or radio towers, several potential launch control centers, and several raised square platforms for air-defense forces, matching those found at the Yumen field (Figure 4). There is also a separate fenced complex—located roughly 10 kilometers from the eastern fence of the main silo field—that includes several tunnels that could potentially be intended for warhead storage.



HAMI MISSILE SILO FIELD, CHINA

The Hami missile silo field, located in Eastern Xinjiang, spans an area of approximately 390 square miles and includes 110 missile silos. Like China's other new silo fields, the Hami complex includes several support facilities, towers, and elevated square pads, likely for air defense. At the time of publication, all previously erected construction camps had been cleared, although it remained unclear whether any silos had been loaded with missiles.

Figure 4. Satellite imagery showing the location of missile silos (red circles), security gates and support facilities (yellow squares), and surveillance towers (orange circles) of the Hami field in Xinjiang, China. (Credit: Federation of American Scientists; Images: Maxar Technologies and Google Earth)

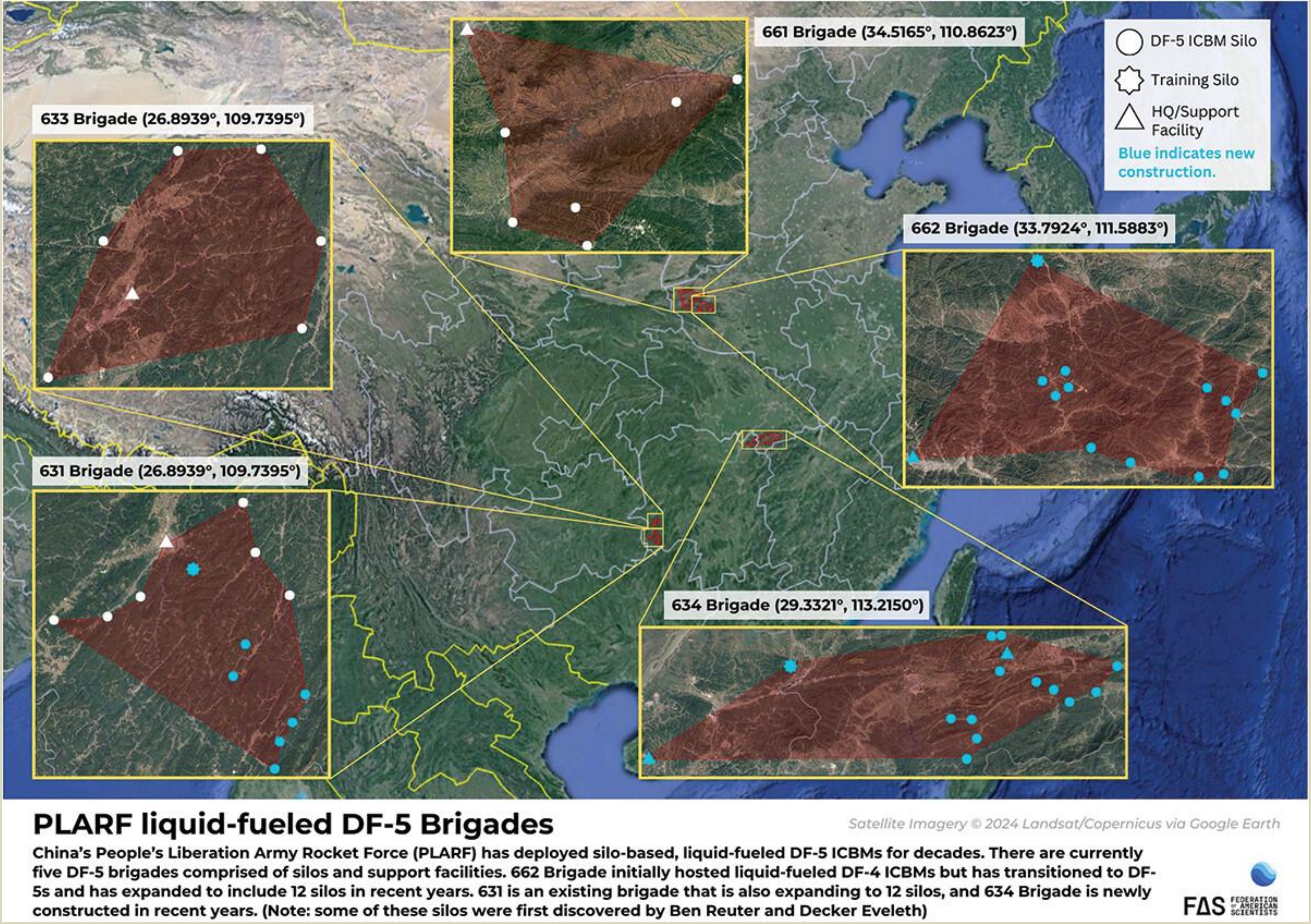
Yulin silo field

The Yulin field, located near Hanggin Banner west of Ordos, is smaller than the other two fields, measuring 832 square kilometers. It includes 90 missile silos, at least 12 support facilities, and several suspected launch control centers and air defense sites. Unlike the Hami and Yumen fields, the Yulin field does not yet have a significant fence perimeter.

Construction at the Yulin field, which was first reported by Roderick Lee (Lee 2021), began shortly after that of the Hami field (in April or May 2021), and it has a different layout than both the Yumen and Hami fields. Unlike the other two fields, the silos at the Yulin site are positioned in a slightly less grid-like pattern, although most silos are still spaced roughly three kilometers apart. In addition, the inflatable domes erected during construction at the Yulin field were all round, as opposed to the rectangular domes found at the Yumen and Hami fields, although this is likely due to logistical or construction reasons rather than a distinct difference between the silos themselves.

China's ICBM force structure

In total, these discoveries suggest that China is constructing 320 new silos for solid-fueled ICBMs across the three fields of Yumen, Hami, and Yulin, excluding the approximately 15 training silos at the Jilantai site. In addition, China is upgrading and expanding the number of silos for the liquid-fueled DF-5 ICBM and increasing the number of silos per brigade (US Department of Defense 2023, 107). This appears to include doubling the number of silos of at least two existing DF-5 brigade and adding two new brigades each with 12 silos. Once completed, based on what is observable now, this project will increase the number of DF-5 silos from 18 to 48 (Figure 5).


661 Brigade (34.5165°, 110.8623°)
633 Brigade (26.8939°, 109.7395°)
662 Brigade (33.7924°, 111.5883°)
631 Brigade (26.8939°, 109.7395°)
634 Brigade (29.3321°, 113.2150°)
○ DF-5 ICBM Silo
Training Silo
△ HQ/Support Facility
Blue indicates new construction.
FAS FEDERATION OF AMERICAN SCIENTISTS

PLARF liquid-fueled DF-5 Brigades

Satellite Imagery © 2024 Landsat/Copernicus via Google Earth

China's People's Liberation Army Rocket Force (PLARF) has deployed silo-based, liquid-fueled DF-5 ICBMs for decades. There are currently five DF-5 brigades comprised of silos and support facilities. 662 Brigade initially hosted liquid-fueled DF-4 ICBMs but has transitioned to DF-5s and has expanded to include 12 silos in recent years. 631 is an existing brigade that is also expanding to 12 silos, and 634 Brigade is newly constructed in recent years. (Note: some of these silos were first discovered by Ben Reuter and Decker Eveleth)

Figure 5. Satellite imagery showing the locations of 30 new silos under construction for the DF-5 liquid-fuel ICBM in eastern China. (Credit: Federation of American Scientists)

Combined, these construction efforts for silo-based ICBMs (in addition to new road-mobile ICBM bases) constitute the largest expansion of the Chinese nuclear arsenal ever. The 350 new Chinese silos under construction exceed the number of silo-based ICBMs operated by Russia and constitutes about three-quarters the size of the entire US ICBM force.

In addition to the construction of new ICBM facilities, there is uncertainty about how many ICBMs China currently operates. The (US Department of Defense's 2023) report about China's military and security developments assessed that, as of October 2023, China had 500 ICBM launchers with 350 missiles in its inventory (US Department of Defense 2023, 186). The previous report from 2022 listed 300 launchers with as many missiles as of the end of 2021 (US Department of Defense 2022b, 167). The sharp increase in launchers over only a two-year period suggests that the US Department of Defense is now counting all of China's new silos in its ICBM launcher estimate. However, it is unlikely that most of these new silos were loaded with missiles as of October 2023. Analysis of satellite imagery show ongoing construction at all three fields indicating that they may still be several years away from full operational capability.

In its 2023 report, the Pentagon assessed that the three new silo fields were "capable of fielding both DF-31 and DF-41 class ICBMs," but noted that China "probably began to load [a silo-based version of a DF-31-class ICBM] at its new silo fields" (US Department of Defense 2023, 104, 107).

If each new silo is filled with a single-warhead DF-31-class ICBM, the total number of warheads in China's ICBM force could potentially reach 648 warheads during the 2030s, more than twice as many as today. In addition, if all the new silos were loaded with DF-41 ICBMs (each carrying up to three warheads), then the active Chinese ICBM force could potentially carry more than 1,200 warheads once all three silo fields are completed. However, it is currently unknown how China will operate the new silos—whether they will be loaded with just silo-based DF-31-class ICBMs or a mix of DF-31As and DF-41s; whether all silos will be filled; and how many warheads each missile will carry. Regardless of what missile type ends up in each silo, the sheer number of silos will likely have a significant effect on US strike plans against China because the US targeting strategy is typically focused on holding nuclear and other military targets at risk.

At this stage of construction, it is unclear how these hundreds of new silos will alter the existing brigade structure for China's missile forces. Presently, each of China's ICBM missile brigades is responsible for six to 12 launchers. Each new missile silo field might be organized as a single brigade, but some analysts have hypothesized that the new silo fields could lead to the creation of entirely new PLARF "Bases" (each with several brigades)—an extremely rare event that has not taken place in more than 50 years (Xiu 2022, 255). For now, the Pentagon's 2023 report on China shows the Hami and Yumen missile silo fields as "Missile Brigades" in the Western Theater organized under Base 64, and the Yulin missile silo field as a "Missile Brigade" in the Northern Theater organized under Base 65 (US Department of Defense 2023, 129, 133).

Although China has deployed ICBMs in silos since the early 1980s, building missile silos on this scale is a significant shift in China's nuclear posture. The decision to do so has probably not been caused by a single event or issue but, rather, by a combination of strategic and operational objectives, including protecting the retaliatory capability against a first strike, overcoming the potential effects of adversarial missile defenses, better balancing the ICBM force between mobile and silo-based missiles, increasing China's nuclear readiness and overall nuclear strike capability to account for improvements in the Russian, Indian, and US nuclear arsenals, elevating China to a world-class military power, as well as national prestige.

Currently two versions of the DF-5 are deployed: the DF-5A (CSS-4 Mod 2) and the MIRVed DF-5B (CSS-4 Mod 3). Since 2020, the Pentagon's annual reports to Congress have noted that the DF-5B can carry up to five MIRVs (US Department of Defense 2020a, 56). We estimate that two-thirds of the DF-5s are currently equipped to carry MIRVs. In its 2023 annual report, the Pentagon indicated that a third modification with a "multi-megaton yield" warhead—known as the DF-5C—is currently being fielded (possibly in some of the new silos) and that China is "probably developing an upgrade" to the DF-5B as well (US Department of Defense 2023, 107).

In 2006, China debuted its first solid-fuel road-mobile ICBM—the DF-31 (CSS-10 Mod 1)—which had a range of about 7,200 kilometers, meaning that it could not reach the continental United States from its deployment areas in China.[2] Since then, China has iterated on its original DF-31 design, producing newer versions of the missile (the DF-31A and DF-31AG, and possibly one additional silo-based variant) with extended ranges and improved maneuverability. As of October 2023, it is assumed that these newer variants have completely replaced all the legacy DF-31s in China's arsenal.

The DF-31A (CSS-10 Mod 2) is an extended-range version of the DF-31. With a range of 11,200 kilometers, the DF-31As can reach most of the continental United States from most deployment areas in China. Each DF-31A brigade used to operate only six launchers but they have recently been upgraded to operate 12 (Eveleth 2020). In 2020, the US Air Force's National Air and Space Intelligence Center (NASIC) estimated the number of DF-31A launchers to be more than 15 (National Air and Space Intelligence Center 2020, 29). However, given the number of bases observed that possess the launchers, we estimate that China now deploys a total of about 24 DF-31As in two brigades.

In his March 2023 testimony before Congress, US STRATCOM Commander Gen. Cotton suggested that the DF-31A ICBM could carry MIRVs. This differs from NASIC's 2020 estimate that the DF-31As are equipped with only one warhead per missile, as well as from the Pentagon's 2022 annual China report, which referred to the DF-41 as "China's first road-mobile and silo-based ICBM with MIRV capability," therefore indicating that the DF-31A is not MIRV-capable (Cotton 2023; National Air and Space Intelligence Center 2020, 29; US Department of Defense 2022b, 94). It remains unclear whether the discrepancy can be attributed to updated intelligence, to an incorrect statement by the US STRATCOM commander, or to divergent assumptions by different branches of the Intelligence Community. It is also unclear how the DF-31 family could be MIRV-capable unless China has also designed a smaller-diameter MIRV warhead. Adding warheads would also reduce the range of the missile due to a heavier payload. For these reasons and in the absence of further information, we assume that the DF-31A is deployed with a single warhead.

According to the Pentagon's 2022 recent China report, Chinese media sources have suggested that a DF-31B variant might be in development; however, no further information was given about the system and it was not included in the Pentagon's 2023 China report (US Department of Defense 2022b, 65; 2023).

Since 2017, China's road-mobile ICBM modernization effort has focused on supplementing, and possibly replacing the initial DF-31 versions with the newer DF-31AG and increasing the number of associated bases. The DF-31AG's new eight-axle launcher is thought to carry basically the same missile as the DF-31A launcher but has improved off-road capabilities. The US Air Force NASIC's 2020 missile report listed the DF-31AG as having an "UNK" (unknown) number of warheads per missile in contrast to the DF-31A, which was listed with only one warhead. This suggests that the AG version could potentially have a different payload (National Air and Space Intelligence Center 2020, 29). However, for the same reasons as for the DF-31A, we assume that the DF-31AG is also deployed with a single warhead.

The Pentagon's 2022 report noted that the number of launchers in mobile ICBM units is increasing from six to 12 (US Department of Defense 2022b, 95), although this is only true for some of brigades as some new bases appear to have eight launchers.

Even though all Chinese DF-31-class ICBMs have traditionally been mobile missiles, the Pentagon's 2023 report noted that China may be currently fielding a silo-based version as well (US Department of Defense 2023, 107). This variant's missile designation is not yet known.

The next phase of China's ICBM modernization is the integration of the long-awaited DF-41 ICBM (CSS- 20) that began development back in the late 1990s. Eighteen DF-41s were mobilized for China's 70th National Day parade in October 2019; the 16 that were displayed were said to come from two brigades (New China 2019). In April 2021, the commander of US Strategic Command testified to Congress that the DF-41 "became operational [in 2020], and China has stood up at least two brigades" (Richard 2021, 7). A third base appears to have been completed and several other bases may be upgrading to receive the DF-41 as well. The number of garages at the bases indicate that there may be approximately 28 DF-41 launchers deployed.

In previous Nuclear Notebooks, we estimated that the DF-41 could carry up to three MIRVs, which the Pentagon's 2023 China report appeared to validate (US Department of Defense 2023, 107). It is unknown if all DF-41s will be equipped with MIRVs or if some will have only one warhead to maximize range. In addition to road-mobile launchers, the Pentagon says that China "appears to be considering DF-41 additional launch options, including rail-mobile and silo basing" (US Department of Defense 2022b, 65). In the Pentagon's 2023 report, the "silo basing" mode appears to refer to China's new silo fields at Yumen, Hami, and Yulin.

China also appears to be developing a new missile, known as the DF-27 (CSS-X-24), which reportedly has a range between 5,000 and 8,000 kilometers (US Department of Defense 2023, 67). This range class is somewhat redundant for the nuclear strike mission, as these distances can already be easily covered by China's longer-range ICBMs. It is therefore potentially possible that the system could ultimately be used in a conventional strike role. The Pentagon's 2023 report indicated that China "may be exploring development of conventionally-armed intercontinental range missile systems," which could potentially refer to the DF-27 (US Department of Defense 2023, 67). Reporting surrounding the DF-27 is highly unclear, however: The Pentagon's 2023 report states that the missile is "in development." Moreover, a US intelligence assessment of February 2023 notes that "land attack and antiship variants [of the DF-27] likely were fielded in limited numbers in 2022," whereas in May 2023 the *South China Morning Post* reported that the DF-27 has been in service since 2019, citing a Chinese military source (Chan 2023; US Department of Defense 2023, 67).

In June 2021, Chinese state media broadcasted videos of was rumored to be a military exercise featuring the DF-27 (Tiandao 2022), which strongly resembles the DF-26 with an attached conical hypersonic glide vehicle (HGV). This would be similar to how the DF-17 resembles a DF-16 with an attached HGV. US intelligence assessed in February 2023 that China conducted a developmental flight test of a "multirole HGV" for the DF-27, which flew for around 12 minutes and traveled approximately 2,100 kilometers (Chan 2023).

The Pentagon's 2023 report noted that "China probably is developing advanced nuclear delivery systems such as a strategic hypersonic glide vehicle and a fractional orbital bombardment (FOB) system" (US Department of Defense 2023, 67). As of October 2023, China has tested each of these systems at least once. In July 2021, China conducted a test of a new FOB system equipped with a hypersonic glide vehicle, an event described as an unprecedented achievement for a nuclear-armed country (Sevastopulo 2021). According to the Pentagon, the system came close to striking its target after flying around the world, and "demonstrated the greatest distance flown (~40,000 kilometers) and longest flight time (~100+ minutes) of any [Chinese] land-attack weapons system to date" (US Department of Defense 2022b, 65). An operational FOB/HGV system would pose challenges for missile tracking and missile defense systems, as it could theoretically orbit around the Earth and release its maneuverable payload unexpectedly with little detection time, although the US missile defense system is not intended to defend against Chinese missiles. In 2023, the Pentagon assessed that China's developmental FOB system is likely intended to have a nuclear strike role (US Department of Defense 2023, 67).

Medium- and intermediate-range ballistic missiles

For decades, the DF-21 missile family constituted China's primary regional nuclear-capable system. The DF-21A (CSS-5 Mod 2) is a two-stage, solid-fuel, road- mobile, medium-range ballistic missile (MRBM) with a range of about 2,150 kilometers (the unclassified range is 1,750 kilometers). Since 2016, China appears to have been fielding a new version of this missile, the CSS-5 Mod 6, possibly known as DF-21E. In recent years, however, several DF-21 brigades have converted—or are in the process of converting—to longer-range missile types, such as the DF-26 IRBM or the DF-31AG ICBM. For the first time, the Pentagon's 2023 report did not include the DF-21 in a nuclear role, apparently implying that all remaining DF-21s are now serving only a conventional role.

With the apparent retirement of the DF-21's nuclear mission, the regional nuclear mission is now assessed to be exclusively performed by the DF-26 (CSS-18) intermediate-range ballistic missile (IRBM). The DF-26 missile is dual-capable and launched from a six-axle road-mobile launcher. With its approximate 4,000-kilometer range, the DF-26 can target important US bases in Guam, as well as large parts of Russia and all of India.

In its annual reports, the Pentagon has stated that the DF-26 force has grown from 16 to 30 launchers in 2018 to 250 launchers with 500 missiles by October 2023 (US Department of Defense 2023, 67). Given how the Pentagon counts other Chinese systems, these estimates may also include launchers in production. We estimate that approximately 216 launchers in six brigades are now in operation, with several other brigades that may be upgrading to also operate the DF-26.

It seems unlikely that all dual-capable DF-26s serve a nuclear mission. Most of them probably serve conventional missions with nuclear warheads having been produced only for use by some of the launchers. One brigade, the 646 Brigade at Korla, is reportedly tasked with both nuclear and conventional strike missions, the first time this type of dual mission had been confirmed within a single brigade (Xiu 2022, 129, 131). To enable this dual mission, the DF-26 is reportedly capable of rapidly swapping out warheads, potentially even after the missile has been loaded onto its launch vehicle (Pollack and LaFoy 2020; US Department of Defense 2023, 67). With the DF-21's nuclear role being retired, we cautiously estimate that probably only half of the DF-26 launchers now serve a regional nuclear role.

The dual-capable role of the DF-26 raises some thorny issues about command and control and the potential for misunderstandings in a crisis. Preparations to launch—or the actual launch of—a DF-26 with a conventional warhead against a US base in the region could potentially be misinterpreted as the launch of a nuclear weapon and trigger nuclear retaliation—or even preemption. China is one of several countries (including India, Pakistan, and North Korea) that mix nuclear and conventional capability on medium- and intermediate-range ballistic missiles.

Citing Chinese defense industry publications, official media commentary, and military writings, the US Department of Defense assessed in 2023 that the DF-26 could eventually be used to "field a lower-yield warhead in the near term" (US Department of Defense 2023, 111–112). In addition, US STRATCOM Commander testified in March 2023 that China was making an "investment in lower-yield, precision systems with theater ranges" (Cotton 2023, 6). It is unclear what "lower-yield" warhead means; it is not necessarily the same as an explicitly "low-yield warhead."

Previous claims that the DF-17 may be dual-capable have not been substantiated. The Pentagon's 2022 China report noted that "[w]hile the DF-17 is primarily a conventional platform, it may be equipped with nuclear warheads" (US Department of Defense 2022b, 65). But this language was removed in the 2023 report, which only describes the DF-17 as a conventional weapon (US Department of Defense 2023). Consequently, we no longer include the DF-17 in our estimate of Chinese nuclear forces.

Submarines and sea-based ballistic missiles

China currently fields a submarine force of six second-generation Jin-class (Type 094) nuclear-powered ballistic missile submarines (SSBNs), which are based at the Yalong naval base near Longposan on Hainan Island. The two newest SSBNs are believed to be improved variants of the original Type 094 design. Some Chinese journals refer to it as the Type 094A but this has not been confirmed by either the Pentagon or the Chinese government. These SSBNs include a more prominent hump, which initially triggered some speculation as to whether they could carry up to 16 submarine-launched ballistic missiles (SLBMs), instead of the usual 12 (Suciu 2020; Sutton 2016). However, satellite images subsequently confirmed that the new subs are equipped with 12 launch tubes each (Kristensen and Korda 2020). The upgrades were later assessed to be related to sound silencing (Carlson and Wang 2023, 18).

Per the Pentagon's most recent China Military Power Report, China has equipped its Jin-class SSBNs to carry either the 7,200-kilometer range JL-2 (CSS-N-14) SLBM or the longer-range JL-3 (CSS-N-20) SLBMs, and China has likely begun replacing the JL-2s with JL-3s on a rotational basis as each submarine returns to port for routine maintenance and overhaul (US Department of Defense 2023, 55). The range of the JL-2 was sufficient to target Alaska, Guam, Hawaii, Russia, and India from waters near China, but not the continental United States—unless the submarine sailed deep into the Pacific Ocean to launch its missiles. With the JL-3's longer range of roughly 10,000 kilometers, a submarine will be able to target the northwestern parts of the continental United States from Chinese waters, but it would still not be able to target Washington, DC without sailing past northeast Japan (National Air and Space Intelligence Center 2020, 33). Unlike the JL-2, the JL-3 allegedly can deliver "multiple" warheads per missile (National Air and Space Intelligence Center 2020, 33). The People's Liberation Army Navy reportedly conducted its first test of the JL-3 in November 2018 (Gertz 2018) and appears to have conducted at least two—possibly three—additional tests since then (Chan 2020; Guo and Liu 2019).

Although the Jin-class is more advanced than China's first experimental SSBN—the single and now inoperable Xia (Type 092)—it is a noisy design compared with current US and Russian missile submarines. It is suspected that the Type 094 remains two orders of magnitude louder than the top Russian or American SSBNs (Coates 2016). For that reason, China would continue to face constraints and challenges when operating its SSBN force in a conflict (Kristensen 2009). It therefore seemed likely that China would end production after its now-completed six boats and turn its efforts to developing the quieter third-generation (Type 096) SSBN, which was scheduled to begin construction in the early 2020s. However, the Pentagon's 2023 report to Congress stated that China has continued constructing additional Jin-class SSBNs and speculates that this could be due to delays in development of the Type 096 (US Department of Defense 2023, 108).

The completion of a new construction hall at Huludao, where the People's Liberation Army Navy's submarines are built, indicated that work would soon begin on the Type 096, which is expected to be larger and heavier than the Type 094 (Sutton 2020). Satellite images show wider hull sections at Huludao, suggesting that production of a larger submarine may have started (Sutton 2021), although it is not clear whether it corresponds to a new attack submarine or the larger Type 096 SSBN. As with all new designs, the Type 096 is expected to be quieter than its predecessor. Some even believe it could be as quiet as Russia's new Borei-class SSBNs (Carlson and Wang 2023, 30), although that would be a significant technological leap for China. Some anonymous defense sources have speculated the Type 096 will carry 24 missiles (Chan 2020), but there are no public official sources confirming this information. Current and projected missile inventories seem to indicate that the SSBN will more likely carry 12 to 16 missiles. The Pentagon's 2023 report stated that the Type 096 SSBNs "will reportedly be armed with a follow-on longer range SLBM," and that these SLBMs will probably be MIRVed (US Department of Defense 2023, 55, 108).

Given that China's SSBNs are assumed to have a service life of approximately 30 to 40 years, the US Department of Defense expects that the Type 094 and Type 096 boats will operate concurrently (US Department of Defense 2023, 108). If confirmed, this could potentially result in a future fleet of eight to 10 SSBNs. All of China's six SSBNs—and several attack submarines—are based at the Yalong naval base on Hainan Island where satellite photos show expansion of piers to accommodate more submarines. Figure 6 shows that five of six SSBNs were in port in July 2023.

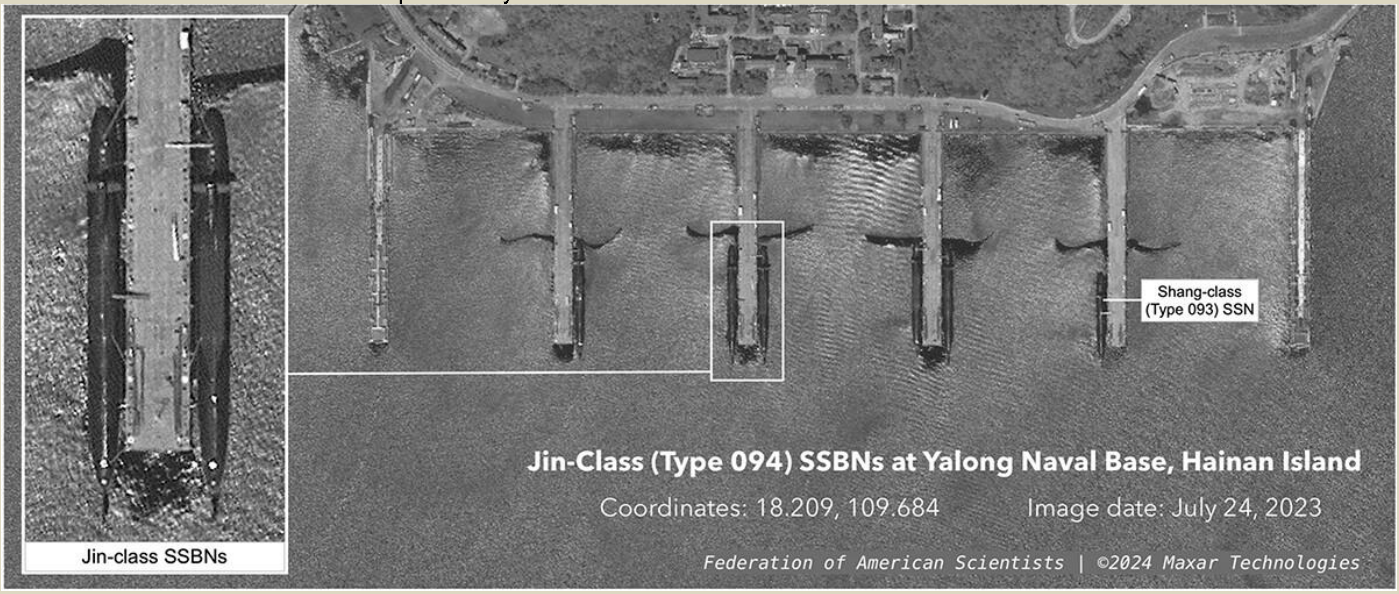

Jin-class SSBNs
Shang-class (Type 093) SSN
Jin-Class (Type 094) SSBNs at Yalong Naval Base, Hainan Island
Coordinates: 18.209, 109.684
Image date: July 24, 2023
Federation of American Scientists | ©2024 Maxar Technologies

Figure 6. Satellite imagery shows five of China's six ballistic missile submarines at the Yalong naval base on Hainan Island. Two new piers are under construction to accommodate additional submarines. (Credit: Federation of American Scientists/Maxar Technologies)

The Pentagon's 2022 report indicated that China had recently begun "near-continuous at-sea deterrence patrols with its six JIN class SSBNs" in 2021 (US Department of Defense 2022b, 96), and the 2023 report asserted that China "probably continued to conduct" these patrols throughout 2022 (US Department of Defense 2023, 108). The term "near-continuous" implies that the SSBN fleet is not on patrol all the time but that at least one boat is deployed intermittently. The term “deterrence patrol” could imply that the submarine at sea has nuclear weapons onboard, although US officials have not explicitly stated so. Giving custody of nuclear warheads to deployed submarines during peacetime would constitute a significant departure from Chinese declaratory policy and a significant change for China’s Central Military Commission, which has historically been reluctant to hand out nuclear warheads to the armed services.

To fully develop a survivable sea-based nuclear deterrent posture, China is presumably improving its command and control system to ensure reliable communication with the SSBNs when needed and prevent the crew from launching nuclear weapons without authorization. Moreover, the SSBN fleet will have to operate safely in patrol areas from where its missiles can reach intended targets. Western military officials have privately stated that the United States, Japan, Australia, and the United Kingdom “are already attempting to track the movements of China’s missile submarines as if they are fully armed and on deterrence patrols” (Torode and Lague 2019). Whenever they put to sea in this region, China’s SSBNs typically appear to be accompanied by a protection detail, including surface warships and aircraft (and possibly attack submarines) capable of tracking adversarial submarines (Torode and Lague 2019). Given the noise level of the SSBNs, it seems likely that China during conflict would keep the submarines inside a protected “bastion” in the South China Sea (US Department of Defense 2023, 108). But even with the JL-3 SLBM, the SSBNs would not be able to target the continental United States from the South China Sea. To do that, they would have to sail far north. Even if they patrolled inside the Bohai Sea, the missiles would only be able to target the northwestern parts of the continental United States—not Washington, DC.

Bombers

China developed several types of nuclear bombs and used aircraft to deliver at least 12 of the nuclear weapons that it detonated in its nuclear testing program between 1965 and 1979. Later, however, the People’s Liberation Army Air Force (PLAAF) nuclear mission became dormant as the rocket force improved and older intermediate-range bombers were unlikely to be useful or effective in the event of a nuclear conflict. Still, it is reasonable to assume that China maintained a small inventory of gravity bombs—perhaps up to 20—for potential contingency use by aircraft. Formally, however, the US Department of Defense assessed in 2017 that the “People’s Liberation Army Air Force does not currently have a nuclear mission” (US Department of Defense 2017, 61).

Coinciding with a renewed emphasis on nuclear aircraft modernization, the US Department of Defense reported in 2018 that the People’s Liberation Army Air Force “has been newly re-assigned a nuclear mission” (US Department of Defense 2018a, 75, 34). This new mission appears to be currently centered around China’s current H-6 “Badger” bomber, which may have two distinct nuclear-capable variants. The upgraded H-6K version is an extended-range version of the original H-6 bomber that has reportedly been described by Chinese media sources as a “dual nuclear-conventional bomber” (US Department of Defense 2019, 41). The H-6N is another variant that is distinct from that of the H-6K bomber through its incorporation of a nose-mounted in-flight refueling probe (Rupprecht 2019) and a modified fuselage that the US Department of Defense has stated can accommodate a nuclear-capable air-launched ballistic missile (ALBM) (US Department of Defense 2022b, 50). Notably, the airframe modification includes the removal of the bomb bay, indicating that if a legacy gravity bomb capability still existed for the PLAAF, the H-6N would not be part of that contingency mission. The ALBM appears to bear resemblance to China’s DF-21 MRBM and the nuclear-capable version has been designated by the United States as CH-AS-X-13. It is potentially possible that a conventional anti-ship variant like that of the DF-21D exists (Newdick 2022; Panda 2019). The developmental ALBM was first tested in December 2016 and at least five times by April 2018 (Panda 2019). In 2019, a US intelligence community source told *The Diplomat* that the missile would be ready for deployment by 2025 (Panda 2019). This fits the US Department of Defense’s early-2020 estimate that a “TBD [name to be determined] ALBM” is “in research & development within 10 years” (US Department of Defense 2020b, 3). The Pentagon assessed that, once complete, this nuclear ALBM will, “for the first time, provide China with a viable nuclear ‘triad’ of delivery systems dispersed across land, sea, and air forces” (US Department of Defense 2019, 67). One of the first bomber units to get an operational nuclear capability with the ALBM might be the 106th Brigade at Neixiang Air Base in the southwestern part of Henan province. The base has been modified extensively with large tunnels into a nearby mountain large enough to accommodate the H-6 bomber. Civilian video footage from October 2020 appears to show an H-6N bomber flying with the possible new ALBM just outside of Neixiang Air Base, one of China’s only airfields with an adjacent air defense site (Lee 2020a, 2020b; Rupprecht and Dominguez 2020).

To eventually replace the H-6, China is developing a stealth bomber with longer range and improved capabilities. The Pentagon asserts that the new bomber, known as H-20, will have both a nuclear and conventional capability with a range exceeding 10,000 kilometers, and may be revealed sometime during the next decade. If equipped with an aerial refueling capability, the Pentagon assesses that the bomber could potentially have intercontinental range (US Department of Defense 2023, 92).

Cruise missiles

From time to time, various US military publications have asserted somewhat vaguely that one or more of China’s cruise missiles might have nuclear capability. For example, a nuclear modernization fact sheet published by the Pentagon in connection with the release of the 2018 Nuclear Posture Review claimed, without identifying them, that China had both air-launched and sea-launched nuclear cruise missiles (US Department of Defense 2018b). The Pentagon has not substantiated this claim since. The 2023 Japanese Defense Paper, however, stated that the H-6 bombers "are believed to be capable of carrying long-range attack cruise missiles with nuclear capability" (Japanese Ministry of Defense 2023, 67). It is still unclear what this missile could be. Therefore, we continue to assess that, although China might have developed warhead designs for potential use in cruise missiles, it currently has no nuclear cruise missiles in its active stockpile. It is possible, but unconfirmed, that the future H-20 could be equipped with a nuclear cruise missile.

This research was carried out with generous contributions from New-Land Foundation, Ploughshares Fund, the Prospect Hill Foundation, Longview Philanthropy, and individual donors.

Notes

[1] Nuclear weapons are stored in central facilities under the control of the Central Military Commission. Should China come under nuclear threat, the weapons would be released to the Second Artillery Corps to enable missile brigades to go on alert and prepare to retaliate. For a description of the Chinese alerting concept, see Kristensen, (2009b). For more on warhead storage in China, see Stokes (2010). For an overview of the People's Liberation Army Rocket Force structure and organization, see Stokes (2018) and Xiu (2022). For an insightful overview of Chinese thinking about nuclear weapons and policies, see Santoro and Gromoll (2020).

[2] The "continental United States" as used here includes only the lower 48 states. US states and territories outside of the continental United States include Alaska, Hawaii, Guam, American Samoa, Puerto Rico, the US Virgin Islands, and many tiny Pacific islands.

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

Hans M. Kristensen is the director of the Nuclear Information Project with the Federation of American Scientists 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 coauthor of 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 coauthored the Nuclear Notebook since 2001.

Matt Korda is a senior research fellow for the Nuclear Information Project at the Federation of American Scientists, where he coauthors the Nuclear Notebook with Hans Kristensen and Eliana Johns. Korda is also an Associate Researcher with the Nuclear Disarmament, Arms Control and Non-proliferation Program at the Stockholm International Peace Research Institute (SIPRI). Previously, he worked for the arms Control, Disarmament, and WMD Non-Proliferation Center at NATO headquarters in Brussels. Korda's research and open-source discoveries about nuclear weapons have made headlines across the globe, and his work is regularly used by governments, policymakers, academics, journalists, and the broader public in order to challenge assumptions and improve accountability about nuclear arsenals and trends. He received his MA in International Peace and Security from the Department of War Studies at King's College London.

Eliana Johns, née 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, Johns 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. Johns graduated with her bachelor's in political science with minors in Music and Korean from the University of Maryland, Baltimore County (UMBC).

Mackenzie Knight is a Herbert Scoville Jr. Peace Fellow on the Nuclear Information Project at the Federation of American Scientists. Previously, Knight worked as a Policy and Communications Intern at the Arms Control Association, as a summer fellow with the James Martin Center for Nonproliferation Studies (CNS), as an Analyst Intern with Shephard Media in London, and most recently as a Graduate Research Assistant at CNS while obtaining her master's degree in Nonproliferation and Terrorism Studies from the Middlebury Institute of International Studies at Monterey. She received bachelor's degrees in Middle Eastern Languages and Cultures and Policy and Intelligence Analysis from Indiana University.

EDITOR'S COMMENT: According to what Bloomberg News describes as a US intelligence report, Chinese authorities discovered that some of their missiles' fuel tanks were filled with water – and that this was a marquee example of corruption whose unraveling led to Chinese President Xi's recent military purge. Bloomberg reported that it got the information from unnamed people who were "familiar with" a US intelligence assessment and that those US sources also said that new Xinjiang missile field silos were fitted with lids that were not installed properly and would not work – taken as another example of corruption. How can one tell from a distance if it is water or fuel? How can they say that lids are dysfunctional? Most probably, fake news with a touch of US propaganda for national consumption! The absurdity of American generals fearing Beijing's military is back!

Nuclear deterrence is the existential threat, not the nuclear ban treaty

By Ivana Nikolić Hughes, Xanthe Hall, Ira Helfand, Mays Smithwick

Source: https://thebulletin.org/2024/01/nuclear-deterrence-is-the-existential-threat-not-the-nuclear-ban-treaty/

Antinuclear activist march to mark the second anniversary of the entry into force of the Treaty on the Prohibition of Nuclear Weapons (TPNW) in New York, January 20, 2023. - The TPNW, the first legally binding international agreement to prohibit nuclear weapons, entered into force on January 22, 2021. (Photo by KENA BETANCUR/AFP via Getty Images)

Jan 22 – In a deeply misguided article in this publication, Zachary Kallenborn contends that the Treaty on the Prohibition of Nuclear Weapons (TPNW) is a threat to humanity. To build this narrative, Kallenborn does not simply present nuclear deterrence as a stable and useful framework for avoiding conventional wars. Rather, he goes beyond the common deterrence arguments to assert that nuclear weapons restrain world wars, which allows nations to work together on addressing existential threats. Nothing could be further from the truth.

Nuclear deterrence is a myth

Nuclear deterrence involves a nation state maintaining a believable threat of retaliation to deter an adversary's attack. This relies on demonstrations of the readiness and the capacity to use nuclear weapons—a highly dangerous form of bluff which, in turn, makes those targeted increase their hardware and rhetoric. We are currently witnessing this kind of escalation among several nuclear weapon possessor states, which could result in nuclear war.

Nuclear deterrence rests on decision makers always behaving rationally; even if different states and parties weigh values, threats, and possible consequences in the same way, individual leaders do not always behave rationally. During the closing weeks of his presidency, Richard Nixon's behavior was so erratic that James Schlesinger, the Secretary of Defense, instructed the Joint Chiefs of Staff to ignore any order to use nuclear weapons unless it was countersigned by himself and Secretary of State Henry Kissinger. Schlesinger had no authority to do this, and it is not clear the instructions would have been carried out if Nixon had ordered the use of nuclear weapons. After his electoral defeat in 2020, Donald Trump's behavior was so bizarre that it triggered similar concerns in General Milley, the chair of the Joint Chiefs of Staff. But troubling behavior is not solely the province of US leaders. Boris Yeltsin, for example, had an alcohol problem, and the recent nuclear rhetoric from Russian leaders has been worrisome at best.

All leaders are capable of making bad decisions, and the stress of a military crisis, during which decisions might have to be made with limited or faulty intelligence and in a very compressed time frame, increases the chance that a leader would abandon the rational position that nuclear weapons should never be used and make a mistake that would be fatal for humanity.

The overarching assumption of nuclear deterrence is that the existence of nuclear weapons can continue indefinitely without anything ever going wrong, leading to the theory's most concerning aspect: lack of plan B. In the words of Melissa Parke, the executive director of the International Campaign to Abolish Nuclear Weapons (ICAN), "Nuclear deterrence may well work until the day it doesn't." What happens when nuclear deterrence fails? The problem is that it is impossible to create a plan for that day. The International Committee for the Red Cross (ICRC) has been warning since 1945 that there can be no adequate humanitarian response even to a single nuclear weapon explosion, let alone to the hundreds or thousands that could be used in today's conflicts. Contrary to the unrealistic logic of deterrence, many medical organizations and other civil society groups, including those that we are a part of, have been arguing, often for decades, that prevention is the only viable option.

The argument that nuclear deterrence has kept the world safe is simply wrong. Numerous close calls and near misses strongly suggest otherwise. From scholarly analyses to a simple list of such known incidents in the United States alone, the message is clear—we have been lucky, rather than smart. As UN Secretary General António Guterres stated at the 10th Nuclear Non-Proliferation Treaty Review Conference in 2022, "Luck is not a strategy."

Close calls and near misses haven't led to nuclear war yet. But nuclear weapons have been the cause of human suffering for decades. In addition to the horrors of what happened in Hiroshima and Nagasaki, nuclear weapons have already harmed millions of people in the process of being developed and tested. Devastatingly, governments of nuclear weapon possessors have harmed their own people, such as the people of Kazakhstan and the United States, and those whose care they've been entrusted with, such as the Indigenous people of Australia, the Marshall Islands, Kiribati, and Maohi Nui (French Polynesia). These humanitarian consequences have provided the impetus for action that is embedded in Articles 6 and 7 of the TPNW and a recently adopted resolution on nuclear justice in the UN General Assembly. Just in 2022, the global expenditure on nuclear weapons was $83 billion, an amount that could have been better spent on social programs and other needs. We are all harmed when societal needs are ignored in favor of weapons of mass destruction.

What the world needs to address other existential threats

Kallenborn is right that the world faces other global threats. And although some of them—just like nuclear weapons—have the potential to wipe out humanity, including a large asteroid impact or an emerging infectious disease, what is thoroughly different about nuclear weapons is that we have created them, and we can therefore eliminate them.

The majority of states in the world have access to the knowledge and very many have access to the means to build nuclear weapons, but they don't. These states refrain from doing so because they see no value in having nuclear weapons. On the contrary, they recognize the threat that possessing nuclear weapons poses. Moreover, a verifiable process for ensuring that existing nuclear weapons have been eliminated and that new ones are not developed would have to be put in place as part of any nuclear abolition plan, including through the TPNW, with a competent international authority put in charge of this key process. Significant work on verification is ongoing through the International Monitoring System of the Comprehensive Test Ban Treaty Organization (IMS of CTBTO), the International Atomic Energy Agency (IAEA), and the TPNW's own Scientific Advisory Group (SAG), which was formed last year.

The elimination of all nuclear weapons and a concurrent international system of verification and monitoring would result in a far better scenario than where we find ourselves today. Even a hypothetical situation in which a nation cheats to make a few weapons following their total elimination would be far less dangerous than where we are today with a current global arsenal of approximately 12,500 warheads, which could destroy the world over and over again.

Climate change is—like nuclear war—an existential threat of great urgency, as its effects are devastating and could make entire regions of the planet uninhabitable. Added to this, climate change is already exacerbating conflicts due to the increase in food scarcity and natural disasters that displace populations and paralyze economies. These impacts will get worse with time. Combined with nuclear weapons, this regional and global instability arguably poses the greatest threat to humanity, as the *Bulletin* has repeatedly made clear with time adjustments to its Doomsday Clock. At the time of the writing of this article, the clock stands at just 90 seconds to midnight.

Nuclear winter refers to the fact that even limited regional nuclear war, such as between India and Pakistan, will trigger global climate disruption and catastrophic famine. Kallenborn alludes to this potential threat but tries to minimize the importance of nuclear winter studies by stating that there is a significant difference of opinion about this danger in the scientific community. He goes even further to warn us that such studies are motivated by "political biases and agendas." Indeed, the one recent study from the Los

Alamos Laboratory that minimizes the extent of climate change due to nuclear war may well be motivated by an agenda other than science; this study has been thoroughly rebutted. Incredibly, Kallenborn proposes that the response to the threat of global nuclear famine should be stockpiling enough food to feed billions of people for several years and cites the utterly inappropriate example of the 1948 Berlin airlift as the kind of effort needed.

Global cooperation, not threats of annihilation, must be the basis for addressing all existential threats. We live on a beautiful planet with a host of human-made and natural challenges that require us to move away from us vs. them attitudes and instead collectively cooperate to achieve global security for all humans in our common home. To this end, we must not normalize violent conflict on battlefields and threats to destroy one another. Instead, competition between states should be reserved for athletic fields and courts, business and commerce, and pursuit of scientific and artistic achievements.

It is useless for the sheep to pass resolutions in favour of vegetarianism, while the wolf remains of a different opinion.
~ William Inge

Editor's comment ▶

The truth about the nuclear ban treaty

Arguably, the biggest falsehoods that Kallenborn promulgates revolve around the TPNW itself. For one, the treaty is not a quick fix that will lead to a sudden abolition of nuclear weapons in a vacuum. Rather, the treaty is an instrument that establishes a legal norm, which will lead to a process resulting in the elimination of nuclear weapons. The path that needs to be taken to reach this goal will, in itself, address the problem of great powers' conflict and regional conflicts, as well as safe disarmament.

It is commonly claimed that nuclear deterrence has prevented a nuclear war from occurring. But we came to the brink of nuclear war several times during the Cold War, including during the Cuban Missile Crisis, and this claim about deterrence completely ignores the role of international agreements in de-escalating tensions and preventing a nuclear conflict. The process of creating instruments of arms control and disarmament establishes structures for regaining trust and verification. In this regard, the last decade has seen an erosion of the disarmament architecture, with the exception of the TPNW. As it stands, we may soon have no more brakes on the arms race.

As Kallenborn himself states, "the best way to reduce the risks of nuclear war is to ensure it never happens in the first place." That precisely is the intention and the motivation of all of the 122 states that negotiated the TPNW in 2017 and an even larger number of states that have been voting in support of the treaty at the UN General Assembly every year since. The nine nuclear weapon possessors and their allies are the ones that need to prove that there is a convincing reason, or indeed any right, to hold the rest of the world hostage to their nuclear weapons. Kallenborn asserts that if nuclear weapons are eliminated, the great powers will launch World War III. In fact, the process of eliminating these weapons will create the conditions needed for a more cooperative relationship among the great powers, by removing the most dangerous issue that divides them.

The truth about the nuclear ban is spelled out in the text of the treaty itself, but also in the recently adopted Declaration that was the result of the Second Meeting of States Parties to the TPNW, held in New York late last year. The Declaration highlights the raison d'être for the ban, as well as the way forward.

Abolition is the only reasonable path

Nuclear weapons and current nuclear weapon policies are, in the words of the late peace and nuclear disarmament activist Daniel Ellsberg, "dizzyingly insane and immoral." Aiming solely for reducing the harm or the possibility of harm that nuclear weapons could cause, rather than being a part of a process to abolish them, is simply not enough. Imagine if the opponents of slavery had aimed not to abolish slavery, but to make life a bit better for the enslaved people? Ultimately, the question of nuclear abolition is not just a moral one, but an existential one. If we don't abolish nuclear weapons, they will abolish us. John F. Kennedy stated this at the United Nations more than 60 years ago. Let's heed his words sooner rather than later and, critically, before it is too late.

●▶ **Acknowledgements:** *Read about the individuals who contributed significantly to the writing of this article at the source's URL.*

Ivana Nikolić Hughes is president of the Nuclear Age Peace Foundation and a Senior Lecturer in Chemistry at Columbia University. She is a member of the Scientific Advisory Group to the Treaty on the Prohibition of Nuclear Weapons. She holds a B.S. with Honors from Caltech and a Ph.D. from Stanford University, both in chemical engineering. Her work on ascertaining the radiological conditions in the Marshall Islands has been covered widely, including by the *Los Angeles Times*. Her writing has appeared in the *Bulletin of Atomic Scientists*, *The Hill*, *Scientific American*, *The Diplomat*, Truthout, Common Dreams, Transcend Media Service, and elsewhere.
Xanthe Hall is co-director, disarmament expert and international campaigner for the German affiliate of International Physicians for the Prevention of Nuclear War (IPPNW). She is also founding member of the German affiliate of ICAN, the International Campaign to Abolish Nuclear Weapons, winner of the Nobel Peace Prize 2017.
Ira Helfand, MD, is a member of the International Steering Group of the International Campaign to Abolish Nuclear Weapons (ICAN), the recipient of the 2017 Nobel Peace Prize. He is also immediate past president of the International Physicians for the Prevention of Nuclear War (IPPNW), the founding partner of ICAN and itself the recipient of the 1985 Nobel Peace Prize. He is also co-founder and past president of Physicians for Social Responsibility, IPPNW's US affiliate.
Mays Smithwick is a nuclear abolitionist and an anticolonial activist. Mays completed their undergraduate degree in the Global Studies department at Eugene Lang College, the New School for Liberal Arts in 2019, with a double minor in Philosophy and Cultural Studies. In 2023, they received a Master of Arts degree from the Department of Experimental Humanities and Social Engagement at NYU.

A moment of historic danger: It is *still* 90 seconds to midnight

23 January 2024 Doomsday Clock Statement
Source: https://thebulletin.org/doomsday-clock/current-time/

Founded in 1945 by Albert Einstein, J. Robert Oppenheimer, and University of Chicago scientists who helped develop the first atomic weapons in the Manhattan Project, the Bulletin of the Atomic Scientists *created the Doomsday Clock two years later, using the imagery of apocalypse (midnight) and the contemporary idiom of nuclear explosion (countdown to zero) to convey threats to humanity and the planet. The Doomsday Clock is set every year by the* Bulletin*'s Science and Security Board in consultation with its Board of Sponsors, which includes nine Nobel laureates. The Clock has become a universally recognized indicator of the world's vulnerability to global catastrophe caused by man-made technologies.*

Bulletin of the Atomic Scientists
IT IS 90 SECONDS TO MIDNIGHT

A moment of historic danger: It is *still* 90 seconds to midnight

Ominous trends continue to point the world toward global catastrophe. The war in Ukraine and the widespread and growing reliance on nuclear weapons increase the risk of nuclear escalation. China, Russia, and the United States are all spending huge sums to expand or modernize their nuclear arsenals, adding to the ever-present danger of nuclear war through mistake or miscalculation.

In 2023, Earth experienced its hottest year on record, and massive floods, wildfires, and other climate-related disasters affected millions of people around the world. Meanwhile, rapid and worrisome developments in the life sciences and other disruptive technologies accelerated, while governments made only feeble efforts to control them.

The members of the Science and Security Board have been deeply worried about the deteriorating state of the world. That is why we set the Doomsday Clock at two minutes to midnight in 2019 and at 100 seconds to midnight in 2022. Last year, we expressed our heightened concern by moving the Clock to 90 seconds to midnight—the closest to global catastrophe it has ever been—in large part because of Russian threats to use nuclear weapons in the war in Ukraine.

Today, we once again set the Doomsday Clock at 90 seconds to midnight because humanity continues to face an unprecedented level of danger. Our decision should not be taken as a sign that the international security situation has eased. Instead, leaders and citizens around the world should take this statement as a stark warning and respond urgently, as if today were the most dangerous moment in modern history. Because it may well be.

But the world can be made safer. The Clock can move away from midnight. As we wrote last year, “In this time of unprecedented global danger, concerted action is required, and every second counts.” That is just as true today.

The many dimensions of nuclear threat

A durable end to Russia’s war in Ukraine seems distant, and the use of nuclear weapons by Russia in that conflict remains a serious possibility. In February 2023, Russian President Vladimir Putin announced his decision to “suspend” the New Strategic Arms Reduction Treaty (New START). In March, he announced the deployment of tactical nuclear weapons in Belarus. In June, Sergei Karaganov, an advisor to Putin, urged Moscow to consider launching limited nuclear strikes on Western Europe as a way to bring the war in Ukraine to a favorable conclusion. In October, Russia’s Duma voted to withdraw Moscow's ratification of the Comprehensive Nuclear Test Ban Treaty, as the US Senate continued to refuse even to debate ratification.

Nuclear spending programs in the three largest nuclear powers—China, Russia, and the United States—threaten to trigger a three-way nuclear arms race as the world’s arms control architecture collapses. Russia and China are expanding their nuclear capabilities, and pressure mounts in Washington for the United States to respond in kind.

Meanwhile, other potential nuclear crises fester. Iran continues to enrich uranium to close to weapons grade while stonewalling the International Atomic Energy Agency on key issues. Efforts to reinstate an Iran nuclear deal appear unlikely to succeed, and North Korea continues building nuclear weapons and long-range missiles. Nuclear expansion in Pakistan and India continues without pause or restraint.

And the war in Gaza between Israel and Hamas has the potential to escalate into a wider Middle Eastern conflict that could pose unpredictable threats, regionally and globally.

An ominous climate change outlook

The world in 2023 entered uncharted territory as it suffered its hottest year on record and global greenhouse gas emissions continued to rise. Both global and North Atlantic sea-surface temperatures broke records, and Antarctic sea ice reached its lowest daily extent since the advent of satellite data. The world already risks exceeding a goal of the Paris climate agreement—a temperature increase of no more than 1.5 degrees Celsius above pre-industrial levels—because of insufficient commitments to reduce greenhouse gas emissions and insufficient implementation of commitments already made. To halt further warming, the world must achieve net zero carbon dioxide emissions.

The world invested a record-breaking $1.7 trillion in clean energy in 2023, and countries representing half the world’s gross domestic product pledged to triple their renewable energy capacity by 2030. Offsetting this, however, were fossil fuel investments of nearly $1 trillion. In short, current efforts to reduce greenhouse gas emissions are grossly insufficient to avoid dangerous human and economic impacts from climate change, which disproportionately affect the poorest people in the world. Barring a marked increase in efforts, the toll of human suffering from climate disruption will inexorably mount.

Evolving biological threats

The revolution in life sciences and associated technologies continued to expand in scope last year, including, especially, the increased sophistication and efficiency of genetic engineering technologies. We highlight one issue of special concern: The convergence of emerging artificial intelligence tools and biological technologies may radically empower individuals to misuse biology. In October, US President Joe Biden signed an executive order on “safe, secure, and trustworthy AI” that calls for protection “against the risks of using AI to engineer dangerous biological materials by developing strong new standards for biological synthesis screening.” Though a useful step, the order is not legally binding. The concern is that large language models enable individuals who otherwise lack sufficient know-how to identify, acquire, and deploy biological agents that would harm large numbers of humans, animals, plants, and other elements of the environment. Reinvigorated efforts this past year in the United States to revise and strengthen oversight of risky life science research are useful, but much more is needed.

The dangers of AI

One of the most significant technological developments in the last year involved the dramatic advance of generative artificial intelligence. The apparent sophistication of chatbots based on large language models, such as ChatGPT, led some respected experts to express concern about existential risks arising from further rapid advancements in the field. But others argue that claims about existential risk distract from the real and immediate threats that AI poses today (see, for example, "Evolving biological threats" above). Regardless, AI is a paradigmatic disruptive technology; recent efforts at global governance of AI should be expanded.

AI has great potential to magnify disinformation and corrupt the information environment on which democracy depends. AI-enabled disinformation efforts could be a factor that prevents the world from dealing effectively with nuclear risks, pandemics, and climate change.

Military uses of AI are accelerating. Extensive use of AI is already occurring in intelligence, surveillance, reconnaissance, simulation, and training. Of particular concern are lethal autonomous weapons, which identify and destroy targets without human intervention. Decisions to put AI in control of important physical systems—in particular, nuclear weapons—could indeed pose a direct existential threat to humanity.

Fortunately, many countries are recognizing the importance of regulating AI and are beginning to take steps to reduce the potential for harm. These initial steps include a proposed regulatory framework by the European Union, an executive order by President Biden, an international declaration to address AI risks, and the formation of a new UN advisory body. But these are only tiny steps; much more must be done to institute effective rules and norms, despite the daunting challenges involved in governing artificial intelligence.

How to turn back the Clock

Everyone on Earth has an interest in reducing the likelihood of global catastrophe from nuclear weapons, climate change, advances in the life sciences, disruptive technologies, and the widespread corruption of the world's information ecosystem. These threats, singularly and as they interact, are of such a character and magnitude that no one nation or leader can bring them under control. That is the task of leaders and nations working together in the shared belief that common threats demand common action. As the first step, and despite their profound disagreements, three of the world's leading powers—the United States, China, and Russia—should commence serious dialogue about each of the global threats outlined here. At the highest levels, these three countries need to take responsibility for the existential danger the world now faces. They have the capacity to pull the world back from the brink of catastrophe. They should do so, with clarity and courage, and without delay.

It's 90 seconds to midnight.

Learn more about how each of the *Bulletin*'s areas of concern contributed to the setting of the Doomsday Clock this year:

Nuclear Risk

The last year was characterized by fraught relations among the world's great powers, who were engaged in vigorous nuclear modernization programs as the nuclear arms control regime continued to collapse. Read more...

Climate Change

Extreme climate impacts seen around the world and the continued rise of greenhouse gas emissions are cause for much concern. But the clean-energy transition has also gathered momentum. Read more...

Biological Threats

The revolution in the life sciences and technologies like AI continues to accelerate, posing increased threats of both accidental and deliberate misuse of biology. Read more...

Disruptive Technologies

Dramatic advances in generative artificial intelligence sparked debate about its potential existential risk, but it is clear that AI-enabled corruption of the information environment may threaten our capacity to address other urgent threats. Read more...

About the *Bulletin of the Atomic Scientists*

At our core, the *Bulletin of the Atomic Scientists* is a media organization, publishing a free-access website and a bimonthly magazine. But we are much more. The *Bulletin*'s website, iconic Doomsday Clock, and regular events equip the public, policy makers, and scientists with the information needed to reduce man-made threats to our existence. The *Bulletin* focuses on three main areas: nuclear risk, climate change, and disruptive technologies, including developments in biotechnology. What connects these topics is a driving belief that because humans created them, we can control them.

The *Bulletin* is an independent, nonprofit 501(c)(3) organization. We gather the most informed and influential voices tracking man-made threats and bring their innovative thinking to a global audience. We apply intellectual rigor to the conversation and do not shrink from alarming truths.

The *Bulletin* has many audiences: the general public, which will ultimately benefit or suffer from scientific breakthroughs; policy makers, whose duty is to harness those breakthroughs for good; and the scientists themselves, who produce those technological advances and thus bear a special responsibility. Our community is international, with half of our website visitors coming from outside the United States. It is also young. Half are under the age of 35.

International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

EXPLOSIVE NEWS

Leveraging Artificial Intelligence in Explosives, Narcotic Detection

Source: https://www.homelandsecuritynewswire.com/dr20231227-leveraging-artificial-intelligence-in-explosives-narcotic-detection

Dec 27 – Harnessing the power and possibilities of artificial intelligence (AI) and machine learning (ML) and applying these emerging capabilities to the Department of Homeland Security (DHS) mission has been, and will continue to be, a high priority for the Science and Technology Directorate (S&T). One way S&T is demonstrating this commitment to applying emerging technologies to pressing national threats is by investing in the development of AI/ML technologies. Specifically in this case, the funding is directed at AI/ML that could soon be used to identify dangerous compounds, like those found in explosives and narcotics.

When the DHS Small Business Innovation Research (SBIR) Program released a solicitation back in FY2020, under the topic "Machine Learning Module for Detection Technologies," the goal was to develop innovative solutions that would ultimately provide DHS operational components with an enhanced ability to identify new threats at aviation checkpoints. In the spring of 2021, following their 6-month Phase I awards to demonstrate concept feasibility, Physical Sciences Inc. (PSI) and Alakai Defense Systems, Inc. (Alakai) were each awarded a $1 million, 24-month SBIR Phase II contract. These awards further lean into the ultimate goal of developing advanced AI/ML-based detection algorithms that can shorten the timeline for deployment of capabilities able to identify threats in the field. The research and development (R&D) being done is important because it addresses a capability gap in the detection of certain types of new threats. S&T believes that AI/ML solutions can help close that gap.

According to Thoi Nguyen, program manager for S&T's Next Generation Explosives Trace Detection Program, "When the intel, special ops, or law enforcement communities find a new threat, maybe a new explosive compound, the threat is validated and prioritized according to urgency levels. DHS S&T is then tasked to develop an R&D solution to detect and identify the threat. Once the solution is tested, evaluated, and verified that it meets DHS detection requirements, DHS Components go through a lengthy DOTMLPF (Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities) process to acquire and deploy the solution. At the end of this process, the chemical 'signature' of the threat is uploaded to DHS equipment at airport checkpoints."

However, adding a new compound to the existing identification library of threat compounds historically has been a slow, meticulous, and labor-intensive process. This can result in a capability gap for updating the database.

The challenge S&T posed with this funding award is to see if an AI/ML solution can significantly expedite the process of updating a detection library, without the intensive human labor.

One of the ways that dangerous compounds are identified at checkpoints is with Raman Spectroscopy. This chemical analytical technique fires a laser at a vaporized and ionized sample that was swabbed from a traveler, or into an object like a closed bottle of liquid. The laser will excite the molecules it encounters in the target, causing them to vibrate. Every type of molecule has its own distinct vibrational frequency. The spectrometer will detect those vibrational frequencies and chart them on a graph. The chemical signature is determined by where specific peaks are found on the graph and the intensity, height, and width of those peaks. Then the system searches the chemical signature library to find a match. If the sample matches an explosive in the database, the alarm is sounded.

So, what's the problem? "The bottleneck is not in the intel process, the bottleneck is in the R&D process and how to add that new threat intel, the new chemical signature, into the library so we can catch the bad guys," said Nguyen. "That's where the AI/ML that our small business partners are developing fits into the equation."

"We love small businesses because they're innovative and nimble," said SBIR Program Director Dusty Lang. "The SBIR program allows us to absorb the risk by funding multiple Phase I proposals to explore feasibility, then move forward to Phase II with the best solutions for DHS needs."

Traditionally, when a new threat compound is introduced into the library, scientists and contractors are brought in to manually create a new classification or channel for it. At that point, the tedious work to enter all the spectrographic characteristics of the chemical into the library begins. The programing of the chemical traits for the channel must be extremely precise to ensure they get the highest Probability of Detection (PD) and the lowest Probability of False Alarm (PFA) when the library is queried with a sample at a checkpoint.

One of the complicating factors for achieving high PD and low PFA is that the software analyzing the compound must be able to see through the background noise in the sample and identify the compound for what it really is.

"For example, pure TNT from a lab may appear different from TNT in a real-world scenario because there may be additives to the TNT, or there may be other environmental interference. So, even though it might have spectrographic peaks at the right places, they might be somewhat obscured by these other excited molecules and their signatures. If you're creating a TNT channel, we would have to account for myriad factors. That's what takes so much time and that's where accuracy is so important. It has to be calibrated perfectly. What we're trying to do here with the AI and the ML is that we want to bypass that slow process."

The first part of that bypass is training the AI to recognize a specific compound. However, the AI can't teach itself. It still needs to be taught how to do it. The ML-based detection algorithm starts as a blank sheet, and it must be taught which peaks on the graph represent which chemicals. "It's like teaching a child what sugar tastes like," said Nguyen. "When you taste this, that is sugar. That's what we call sweet. And this is sugar with a little bit of lemon. You taste the sour lemon, but it's still sugar. It's the same thing with teaching the AI to not get confused by the background noise."

In Nguyen's example, the important thing for the child to understand is that the sample is still sugar, and the lemon is just an additive. In the explosive detection world, that lemon might be a fuel added to TNT to make it more powerful. Making sure that the explosives detection algorithm is smart enough to determine that the TNT is mixed with another fuel compound is incredibly important.

That brings us to the second part, which is validation. Once the AI is taught the signature characteristics of the compound, and potential noise distractions have been accounted for, the AI is evaluated for accuracy by running tests designed to trick it. Chemicals are added to the original compound in attempts to shield or mask the spectrographic signature behind other noise.

Nguyen emphasizes the importance of this part, adding that, "We don't just trust AI completely. We say, 'trust, but verify,' to see whether or not the alarm that was just triggered complies with our understanding of how the vibration of the molecules we are testing should present themselves."

For a limited set of explosives, S&T demonstrated that the AI/ML solution identified explosives with very high PD, yet low PFA—a major success by itself. Even more remarkable is the way that this AI/ML solution has closed the critical time capability gap.

"What traditionally can take as many as one to two years, the AI/ML that our partners developed can now learn, classify, and upload new threats to the library in a matter of days or weeks," said Nguyen. "That has significant real-world impact. And I want to make sure that we give credit to SBIR, because without their collaboration, funding and support, this project would never have happened."

SBIR's Lang added, "These two companies, PSI and Alakai, demonstrate the impact small business can have and why we are always working to strengthen the SBIR reach and support. It is very rewarding to be able to work with program managers like Thoi to facilitate the connections of ideas and needs."

This round of Phase II funding from the SBIR Program resulted in confirmation that AI/ML has a place in the future of explosive detection. The shortened deployment cycle to chemical libraries in the field, coupled with maintaining the high PD and low PFA, is something that human hands can't match. That's the power of trustworthy AI/ML and that's what S&T is looking to leverage to further secure the nation.

In terms of looking back on the work that has been developed under the program, Nguyen finished up stating, "It was a success beyond our imagination."

In the future, AI/ML modules will be tested and evaluated at the U.S. Army's Chemical Biological Center. The goal there will be to determine compatibility between three types of Raman Spectrometers and their interoperative capabilities.

IEDs: Live Agent and Delivery System Developments

By Fritz Pfeiffer

Source: https://nct-cbnw.com/ieds-live-agent-and-delivery-system-developments/

Researcher at the *Büro für Umweltgeologie & Sicherheitsforschung* in Germany Fritz Pfeiffer discusses results from recent IED trials with simulants and the challenges they pose. Nowadays we frequently observe less than satisfactory stories on the illicit availability and use of live chemical agents. Despite OPCW goals being reached, there is not much space for optimism of any kind. Enormous amounts of dumped chemical munitions in various states of decay still offer sources to profit from.

New techniques of preparing microencapsulated agents or modifications of existing delivery systems are the current concern and research issue at the *Büro für Umweltgeologie & Sicherheitsforschung / Office for Environmental Geology & Security Research* (BfUS). Although a sensitive topic, we can reveal some results from trials with simulants and the challenges they pose.

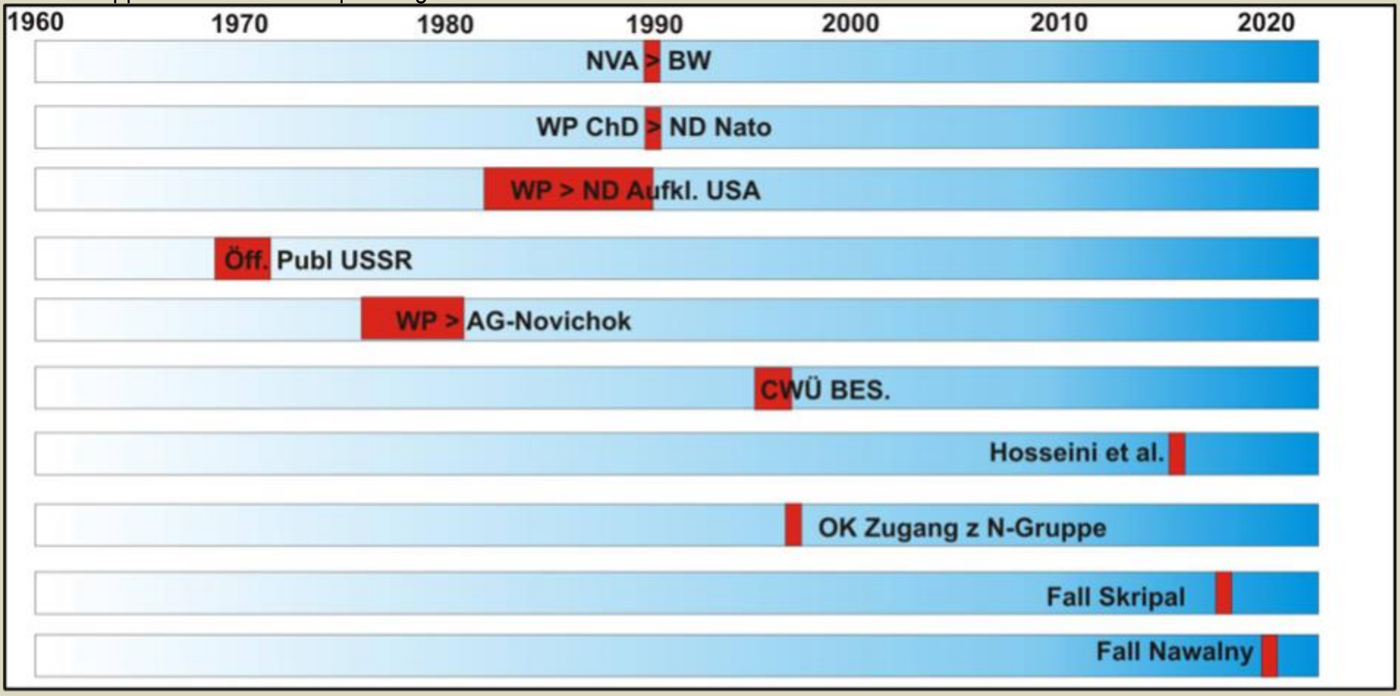
For the targets affected, the ease of negating protective envelopes is evident as reasonably small improvised explosive devices (IEDs) can penetrate up to 500 mm of reinforced concrete, or 250 mm Rolle Homogenous Armor (RHA), and still deliver significant amounts of agent into small volumes up to 30m³.

Equally disturbing are simple homemade subtypes of shaped charges with significantly smaller maximum penetration, but capability to deliver comparatively large volumes of agents. They can contaminate up to 100 m³, with excessive contamination both on and behind the point of entry.

Live Agent Developments

- **The Novichok Group (N-Group)**
  This is a relatively new group of Soviet-developed nerve agents with a characteristic phosphorous-nitrogen-carbon bond. There exist several different judgments on the toxicological

and physical properties of N-Group members. At the very least, one can to some extent reconstruct the timeline of the appearance of N-Group live agent members before and after the fall of the Iron Curtain.



Appearance of information about and/or samples of N-Group members in military use.

Contrary to public opinion, knowledge of the latest Eastern Bloc nerve agents – either unitary or binary – came to NATO only after the Eastern Bloc's collapse. It is notable that all Eastern Bloc army CBRN-labs held samples to identify friendly or enemy nerve agent release. Therefore, adequate reference was present at an army level, but usually not below. These are samples whose study has become of increased interest in the West.
The chart above shows the flow of information from open literature related to interest in organic chemical structures with an element composition and bonds later found in the N–Group of live agents by a then member of the agent development team.

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

Fritz Pfeiffer is a CBRNe expert in analytics and counterterrorism at the National Infocentre of Chemical Warfare Agents, and conducts research at the *Büro für Umweltgeologie & Sicherheitsforschung*.

IED Threats: An Update

By Andy Oppenheimer
Source: https://nct-cbnw.com/ied-threats-an-update/

While attacks using IEDs (improvised explosive devices) have declined in the past year, they remain a weapon of choice for violent Jihadist groups, far right groups, sundry lone actors, dissident Irish groups, as well as in criminal revenge attacks.

Pakistan and Afghanistan
On 31 January, a bomb blast destroyed a mosque in a police compound in Peshawar, northwestern Pakistan, killing at least 100 and injuring more than 217. Planted by a suicide killer – still a common mode of IED emplacement – the 12kg device was detonated during prayers observed mainly by Pakistani law enforcement personnel.
This deadly attack highlighted the ongoing terror threat posed by the Pakistani Taliban, the Tehreek-e-Taliban (TTP), which claimed the attack was "revenge" for the death of TTP member Khalid Khorasani in 2022.
The rapid re-establishment of power in Afghanistan by the ultra-extremist Taliban in August 2021 has been a major factor in boosting the TTP and other terrorist groups. One of the Afghan Taliban's first moves was to release hundreds of TTP prisoners.

A Pakistani offshoot of the tyrannical Afghan Taliban, the TTP have increased its attacks on security forces and civilians. During 2022, they killed hundreds of people, including security forces. It was responsible for a failed vehicle-borne IED (VBIED) attack in Times Square, New York City, on 1 May 2010.

Peshawar mosque bombing on January 31, 2023 © Kanal13

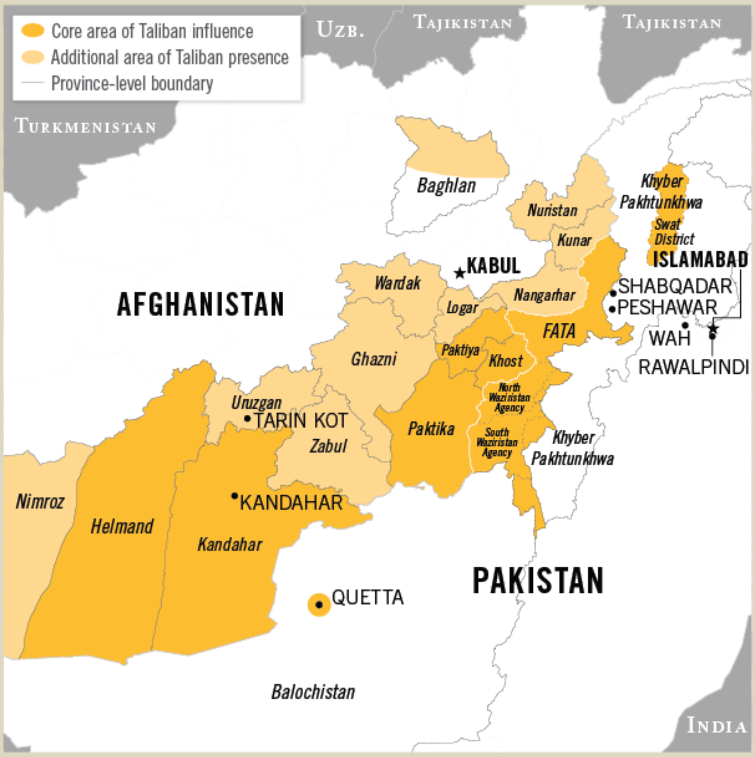


Image: Taliban-map – Caption: Core areas of Pakistani Taliban (Tehreek-e-Taliban, TTP) influence. This group was responsible for the bombing of a mosque in a police compound in Peshawar, northwestern Pakistan, on 31 January, killing at least 100.

Core areas of Pakistani Taliban (Tehreek-e-Taliban, TTP) influence. This group was responsible for the bombing of a mosque in a police compound in Peshawar, northwestern Pakistan, on 31 January, killing at least 100. ©National Counterterrorism Center

Deadly legacy: Ukraine

Thousands of landmines and IEDs are a deadly war legacy awaiting long years of disposal operations in many countries. Ukraine is the latest theatre where IEDs and mines have been laid. It was claimed in mid-2022 that the Russians had planted dozens of explosive devices that resembled children's toys (an M.O. previously deployed by ISIS).

It was reported in May 2022 that Ukrainian troops were deploying IEDs to disrupt the invading Russian forces. Devices are similar to those deployed by al-Qaeda and ISIS in the Middle East. Iraqi insurgents – al Qaeda in Iraq, then ISIS, and the Taliban in Afghanistan – inflicted severe losses and injury on US and UK forces through roadside IEDs and these and the thousands of mines left over from these and many other wars will take years, or decades, to clear.

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

Andy Oppenheimer is author of *IRA: The Bombs and the Bullets – A History of Deadly Ingenuity* (2008) and a former editor of *CBNW* and *Jane's NBC Defense*. He is a Member of the International Association of Bomb Technicians & Investigators and an Associate Member of the Institute of Explosives Engineers and has written and lectured on the IRA since 2002.

The Islamic State Claims Suicide Bombings in Iran

By Aymenn Jawad al-Tamimi

Source: https://www.meforum.org/65416/the-islamic-state-claims-suicide-bombings-in-iran

91 dead

Jan 04 – Today, the Islamic State's al-Furqan media released a new speech from Islamic State spokesman Abu Hudhayfa al-Ansari. The speech, entitled "And kill them wherever you find them" (taken from Qur'an 2:191), focused primarily on the Israel-Gaza war but was a very predictable reiteration of the group's talking points: (i) that the battle in Palestine is a religious war against Jews, and not one about liberation to establish a national homeland, (ii) denunciation of the various 'nationalist' Palestinian factions and those like Hamas aligned with the broader Iranian-led 'resistance' axis, which is utilised by Iran as a Shi'i expansionist project that is no less dangerous if not more so to Islam and Muslims than the state of Israel, (iii) the various Sunni Arab governments are 'apostate' entities that are part of the Jewish-'Crusader' alliance against Islam, (iv) the correct form of jihad is one the Islamic State pursues to establish the rule of God's law, and fighting all the disbelievers.

Within this context, the Islamic State has now launched a new expedition entitled "Kill them wherever you find them," beginning with claiming responsibility for the two bombings that took place on in the hometown of the Islamic Revolutionary Guard Corps' Quds Force commander Qasim Sulaymani on the fourth anniversary of his assassination by the Americans. As soon as the sheer scale of the killing of people in such an indiscriminate terrorist attack, it became evident to me that the bombings were likely an Islamic State operation (though it is always wise to wait and see if the group claims a particular attack). Blaming Israel for the incident, as John Hopkins professor Vali Nasr

did, was frankly ludicrous. It is simply not Israel's modus operandi to engage in such terroristic acts inside Iran: rather, Israel pursues carefully targeted killings for specific goals like undermining Iran's nuclear program. The suggestions that the attacks might have been an inside Iranian job also struck me as ridiculous. These attacks illustrate the Islamic State's unchanging basic worldview and that it is ultimately a marginal player in wider regional geopolitics. The Islamic State pursues an ideologically purist agenda based on fighting all others who do not share its rigid political program, wherever it is possible for the group's members and supporters to do so. Ultimately, this amounts to the same old messaging and the same old tactics. While there was concern that these bombings would somehow trigger further 'regional escalation,' they are in reality a sideshow, especially now that the Islamic State has officially claimed the attacks. Below is the statement by Islamic State claiming responsibility for the Iran bombings, translated by me. As part of the 'And kill them wherever you find them' expedition: the killing and wounding of more than 300 of the idolatrous Rafidites [Shi'a] in a dual martyrdom operation [suicide bombing] in Iran.

Iran: Thursday, 22 Jumada al-Akhira 1445 AH

Through granting of success by God Almighty, and as part of the 'And kill them wherever you find them' expedition, two martyrdom operative brothers- Omar al-Muwahhid and Sayf Allah al-Mujahid (may God Almighty accept them both)- headed yesterday towards a great gathering of idolatrous Rafidites, near the tomb of their hypocrite leader 'Qasim Sulaymani' in the town of Kerman in southern Iran. There, they blew up their explosive belts amid their gathering. This resulted in the killing and wounding of more than 300 idolatrous Rafidites. Thanks and praise be to God.

May the idolatrous Rafidites know that the mujahidin lie in wait for them and their projects, by the permission of God Almighty.

Aymenn Jawad Al-Tamimi is an Arabic translator and editor at Castlereagh Associates, a Middle East-focused consultancy, and a writing fellow at the Middle East Forum. He runs an independent newsletter at aymennaltamimi.substack.com.

The Future of Terrorist Use of Improvised Explosive Devices: Getting in Front of an Evolving Threat

By Austin C. Doctor and Sam Hunter

December 2023, Volume 16, Issue 11

Source: https://ctc.westpoint.edu/the-future-of-terrorist-use-of-improvised-explosive-devices-getting-in-front-of-an-evolving-threat/

On April 15, 2013, two improvised explosive devices (IEDs) were placed roughly 200 yards apart on Boylston Street in Boston, Massachusetts, and detonated near the final stretch of the Boston Marathon.[1] The joint explosions killed three people—eight-year-old Martin Richard, 23-year-old Lu Lingzi, and 29-year-old Krystle Campbell—and injured more than 250 others.[2]

Investigators concluded that the attackers were motivated by extremist beliefs, though "not connected to any known terrorist groups."[3] The perpetrators responsible for the attack, 26-year-old Tamerlan Tsarnaev and 19-year-old Dzhokhar Tsarnaev, had learned how to construct the explosive devices from a popular article published in Inspire magazine, an English-language online publication produced by al-Qa`ida in the Arabian Peninsula.[4] The improvised devices used in the attack were two six-quart pressure cookers packed with low explosives, ball bearings, nails, and other metal used as shrapnel.[5] The explosions most likely came from up to 20 pounds of powder from fireworks and/or similar pyrotechnic materials.[6] The attackers detonated each bomb remotely by sending a signal to a receiver on each device, which used power from battery packs to light Christmas tree bulbs that had the glass covers removed.[7] These sparked and ignited the IEDs' contained explosives.[8] According to one report, the devices may have cost as little as $100 to build.[9]

Improvised explosive devices are easy to make, difficult to combat, and cause significant harm and disruption. Militant IED attacks have caused countless civilian and troop casualties in conflict zones abroad. Likewise, they are responsible for considerable death, destruction, and panic within the United States. Major ongoing conflicts, such as the war in Ukraine and the recent surge of hostilities in Israel and Gaza, can serve as highly publicized testbeds for novel means of IED development and employment. Because of their outsized impact—as well as the wide availability of device components—violent extremists continue to consider IEDs a valuable part of their arsenal.

Yet, the expected persistence of a threat should not be mistaken for rote repetition. The terrorist IED threat is not static. Violent extremists continue to innovate, drawing on emerging technologies and creative problem solving. In response, law enforcement, military, and intelligence practitioners devise new preventative and interdiction methods. Terrorists respond by finding novel ways to conduct successful attacks. The cycle repeats itself. As a result, despite billions of dollars invested in the counter-IED mission over the past 20 years, yesterday's solutions are at risk of being poorly suited to tomorrow's threats.

The onus of initiative requires that practitioners and applied researchers look over the horizon to identify emerging threats. In support of this need, the authors offer a forward-leaning taxonomy of emerging threats related to terrorist use of IEDs in the United States and consider its implications. The article proceeds as follows. First, the authors provide a framework with which to conceptualize and classify IEDs and IED-related incidents. Next, they briefly analyze recent global trends in terrorist use of explosives. Third, they identify key emerging threats related to the threat actors, methods, and targets connected to IED-related incidents in the United States. Finally, the article concludes with a discussion on the implications that these emerging threats may hold for the counter-IED mission community, supporting research efforts, and U.S. national and homeland security.

A Rapid-Fire IED Taxonomy

Although IEDs are not new, the term "improvised explosive device" only emerged as recently as the 1970s. It has since been tethered to a wide array of definitions and taxonomies. These occasionally differ regarding the nature of device components, the source of a device's "improvised" nature, and the intended use by whomever is conducting an attack. The lack of consistency is driven partially by the fact that practitioners and academics both heavily contributed to this debate with limited communication across disciplines and with distinct purposes behind them.

Most academic definitions contain a broader selection of inclusionary characteristics, encapsulating the development process, ingredient types, desired effect from usage, and types of adversaries that may or may not use this method of attack. Prioritizing inclusivity and practicality as guiding principles, Paul Gill and his colleagues synthesize nearly 30 different definitions to offer the following conceptualization:

An explosive device is considered an IED when any or all of the following — explosive ingredient, initiation, triggering or detonation mechanism, delivery system — is modified in any respect from its original expressed or intended function. An IED's components may incorporate any or all of military grade munitions, commercial explosives or homemade explosives. The components and device design may vary in sophistication from simple to complex and IEDs can be used by a variety of both state and non-state actors. Non-state actors can include (but not be limited to) terrorists, insurgents, drug traffickers, criminals and nuisance pranksters.[10]

Practitioners face a similar issue. IED taxonomies can vary considerably across different elements of the counter-IED mission community (e.g., military Explosive Ordnance Disposal technicians, intelligence community analysts, local bomb squad units, and federal law enforcement officers). The lack of a standardized and universally adopted framework—the systematic description of key device components—can inhibit the data collection, information sharing, and synchronized implementation needed to mitigate current and future IED-related threats.

While IEDs are inherently bespoke, most modern devices feature five basic component types: (1) a switch, (2) an initiator, (3) a main charge, (4) a power source, and (5) a container. Figure 1, taken from the United Nations Mine Action Service, summarizes this IED technical categorization framework.[11]

Some IEDs also make use of enhancements, which terrorists add to a device to increase its physical or psychological effects. Common enhancements include shrapnel (e.g., nails, screws, or ball bearings) and fuel (e.g., propane or other gas). Terrorists could create "dirty bombs" by adding chemical, biological, radiological, or nuclear (CBRN) agents.[12] In 2014, the Islamic State successfully enhanced an unknown number of IEDs delivered via aerial and land vehicles, as well as roadside victim operated IEDs, with chlorine and mustard gas.[13] Reportedly, the Islamic State had access to university laboratories in Mosul and chemical experts to conduct these attacks.[14]

A clear, concise conceptualization and taxonomy of IEDs are necessary to identify and characterize emerging threats in this space. Looking ahead, one can expect to see terrorists innovate around IEDs in two general ways: first, in the component composition of the device itself, and second, in the methods by which they plan and conduct IED-based attacks. In the next section, before elaborating on emerging trends in the United States along these dimensions, the authors summarize recent trends in IED-related terrorist activity.

Recent Global and Domestic Trends in Terrorists' Use of IEDs

The IED threat is, regrettably, alive and well. A recent report by Action on Armed Violence (AOAV) identified a total of 640 incidents worldwide involving IEDs across 33 countries and territories from January to June 2023.[a] These attacks were responsible for a recorded 1,456 civilian casualties, including 450 deaths. Notably, after years of steady decline in IED-based violence, the rates reported for this year thus far portend a possible increase in IED use for the first time since 2018.

It is unsurprising that improvised explosives continue to be one of the most common tools and methods used by terrorists and militant organizations abroad. As tactical instruments, IEDs are capable of wielding outsized, even strategic, effects. The widespread use of IEDs by local insurgent forces in Afghanistan and Iraq against U.S. forces, for example, often compelled deployed troops to restrict themselves to armored vehicles, avoid key travel routes, and advance at a snail's pace through sensitive areas.[15] And with justified cause. By some estimates, at least half of American troop fatalities in Iraq as well as in Afghanistan were caused by IEDs.[16] [b] IEDs can quickly level an asymmetric playing field.

Groups and individuals associated with the Islamic State and al-Qa`ida continue to drive much of IED-related activity around the world, accelerated by both organizations' ongoing regional expansion. Notably, al-Qa`ida affiliate al-Shabaab has long relied on IEDs as a critical tool against both civilian and military targets in Somalia.[17] Now an operational trademark of the group, combatants often integrate vehicle borne IEDs (VBIEDs) and/or person borne IEDs (PBIEDs) in multi-stage, complex ground assaults.[18] Al-Shabaab operatives were reportedly responsible for the recent surge of IED-based attacks around key border areas in Kenya, such as Garissa and Lamu counties.[19] Observers have noted a similar, concerning trend by violent extremist forces in the Sahel and West Africa.[20]

Other global regions are also experiencing sustained or increased IED activity. Militant actors in Afghanistan and Pakistan continue to perpetrate IED attacks at a high tempo. In a June 2023 report, the UN Assistance Mission in Afghanistan's Human Rights Service reported that 3,774 civilians were seriously injured or killed by conflict actors between August 2021 and May 2023.[21] Roughly 75 percent of those recorded casualties are attributed to militant use of IEDs in crowded public spaces, including houses of worship, schools, and markets.[22] In the immediate aftermath of the Taliban takeover in August 2021, IED attacks by the Islamic State's affiliate in Afghanistan, Islamic State Khorasan Province (ISK), increased significantly, including an uptick in observed suicide PBIEDs attacks.[23] Drawing on an original dataset of extremists charged in U.S. courts for their roles in planning or perpetrating attack plots tied to the Afghanistan-Pakistan region, Andrew Mines found that IEDs have been the most frequent method of attack between 1985 and 2023.[24]

The IED threat is hardly limited to foreign wars or political unrest abroad. This issue hits home for many Americans. Of course, there are the devastating and well-documented domestic terrorism incidents, such as the 2013 Boston bombing and the 1995 Oklahoma City bombing. Looking back further into American history, explosives-based attacks emerge as a regular feature of domestic extremist activity: Consider the Weather Underground bombings in the 1970s, the 16th Street Baptist Church bombing of 1963, and the 1920 anarchist bombing of the J.P. Morgan Building on Wall Street, for example.[25] Audrey Cronin records a staggering 216 unique bombing incidents between 1867 and 1934 in the United States as political dissidents of various kinds made regular use of newly developed and widely accessible dynamite.[26] In short, ideologically motivated actors in America have long used explosives to coerce outgroups or challenge the political status quo. And the threat remains. For example, one day before the January 6 insurrection, a still unidentified individual left two pipe bombs outside the Republican National Committee and Democratic National Committee headquarters on Capitol Hill. The devices did not detonate.[27] Even more recently, amid concern that there could be a resurgence in jihadi terrorism in the West because of the war in Gaza, in October 2023 a Jordanian man living in Texas was arrested after allegedly posting online about his support for killing Jews and viewing "specific and detailed content posted by radical organizations on the internet including lessons on how to construct bombs or explosive devices."[28]

While there have been relatively few successful terrorist bombings overall, U.S. intelligence and law enforcement efforts have successfully thwarted several local IEDs plots and attacks. In August 2023, for example, authorities arrested a 17-year-old resident of Philadelphia, Pennsylvania, alleging "he was preparing to build bombs and select targets after being in touch with an al-Qaida affiliate in Syria."[29] The suspect's phone messages and internet history revealed instructions for how to make improvised explosive devices. Additional surveillance found that the teen had purchased materials to make the bombs in the weeks prior to his

arrest, including chemicals, wiring, and devices that could be used as detonators.[30] In addition, U.S. Customs and Border Protection provided records revealing 14 international shipments of military tactical gear to the teen's home address.[31] The case is ongoing.

In January 2011, Kevin Harpham, a white supremacist affiliated with the National Alliance, admitted to placing an IED along the route of a Martin Luther King parade in Spokane, Washington.[32] The device, a shaped charge, was designed to scatter shrapnel covered with rat poison to keep victims' wounds from coagulating.[33] The IED was discovered less than an hour before the parade started and was subsequently disarmed.[34] In February 2020, Demetrius Nathaniel Pitts, a U.S. citizen who had pledged his allegiance to al-Qa`ida, was sentenced for plotting to bomb a July 4th parade in downtown Cleveland in 2018.[35] Pitts planned to use both remote-control cars filled with explosives and loaded with metal shrapnel and a larger vehicle packed with explosives to "cause maximum damage."[36] The attack was stopped by an FBI employee acting in an undercover capacity.[37]

In a more recent example, in February 2022, Christopher Cook, Jonathan Frost, and Jackson Sawall pleaded guilty to conspiring to conduct a domestic terror attack—one that presumably, if not foiled, would have involved the use of explosives.[38] The men had met on Iron March, a neo-Nazi online forum, and joined forces. Federal prosecutors argued that the group's intended target for a large-scale attack was the U.S. power grid "to stoke division in furtherance of white supremacist ideology."[39] As part of the conspiracy, each member of the group was reportedly assigned a substation in a different region of the United States.[40] Their group used an encrypted messaging app to share information with one another about gathering firearms and explosives for use in the attack. And, in an August 2020 search of the defendants' homes, the FBI found precursor chemicals "which could be used to create an explosive device."[41] Cook and Frost were sentenced in April 2023.[42]

It is worth mentioning that the future IED threat in the United States may also stem from conspiracy-based ideologies, some of which may have links to violent extremist beliefs but do not necessarily on their own constitute domestic terrorism. On Christmas Day 2020, a vehicle borne IED exploded in downtown Nashville, Tennessee. The bombing occurred outside of an unmarked communication building and, according to one report, caused extensive communications and power outages, flooding, and a fire within the building.[43] Federal law enforcement determined that the action was not related to terrorism, but the investigation team notes that the perpetrator, Anthony Quinn Warner, maintained "long-held individualized beliefs adopted from several eccentric conspiracy theories."[44]

In summary, despite the relatively slow cadence of successful domestic bombings of late, the authors warn against laxity—the IED threat is not going anywhere. A declassified U.S. military report on improvised methods utilized by Viet Cong forces describes the complexity of observed IED-based attacks as being "only limited by the ingenuity of the man who constructs them."[45] More than 50 years later, this is no less true. The near-endless combinations of IED design (i.e., technical categorization) and application (i.e., tactical characterization) continue to present a significant challenge to the counter-IED mission community.

When terrorists and violent extremists innovate, they gain an advantage, even if temporarily, in circumventing existing detection and interdiction methods. Therefore, anticipating the timeline and locus of innovation is essential to maintain a proactive posture in countering terrorist use of explosives. In the next section, the authors describe how the terrorist IED threat is evolving and outline a five-part framework for classifying related emerging threats.

Emerging Threats in Terrorist Use of IEDs in the United States

The authors anticipate a number of emerging threats related to the methods and targets of IED-based plots and attacks in the United States.[46] Anticipating how terrorists might attack in the future—and why—is central to the design of efforts to protect the security of both individual targets and the nation as a whole. Some of the emerging threats discussed here represent incremental evolutions, indicating areas for targeted adjustment within the existing counter-IED infrastructure.[47] Others point to potential structural shifts in the terrorism milieu, requiring deeper thought and potential responsive action around how the interagency counter-IED mission community organizes its future efforts.

The authors identify five overlapping categories that they expect to act as underlying currents propelling the future explosives threat: the threat actor landscape, technical categorization, tactical characterization, malign use of emerging technologies, and the target surface. Each emerging threats category features key indicators or propellants, which will be discussed. Combined, these categories speak to critical questions: *Who* is likely to use IEDs, *how* are they likely to develop and employ IEDs, and *where* will IED attacks be targeted? Importantly, this set of related analytic categories transcends the boundaries exclusive to a single critical mission area—such as prevention, detection, or render safe—and creates an opportunity for cross-cutting insights.

1. The Threat Actor Landscape in the United States

The terrorism milieu in the United States is increasingly fragmented. It is a problem of addition, not substitution. Jihadi terrorism still presents a significant threat to the United States and its partners, especially through homegrown violent extremism (HVE). The simultaneous rising activity of various domestic violent extremists—such as racially and ethnically motivated violent extremists (RMVE) and anti-government/anti-authority violent extremists (AGAAVE)—in the United States has led to a structural shift in the threat actor space. It is ideologically diverse and geographically diffuse. While some foreign terrorist organizations likely maintain a capability and intent of striking the U.S. homeland, the greatest likelihood of an attack in the United States comes from within.[c]

Domestic violent extremists and homegrown violent extremists showcase significant range in their ideological agendas, espoused grievances, and general relationship to the status quo. But as a tactical tool, the IED is more ecumenical and will have a catholic appeal across tomorrow's threat actor ecosystem. Instructions for the construction of IEDs and the call for their use are featured strongly in salafi-jihadi publications, such as Inspire; white supremacist RMVE channels, such as Terrorgram; and anarchist violent extremists' canon texts, such as The Anarchist Cookbook.[48] As such, the general use of IEDs or specific TTPs reflected in observed plots and attacks may not necessarily vary meaningfully across this fragmented actor landscape.

However, the fragmentation of the threat actor landscape in the United States—compounded by the simultaneous presence of organized violent extremist groups, decentralized cells, and seemingly "lone actors"—may shape where and why one expects to see explosives used in domestic terrorist attacks.[49] Some may focus on accelerating "mayhem," i.e., overthrowing or destabilizing the prevailing political and social order.[50] Others clearly remain intent on generating mass casualties. For extremists intent on using explosives, their respective ideologies may shape their target selection.[51] For example, drawing on federal court documents from 2016 to 2022, one report finds evidence that salafi-jihadi and white supremacist attack planners have largely targeted different U.S. critical infrastructure sectors, with "the former focusing on the commercial facilities, government facilities, and emergency services sectors, and the latter predominantly focusing on the energy sector."[52] This suggests distinct underlying logics—corresponding with different ideological foundations and related objectives—behind the use of IEDs by violent extremists in the United States.

As a result, rather than one target profile in IED attacks, there will likely be multiple. Different types of targets (e.g., public crowded spaces, the power grid, etc.) will likely carry unique symbolic or practical value for different sorts of U.S.-based violent extremists.[53]

Of particular concern is the rising number of threats, plots, and attacks against U.S. public officials and elected representatives. This trend has been mostly driven by anti-government anti-authority violent extremists, though not exclusively.[54] Many such incidents in the future may involve IEDs, an instrument firmly rooted in the history of political assassinations. In August 2023, for example, James Clark pleaded guilty to sending a bomb threat to an election official in the Arizona Secretary of State's office. Clarke warned the official that she needed to "resign by Tuesday February 16th by 9 am or the explosive device impacted in her personal space will be detonated."[55] According to federal investigators, the would-be attacker had conducted online searches that included the full name of the election official, instruction on how to kill, the official's residential address, as well as details on the Boston Marathon bombing.[56]

This presents a fundamentally different challenge than protecting the homeland from another 9/11 type attack. It points to the risk of normalization of political violence and an erosion of civic norms – all propelled by the increasingly diverse set of violent extremists present in the United States.[57]

2. IED Technical Categorization

Terrorists have ample opportunity to innovative in the design and manufacture of IEDs through its various components. A focus on patterns of IED technical categorization (i.e., a systematic construct of an IED's components; see Figure 1) can provide useful leverage over emerging trends in terrorist use of explosives. The communication and diffusion of novel inventions, which may originate from terrorist bombmaking camps, basement labs, or benign hobbyist communities, reduce barriers of entry for would-be attackers and increase challenges for interdiction.

When developing an IED, most terrorists in the United States have relied on commercial explosives such as propellants (e.g., black and smokeless powders) and pyrotechnics (e.g., flash powders) as main charges or use readily available precursors chemicals such as peroxides and fuel-oxidizer mixtures (e.g., ammonium nitrate-fuel oil) to manufacture homemade explosives (HMEs).[58] The use of military explosives (e.g., Semtex) is exceptionally rare in U.S. bombing incidents. In general, the set of common IED main charges has been relatively unchanged over the past 15 years and is unlikely to shift significantly in the coming years.[d] However, current limitations in detecting inorganic species and complex mixtures, such as homemade fuel-oxidizer explosives, across a range of environmental conditions, continues to present challenges and represents part of the still evolving threat.

Another emerging threat stemming from IED technical categorization is presented by a different key device component: the switch. Significant advances in electronics over the past few decades have enabled terrorists to make creative changes to device switches. These advancements matter; how a device is commanded or activated is a critical part of an attack plan that determines where the responsible terrorist(s) may be at the time of the bombing. It affects the set of viable prevention, detection, and defeat options available to the counter-IED mission community. Electronic triggers have evolved from the use of Casio watches to radio transmitters and from garage door openers to mobile phones. Timing chips sell for a few dollars, and small computing chips sell for well under $100, making such materials inexpensive to acquire. These advancements open the field for command, time, and victim-operated switches, standing to increase the operational range and fidelity of terrorist IED attacks. In particular, the authors observe the emerging potential opportunity for devices controlled or activated via WiFi as well as the potential for increased use of sensor-based switches to facilitate more sophisticated or targeted attacks.

Lastly, it is worth noting that terrorists constantly imagine and adopt new containers both for the confinement of the main charge but also for the purpose of concealment. Metal pipes and pressure cookers are among the most common containers used in U.S. attacks, but creativity abounds. Recent incidents, for example, have seen terrorists in the United States or abroad use handheld radios, printers, synthetic rocks, aluminum drink cans, and other non-descript items as containers.[59] The sheer scope of possible containers creates Herculean challenges to forecasting—and therefore mitigating—potential trends in their adoption.

3. IED Tactical Characterization

Terrorists continue to show great creativity in the tactical characterization of IED-based attacks (i.e., the way in which an IED incident is planned and conducted). This can be assessed across multiple phases of the terrorist attack sequence, including operational preparation and device employment.

A major contributor to—if not a key enabler of—the evolving IED threat is the sharing and dissemination of malign tactics, techniques, and procedures (TTPs) through online platforms and communication channels, such as YouTube, Facebook, WhatsApp, and microblogs.[60] For would-be attackers with minimal prior experience or knowledge, the dissemination of best practices and novel solutions lowers barriers of entry to building a functional IED. It is not only the wide dissemination of articles like "How to Build a Bomb in the Kitchen of Your Mom."[61] It is also dissemination of TTPs at scale through online micro-engagements enabled by increased user technological savvy and an ever-widening range of platform options. This risk was specifically reinforced in the 2023 Europol Terrorism Situation and Trend Report, which assessed that "terrorists and violent extremists remain apt in evading restrictive measures and monitoring related to explosive precursors in the EU. For instance, a pro-IS group released a document on a cloud-based instant messaging platform, suggesting the use of alternative precursors for HMEs."[62] Further compounding this threat, the advents of the metaverse and Web3 offer further opportunities through obscured website launch, file-hosting services, and discrete communication for evasion of present content moderation and monitoring efforts.[63] This, paired with the exploitation of readily available off-the-shelf technologies, means that violent extremists are able to both develop and employ IEDs with a relatively small investment and higher degree of reliability.[64]

Employment—the means by which IEDs are delivered to a target—is a major component of an IED attack tactical design. One of the highest tempo evolutions in the IED threat area is found in the potential for delivery of explosives via unmanned systems (UxS).[65] This threat is still evolving.[66] Unmanned vehicles can range from a toy-radio-controlled boat or car to a quadcopter aerial drone to an autonomous ground- or surface- based vehicle. Thus far, the greatest attention has been given to unmanned aerial systems. In November 2012, Rezwan Ferdaus was sentenced for plotting an attack in support of al-Qa`ida on the Pentagon and the U.S. Capitol using a model aircraft filled with C-4 plastic explosives.[67] As reported by FBI investigators involved in the case, the would-be attacker was the mastermind behind the operational plan: "Mr. Ferdaus' sentence reflects that he alone conceived the plot, was responsible for his illegal acts, and acted purposefully."[68] To be sure, this plot was dependent on the supply of explosive materials by an FBI undercover employee, suggestive of some control over this threat incident.[69] However, the highly publicized spike in the use of armed unmanned aerial vehicles in Syria and Iraq by the Islamic State, and possibly the ongoing central role of small UAS in the Ukrainian resistance, may inspire a greater frequency of similar attempts by terrorists in the United States.[70] In February 2022, FBI Director Christopher Wray reported to the U.S. Senate Homeland Security and Governmental Affairs Committee that the FBI was "investigating, even as we speak, several instances within the U.S. of attempts to weaponize drones with homemade IEDs. That is the future that is here now."[71]

In January 2023, a graduate student in the United Kingdom was arrested for building a drone to deliver a bomb on behalf of the Islamic State.[72] The student had filled out an Islamic State application form. During the arrest, authorities seized several devices. A 3D printer was also found at the property.[73] The case is ongoing, but it indicates that the tactics developed and honed in conflict zones abroad may be adopted by like-minded persons living in otherwise peaceful environments. Compounded by the concurrent advancement of other emerging technologies, terrorist use of unmanned systems is an evolving threat that will continue to present a host of novel challenges to current security infrastructure and protocols.[74]

4. Malign Use of Emerging Technologies

Serving as a force multiplying function to a number of the threats identified above, the malign use of emerging technologies provides feasible means of novel IED design and employment. Of notable concern is that such emerging technologies are rarely military systems, but rather commercial off-the-shelf. As these become more affordable, more reliable, and widely available, the threat they present will only become greater.[75]

Although hardly exhaustive, the authors offer a handful of emerging technologies that carry notable implications for the future IED threat. The growing knowledge and use of microcontrollers (e.g., Arduino Uno) and single-board computers (e.g., Raspberry Pi) present a worrying new means of device construction, with disquieting implications for their application.[76] They provide a low-cost, easy way for novices and experts alike to construct IEDs that interact with motors and sensors that may measure light, temperature, pressure, and other environmental variables.[77] Adding to this threat, the lawful online activities carried out by communities of hobbyists and in “maker spaces” around these technologies is a growing avenue through which individuals and groups with malign intent may become sufficiently knowledgeable and skilled in their use with relatively little cost or time.

Relatedly, the sustained advancements in infrastructure surrounding the Internet of Things (IoT), including high-speed internet and 5G/6G telecommunication networks, open a new threat vector related to IED-based attacks.[e] Extending the logic of a radio-controlled device, a WiFi-connected IED could be controlled through an extensive array of methods, and from a much wider geographic range. As a recent report on IED threats put it: “We are at a stage … where the ‘internet of things’ offers an endless choice of switches.”[78] If addition, a device’s integration into the IoT may also support the employment of an IED device through the operation of an autonomous vehicle or unmanned system (UxS).

In another vein, the past year has seen a surge of public use of generative artificial intelligence (AI) through the release of ChatGPT, DALL-E, and other programs built around machine learning-based models. Opportunities for malign use abound. In the realm of IEDs, generative AI may provide new avenues for the development of explosives, the identification of attack targets, operational planning, training, and other key tasks. To be sure, it is unlikely that generative AI will wash out a dependency on individual expertise, but it will help to level the playing field, reducing the time required for any given individual to develop viable homemade explosives and improvised devices.

Finally, rapid and significant advancements in additive manufacturing (AM) (i.e., the process of creating a three-dimensional object by building up a series of successive layers of material(s) over time) are a key part of the evolving IED threat landscape. Recent efforts, for example, have demonstrated the possibility of using 3-D printing to create elements of energetic materials applicable to high explosives, propellants, and pyrotechnics.[79] These could presumably be used in device boosters or main charges and, in some cases, help aspiring attackers to circumvent current prevention barriers. Logistically, AM may reduce time sensitivities, provide opportunities for rapid prototyping, and circumvent supply-chain constraints—all in an operationally secure environment. These functions reduce common barriers to developing IEDs. Additive manufacturing also opens a new avenue for crafting IED containers and other key device components in a way that is both low cost and discrete.

5. Expanding Target Surface

The target surface for IED attacks is complex and varied, but the authors observe several trends regarding the targets that may appeal to threat actors in tomorrow’s political environment. This is important as threat assessments, intervention efforts, and preventative security measures will likely differ for different target types, albeit with some overlap. Among these include U.S. critical infrastructure, crowded spaces, and public officials.

Critical infrastructure sites such as power grid substations, transportation systems, and crowded spaces are among the most frequently targeted soft targets for threat actors. Earlier this year, the U.S. Department of Homeland Security identified rising threats to critical infrastructure as a leading national risk. For example, violent extremists are likely to maintain the growing operational focus on the U.S. power grid; neo-Nazi extremists Brandon Russell and Sarah Beth Clendaniel conspired to conduct a series of “sniper attacks” on Maryland electrical substations earlier this year.[80] In addition to transportation and energy, other national critical infrastructure sectors are also generally seen as attractive targets for extremist attacks, including communications, food and agriculture, and healthcare and public health. These incidents tend to garner mass attention and cause significant harm and disruption, aligning with the doctrine of multiple elements of today’s violent extremist ecosystem. Extremists may use a wide range of TTPs for such attacks, including the use of IEDs.

As expressed in a recent government threat advisory bulletin, the terrorism threat may originate from a wide range of ideologically motivated individuals or groups and could focus on a multitude of soft targets: mass transit areas, arenas, shopping malls, open-area gatherings, houses of worship, and others.[81] Crowded public spaces, including large public venues, present one of the greatest challenges for detection and protection owing to their numerous entrance and egress points, open spaces, and lack of security by design. For terrorists looking to maximize casualties, unrestricted public areas are ‘low-hanging fruit.’

Public officials are also an increasingly frequent target of violent extremist activity. A long-standing tool of assassination, explosives were used in the earliest phases of modern terrorism by violent extremist groups such as Narodnaya Volya.[82] A growing number of plots are targeting U.S. elected officials and federal law enforcement.[83] Notably, these threats may come from across the violent ideological spectrum.”[84] In May 2023, Jessica Higginbotham, a former security subcontractor working at the Athens-Clarke County Democratic Party campaign office, pleaded guilty to threatening to bomb their local headquarters while the U.S. Senators from Georgia were in town for campaign events. In August 2018, Venezuelan President Nicolás Maduro survived an assassination attempt involving explosive drones.[85] Based on the open-source information available, it appears that an attack involved two drone-borne IEDs while Maduro was giving a speech in Caracas, celebrating the 81st anniversary of the National Guard.[86] Given widespread access to commercial-off-the-shelf systems and the rising rate of threats and plots against U.S. public officials, the authors anticipate that similar attempts may be made by ideologically-motivated actors in the United States in the future.

Looking Ahead

IEDs are easy to make, difficult to combat, and cause disproportionate harm and disruption. In 2015, terrorism and insurgency expert David Kilcullen remarked "I sometimes hear people express the hope that the IED threat will diminish as Western forces pull out of Afghanistan. Unfortunately, nothing could be further from the truth—the IED has now entered the standard repertoire of irregular forces in urban areas across the planet, and there are no signs this threat is shrinking; on the contrary, it seems to be growing."[87]

Over the past decade, there has been a relative increase in violent extremist activity across the United States. Yet, successful bombings have been relatively few. Given the steady cadence of attempted IED attacks, however, motive or intent does not seem to be waning. The authors, therefore, warn against a false sense of security. The fact that intelligence and law enforcement practitioners have thwarted so many of the recent attack plots in the United States may indicate a future risk that terrorists will be oriented toward developing novel means of IED development and employment.[f] This would pose new challenges to those responsible for combating terrorist use of explosives.

The U.S. domestic counter-IED mission community is currently organized around five critical mission areas: deterrence, prevention, detection, protection, and response.[88] These are suitable categories for action, but less useful as analytic concepts. Far too many emerging threats bleed across the missions' boundaries. Thus, to support proactive assessment and mitigation, the authors have presented a five-part framework for identifying and assessing emerging threats related to the development of IEDs and their employment. They argue that there is value in dissecting key features of this evolving threat, including attention to the threat actor landscape, IED technical categorization, IED tactical characterization, malign use of emerging technologies, and the target surface.

Looking ahead, and thinking about next steps, the authors offer three guiding principles for practitioners and academic researchers as they work to proactively identify actionable, sustainable, and durable solutions to the evolving IED threat.

1. Inhibit terrorist access to IED materials. This means reducing malign actors' acquisition and use of precursor chemicals and known bomb-making materials. This work is already well underway as a critical mission area,[g] but the authors' analysis suggests the need for additional considerations. Based on the set of emerging technologies identified here, for example, law enforcement and first responders should include small UxS, microcontrollers and single board computers, 3-D printing systems, and such components on lists of potential plot-warning indicators. A focus on this goal will also require monitoring the avenues by which terrorists disseminate TTPs, best practices, and general knowledge on the development of HMEs and the construction of IEDs. As discussed, much of this is occurring online. Microblogs and Web3, social media platforms, encrypted message applications, and the emerging metaverse will all be viable points of access for lethal 'know how.'

2. Disrupt IED facilitation networks and IED plots. In some cases, efforts to restrict terrorist access to precursor and bomb-making materials will be unsuccessful. The next objective should be intercepting potential attackers and disrupting their facilitation networks. This demands a clear understanding of targets at risk, probable locations for sourcing and IED development, tactics, techniques, and procedures (TTPs), and the actors likely to be behind an attack. In addition to maintaining robust intelligence and law enforcement capabilities, this requires deep knowledge on both established and emerging trends. Given the changing nature of the threat actor landscape and an expanding target surface, the authors see notable value in an updated analysis of the individual- and environment-level precedents of IED adoption and tactical design. More generally, analytic initiatives should be oriented on future, anticipated challenges. Future-focused methodologies such as horizon scanning, predictive scenario-simulation analysis, and/or risk assessment evaluations may be especially useful toward bridging the gap between previous and anticipated manifestations of the IED threat and developing forward-leaning solutions focused on future plots.

3. Enhance interagency and inter-sector coordination. From 2006 to at least 2015, a large part of the counter-IED effort—and connected federal research and development funding—was driven by military needs based on U.S. activity in Afghanistan, Iraq, and other theaters. The Joint IED Defeat Organization (JIEDDO) was a gravitational center of this effort, boasting more than $18 billion in funding over much of that period.[h] But these are leaner times. As defense priorities shift from counterterrorism to great power competition and as violent extremist activity increases domestically, "much of the U.S. prevention and counterterrorism workforce will be expected to do more with less as they hold the line."[89] Under these circumstances, effective action to counter emerging and evolving IED threats will require clearly identified roles and responsibilities and formal mechanisms of information sharing, coordination, and collaboration across the interagency mission community. Moreover, robust partnerships between government practitioners, industry leaders, and academic experts will be constructive toward developing and implementing actionable and evidence-based mitigating strategies.

While this article largely focuses on the potential implications of this evolving threat for U.S. national and homeland security, much of the discussion presented here will also pertain to other countries including across Western Europe, Canada, Australia, and New Zealand as well as certain hostile environments in the Middle East, Central and South Asia, and sub-Saharan Africa.

The desired end state is the safeguarding of local communities, the protection of critical infrastructure, and the minimization of harm in cases of successful IED attacks. Combating future terrorist use of IEDs in the United States and elsewhere necessitates a frank assessment of where the IED threat is heading, where existing security measures are sufficient, and where the current counter-IED architecture may require a remodel to match the changing times.

Substantive Notes

[a] Regarding the AOAV report methodology: Because attribution is not always possible, it is possible that some of the recorded incidents may not reflect activity by armed non-state actors. However, militants are recorded as the most common perpetrators of IED attacks, specifically the Islamic State, al-Shabaab, and the Baloch Liberation Army. See Chiara Torelli, "Explosive Violence Monitor 2022," Action on Armed Violence, 2023; Iain Overton, "Report on IED Incidents for January-June 2023," Action on Armed Violence, July 13, 2023.

[b] An estimated 16,500 IEDs were "detonated or discovered being used against U.S. forces in Afghanistan in 2011" alone. "Counter-Improvised Explosive Devices: Multiple DOD Organizations are Developing Numerous Initiatives," GAO-12-861R, U.S. Government Accountability Office, August 1, 2012.

[c] According to a recent U.S. Government Accountability Office (GAO) report on domestic terrorism, over the past decade, RMVE actors have been responsible for a 357 percent increase in domestic terrorism-related cases, accounting for many of the most violent incidents from 2010 to 2021. See "The Rising Threat of Domestic Terrorism in the U.S. and Federal Efforts to Combat It," U.S. GAO, March 2, 2023, as well as Don Rassler, *The Compound Era of U.S. Counterterrorism* (West Point, NY: Combating Terrorism Center; Tampa: Joint Special Operations University, August 2023).

[d] In 1998, the National Academy of Sciences (NAS) National Research Council issued its Containing the Threat from Illegal Bombings report. In 2018, NAS published Reducing the Threat of IED Attacks by Restricting Access to Chemical Explosive Precursors. Comparison of these reports and additional data published by the U.S. Bomb Data Center confirms that the set of precursor materials assessed most likely to present a threat remained relatively unchanged over that 20-year period. Explosive materials follow a similar trend: The use of pyrotechnics and fireworks continue to lead explosive instances in the United States by a sizable margin.

[e] As defined by the U.S. Cybersecurity and Infrastructure Security Agency, the Internet of Things (IoT) refers to "any object or device that sends and receives data automatically through the Internet. This rapidly expanding set of 'things' includes tags (also known as labels or chips that automatically track objects), sensors, and devices that interact with people and share information machine to machine." See "Securing the Internet of Things (IoT)," Cybersecurity and Infrastructure Security Agency, February 1, 2021. See also Zakria Qadir, Khoa N. Le, Nasir Saeed, and Hafiz Suliman Munawar, "Towards 6G Internet of Things: Recent advances, use cases, and open challenges," *ICT Express* 9:3 (2023).

[f] For example, some reports suggest that the Islamic State may have responded to new counter-drone measures by designing their systems "in such a way as to reduce their radar signature" including wrapping their drones in tape to avoid detection. See Arthur Holland Michel, "Counter Drone Systems," Center for the Study of the Drone, December 2019; Austin C. Doctor, "The Militant Drone Threat is No Longer New. Why Does It Still Feel Novel?" Modern War Institute, West Point, February 2, 2022.

[g] For example, the U.S. Cybersecurity and Infrastructure Security Agency Office for Bombing Prevention manages the Bomb-Making Materials Awareness Program. See "Counter-IED Resource Guide," CISA Office for Bombing Prevention, March 2017. For an example of a similar program in the European Union, see "Regulation EU 98/2013 on the marketing and use of explosives precursors," European Union Migration and Home Affairs, May 24, 2017. The U.K. Home Office requires that "Members of the public who want to import, acquire, possess or use these chemicals must hold an Explosives Precursors and Poisons (EPP) licence issued by the Home Office and an associated photographic identity document." See "Guidance: Supplying explosives precursors and poisons," United Kingdom Home Office, August 15, 2023.

[h] The JIEDDO mission has been re-organized but continues. "In March 2015, after considering a range of options, the Deputy Secretary of Defense designated JIEDDO a combat support agency focused on counter-terrorism, counter- insurgency, and other related operational areas, including counter-IED. In April 2015, JIEDDO's name was changed to JIDA to reflect this expanded mission. In February 2016 DOD renamed JIDA to JIDO and placed it under the authority of the Director, DTRA, effective October 1, 2016." For more, see "Warfighter Support: DOD Needs Strategic Outcome-Related Goals and Visibility over Its Counter-IED Efforts," U.S. GAO, GAO-12-280, February 22, 2012.

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

Austin C. Doctor is a political scientist at the University of Nebraska at Omaha and the Head of Counterterrorism Research Initiatives at the National Counterterrorism Innovation, Technology, and Education (NCITE) Center, a Department of Homeland Security Center of Excellence. He has served as a non-resident fellow with the Modern War Institute at the United States Military Academy at West Point as well as the National Strategic Research Institute, a Department of Defense University Affiliated

Research Center. His research focuses on militant actors, terrorism and political violence, irregular warfare, and emerging threats. He earned his PhD from the School of Public and International Affairs at the University of Georgia.

Sam T. Hunter is the Regents-Foundation professor of Industrial and Organizational Psychology at the University of Nebraska Omaha and Head of Strategic Initiatives at the National Counterterrorism Innovation, Education, and Technology (NCITE) Center, a Department of Homeland Security Center of Excellence. His research focuses on leadership and innovation, spanning both malevolent and benevolent application. He is a fellow in the Society of Industrial and Organizational Psychology, the National Strategic Research Institute, and the International Society for the Study of Creativity and Innovation. He earned his PhD in Industrial and Organizational Psychology from the University of Oklahoma in 2007.

Did you know?

Nobel Laureate Who Turned Explosives into Medicine Dies

Dr Ferid Murad, the American physician and pharmacologist who won the Nobel Prize in 1998 for discovering that **nitroglycerine** and other vasodilators act by releasing nitric oxide gas, passed away on September 4 at the age of 86. The transformation of nitroglycerine from an explosive agent to a cardiovascular drug, saving millions of lives, is one of the most curious stories in medicine. Discovered by the Italian physician and chemist Ascanio Sobrero in the 1840s, nitroglycerine was stabilised and then turned into dynamite by Alfred Nobel, a fact that Sobrero always regretted. Nitroglycerine's entry into medicine can be attributed to homeopaths who began prescribing it in low doses for headaches based on Sobrero's observations, noticing it lowered blood pressure instead of relieving headaches; and 19th-century workers handling dynamite, who noticed it alleviated chest pain. From the late 1870s, William Murrell and Fancourt Barnes promoted the use of nitroglycerine and amyl nitrate for angina, a practice that expanded during the early decades of the 20th century.

"So what if you found it? Whatever it is, it belongs to *ME!* Now, get off my beach!"

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

CYBER NEWS

C2BRNE DIARY

The Evolving Cybersecurity Landscape in 2024

Source: https://i-hls.com/archives/122243

Dec 27 – The ever-evolving cybersecurity landscape promises to bring new cyber threat actors, vulnerabilities, and weaknesses to counter, and as technology evolves, so do cyber threat actors' tactics, techniques, and procedures (TTPs) to take advantage of unsuspecting organizations for personal gain. Following are the top five predictions for cybersecurity threats organizations will confront in 2024, according to cybersecurity experts in HS Today:

1) Human-operated Ransomware

Human-operated ransomware attacks have been a persistent threat, and they are not going anywhere. 2023 saw major companies lose 100s of millions of dollars in very high-profile, human-operated ransomware attacks. Such attacks involved cybercriminals making fraudulent phone calls to help desks to phish for credentials, which they used to access the network and deploy ransomware. It is likely that in 2024 these attacks will get more sophisticated, with more advanced encryption techniques and diversified targets.

2) AI-generated Threats

Artificial intelligence (AI) tools have been widely adopted worldwide in many fields, including cybercrime. Cybercriminals began leveraging AI to automate and optimize their attacks, for example, to efficiently create convincing phishing messages.

In 2024 we are likely to see an increase in AI-powered malware that adapts and learns from its environment, making it more challenging to detect and mitigate in the future.

3) Supply Chain Attacks

The software supply chain is becoming an attractive target for cybercriminals as organizations get more interconnected and reliant on third-party applications. A major example from 2023 is the MOVEit cyberattacks, a file transfer tool that is used by many major companies and government entities across the US, the impact of which affected millions of people.

2024 is likely to see an increase in attacks targeting the software supply chain, aiming to compromise the integrity of widely used applications and services.

4) Mandatory Cybersecurity Self-Assessments

It is anticipated that in 2024 both the US and EU will push to implement significant cybersecurity initiatives, after the recent laws mandating the reporting of breaches involving customer data. There will probably be a push to further those laws by taking a more proactive approach to cybersecurity that includes mandatory self-assessments, requiring that organizations evaluate their cybersecurity measures, identify vulnerabilities, and implement necessary safeguards.

5) Critical Infrastructure

Political conflicts and worldwide involvement in them bring a rising threat of infrastructure cyberattacks (on energy, transportation, healthcare, and more). Such attacks can be performed for financial gain through ransom demands, geopolitical motivations, or even sabotage to destabilize a region or nation. An example is the recent attack on Iran's gas stations, which completely deactivated 70% of the country's fuel. Cybersecurity experts advise organizations to adopt a preemptive cybersecurity strategy- conduct continuous security assessments, implement employee training programs, collaborate with security experts in the industry, and emphasize that a proactive stance is key to staying ahead of emerging cyber threats.

New Dangerous Cyberattacks Target AI Systems

Source: https://i-hls.com/archives/122355

Jan 08 – A new report by Computer scientists from the National Institute of Standards and Technology presents **new kinds of cyberattacks that can "poison" AI systems.**

AI systems are being integrated into more and more aspects of our lives, from driving vehicles to helping doctors diagnose illnesses to interacting with customers as online chatbots. To perform these tasks the models are trained on vast amounts of data, which in turn helps the AI predict how to respond in a given situation.

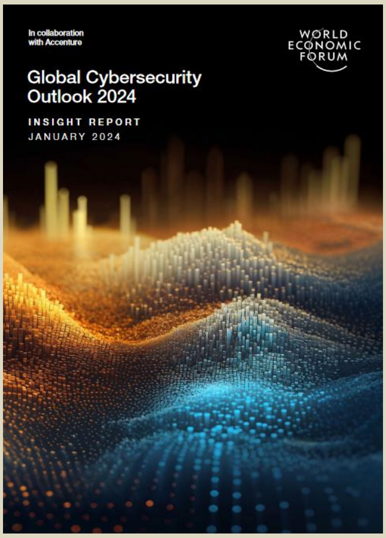
One major issue highlighted by the report is the possible corruption of that data—both during an AI system's training period and afterward, while the AI continues to refine its behaviors by interacting with the physical world. This data corruption can make the AI malfunction or straight up not work.

According to Techxplore, the report presents four major types of attacks, and then classifies them according to criteria like the attacker's goals and objectives, capabilities, and knowledge.

- **Evasion attacks** occur after an AI system is deployed and attempt to alter an input to change how the system responds to it (for example adding markings to stop signs to make an autonomous vehicle misinterpret them as speed limit signs).
- **Poisoning attacks** occur in the training phase by introducing corrupted data (for example inserting many instances of inappropriate language into conversation records so that a chatbot thinks they are common enough to use in its own customer interactions).
- **Privacy attacks** occur during deployment and are attempts to learn sensitive information about the AI or the data it was trained on in order to misuse it. Malicious actors can ask a chatbot legitimate questions, and then use the answers to reverse engineer and find the model's sources. Adding undesired examples to those online sources could make the AI behave inappropriately. Additionally, making the AI unlearn those specific undesired examples after the fact can be very difficult.
- **Abuse attacks** are the insertion of incorrect information into a source (like a webpage or online document) that an AI then absorbs. Unlike poisoning attacks, abuse attacks attempt to give the AI incorrect pieces of information from a legitimate but compromised source to repurpose the AI system's intended use.

Co-author Alina Oprea, a professor at Northeastern University, further explains that most of the mentioned attacks are fairly easy to mount and require minimum knowledge of the AI system and limited adversarial capabilities. "Poisoning attacks, for example, can be mounted by controlling a few dozen training samples, which would be a very small percentage of the entire training set," she adds.

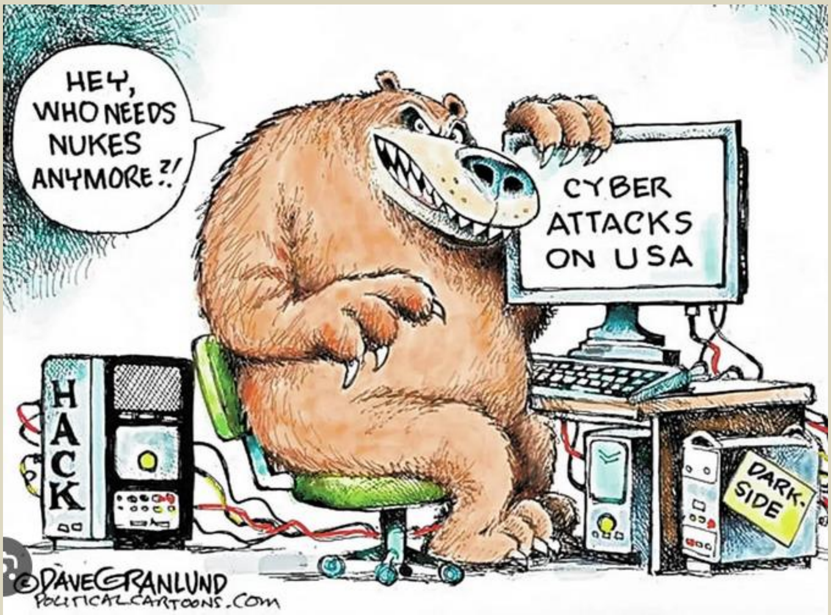
Despite breaking down each attack class and providing mitigation approaches, the research acknowledges that the defenses AI experts have devised for adversarial attacks thus far are incomplete at best. Nevertheless, having awareness of these limitations is important for developers and organizations looking to deploy and use AI technology.


In collaboration with Accenture
WORLD ECONOMIC FORUM
Global Cybersecurity Outlook 2024
INSIGHT REPORT
JANUARY 2024

Global Cybersecurity Outlook 2024

Source: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

The World Economic Forum's Global Cybersecurity Outlook 2024, produced in collaboration with Accenture, examines the cybersecurity trends that will affect economies and societies in the year to come. The report illuminates major findings and puts a spotlight on the widening cyber inequity and the profound impact of emerging technologies.


HEY, WHO NEEDS NUKES ANYMORE?!
CYBER ATTACKS ON USA
HACK
DARK SIDE
©DAVEGRANLUND POLITICALCARTOONS.COM

International CBRNE Institute

CBRNE-Terrorism Newsletter

C²BRNE DIARY

& Robotic DRONE NEWS

The Role of AI in Enhancing Robotic Bioterrorism Response

Source: https://anyuakmedia.com/the-role-of-ai-in-enhancing-robotic-bioterrorism-response/#gsc.tab=0

Dec 23 – Artificial intelligence (AI) has become an increasingly vital tool in various fields, and one area where it has shown great potential is in enhancing robotic bioterrorism response. The ability to quickly and effectively respond to bioterrorism threats is crucial in order to minimize the potential damage and protect public safety. With the integration of AI, robots can play a significant role in detecting, containing, and neutralizing these threats. One of the key advantages of using AI in robotic bioterrorism response is the ability to analyze vast amounts of data in real-time. AI algorithms can process and interpret data from various sources, such as sensors, cameras, and databases, at a much faster rate than humans. This enables robots to quickly identify potential bioterrorism threats, such as the presence of hazardous substances or abnormal patterns of behavior, and take immediate action. Furthermore, AI-powered robots can be equipped with advanced sensors and imaging technologies that enable them to detect and identify hazardous substances with high accuracy. For example, robots can be equipped with chemical sensors that can detect the presence of dangerous toxins or biological agents. By analyzing the data collected by these sensors, AI algorithms can determine the nature of the threat and provide valuable information to human responders. In addition to detection, AI can also enhance the capabilities of robots in containing and neutralizing bioterrorism threats. AI algorithms can enable robots to autonomously navigate through complex environments, such as contaminated areas or crowded spaces, in order to reach the source of the threat. This reduces the risk to human responders and allows for a more efficient and effective response. Moreover, AI can enable robots to perform tasks that would be difficult or dangerous for humans. For example, robots can be programmed to perform decontamination procedures or handle hazardous materials, minimizing the risk of exposure to human responders. AI algorithms can also enable robots to adapt and learn from their experiences, improving their performance over time and enhancing their ability to respond to new and evolving bioterrorism threats. However, it is important to note that while AI can greatly enhance robotic bioterrorism response, it is not a substitute for human expertise and decision-making. Human responders play a crucial role in interpreting the information provided by AI algorithms and making informed decisions based on their knowledge and experience. Therefore, the integration of AI in robotic bioterrorism response should be seen as a collaboration between humans and machines, with each complementing the strengths of the other. In conclusion, AI has the potential to greatly enhance robotic bioterrorism response by enabling robots to quickly detect, contain, and neutralize bioterrorism threats. The ability of AI algorithms to analyze vast amounts of data in real-time, coupled with advanced sensors and imaging technologies, allows robots to identify and respond to threats with high accuracy. However, it is important to remember that AI is not a substitute for human expertise and decision-making. The integration of AI in robotic bioterrorism response should be seen as a collaborative effort, with humans and machines working together to protect public safety.

Drone Strike on Chemical Tanker: A New Chapter in Unmanned Warfare

Source: https://bnnbreaking.com/world/us/drone-strike-on-chemical-tanker-a-new-chapter-in-unmanned-warfare/

Dec 24 – On a quiet morning in the Indian Ocean, 200 nautical miles off the coast of India, a commercial chemical tanker sailing towards its destination was jolted out of its routine by an unusual and unsettling event. A drone, identified as Iranian, struck the vessel, causing a brief fire but thankfully no casualties. This incident, while alarming, is not an isolated one. Rather, it signals a growing trend in the realm of international security – the rise of drone warfare outside traditional battlefields.

An Unseen Threat from Above

The vessel in question, the **Chem Pluto**, was not just any commercial ship. It was a Liberia-flagged, Japanese-owned, and Netherlands-operated chemical tanker, making its way from Saudi Arabia to India. The drone that hit it was a **one-way attack drone**, launched directly from Iran. This marked the seventh such attack on commercial shipping since 2021, all attributed to Iran, according to the U.S. Department of Defense.

Response and Ramifications

In response to the attack, the Indian navy promptly dispatched aircraft and a warship to offer assistance. The safety of the crew and the ship was confirmed, and the vessel was escorted by the Indian coast guard to Mumbai. Meanwhile, the U.S. military maintained communication with the ship throughout the incident. However, the implications of this drone strike extend far beyond the immediate response.

Uncharted Waters of Warfare

Such incidents of drone striking commercial vessels not only raise concerns about maritime security but also highlight the need for robust defenses against UAV threats. The trend of utilizing drones for offensive

operations outside traditional battlefields has been growing. This poses not just a security challenge, but also a diplomatic one. Iran's alleged involvement in these attacks can potentially escalate tensions with other countries that may be affected by such actions. Overall, this drone strike off the coast of India is a stark reminder of the evolving nature of war and conflict. As the world navigates these uncharted waters, the incident serves as a clarion call for enhanced maritime security measures and diplomatic efforts to mitigate such threats in the future.

World's 10 Most Advanced Military Robots

Source: https://i-hls.com/archives/122194

Dec 15 – Armies worldwide use various automated machines for military purposes, combat, cargo, intelligence gathering, and much more. The following are 10 of the world's most innovative, helpful, and deadly robots, as gathered by Interesting Engineering:

1. **MQ-28 Ghost Bat (developed by Boeing)**

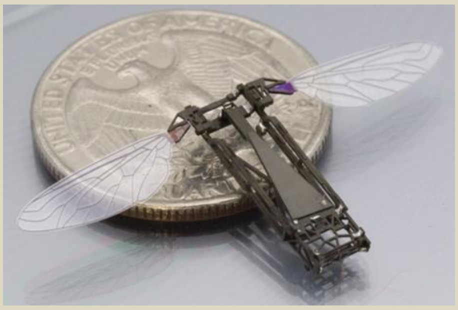
This UAV is an 11.5-meter-long wingman drone that can fly for over 3704 kilometers. The Ghost Bat is equipped with a variety of sensors and supports reconnaissance, surveillance, and intelligence missions, utilizing AI for independent flight. It can also be used in conjunction with crewed aircraft. The Ghost Bat's modular system allows the nose of the aircraft to be swapped out with those containing other equipment packages, so equipment modules can vary depending on the mission.

2. **RIPSAW M5 (developed by Howe & Howe Technologies, owned by Textron Systems)**

An unmanned ground combat vehicle (UGV) designed for speed and maneuverability on the battlefield. It can be useful in various applications, from protecting convoys and conducting rescue missions to setting up a perimeter defense, surveillance, bomb disposal, patrolling the border, and crowd control. The UGV has great situational awareness with mounted cameras providing 360-degree coverage to the operator.

3. **THeMIS (developed by Milrem Robotics)**

The THeMIS is a ground vehicle meant to reduce troop numbers on the battlefield. It can be reconfigured for transport, attack, ordnance disposal, and intelligence operations. The vehicle can reduce the load soldiers have to carry and support logistical activities at a base or for last-mile resupply. It can be used to carry mortars of up to 81mm or configured to help with quick evacuation of casualties to medical facilities.



4. **Robobee (developed by Harvard's Microbotics Laboratory)**

A tiny flying robot for both military and civilian purposes. Robobee is smaller than a quarter and can fly and swim. It is equipped with sensors and electronics that mimic the eyes and antennae of bees so it can d ynamically interact with their environment. The tiny robot could be used for reconnaissance and search missions, crop pollination, disaster relief, and high-resolution monitoring of weather. Large groups of Robobees that work together with coordinated behavior are in the works.

5. **Ghost 4 (developed by Anduril Industries)**

A quiet, smart, and modular UAS geared for intelligence, surveillance, and reconnaissance missions, but can also be used for delivering cargo, electronic warfare, or fighting intrusions. It is less than 3 meters long and has Vertical Take-Off and Landing (VTOL) capabilities. It is weatherproof can withstand high winds and other difficult flight conditions and be submerged one meter.

6. **StrykerX (developed by General Dynamics)**

The StrykerX has a wide range of technologies to support soldiers in battle and allows unprecedented cooperation with the operators. It can shoot laser weapons, launch drone attacks, and carry out electronic warfare. It has a hybrid-electric engine for quieter operations, so the vehicle can conduct reconnaissance missions. It also has an unmanned 30mm cannon for long-range firing.

7. **Jaguar (developed by the IDF and IAI)**

The Jaguar is a robotic vehicle that replaces soldiers on the battlefield and border patrol missions. The vehicle has high-resolution cameras, headlights, a communication PA system, and transmitters. The Jaguar has a machine gun that can shoot while stationary or on the move, and it can self-destruct if captured by the enemy.

8. **DOGO (developed by General Robotics)**

The small "tactical combat robot" is a UGV watchdog for soldiers in the field meant to assist in anti-terrorism operations (like urban warfare or hostage rescue). The DOGO can be controlled by a touchscreen, is armed with a 9mm Glock pistol, and can utilize its heavy-duty treads to traverse any terrain. DOGO is very portable and can be carried one-handed by a soldier. The UGV has 8 cameras, a 360-degree view, and two-way audio, which can be employed in negotiations.

9. **MAARS (developed by Qinetiq)**

MAARS (Modular Advanced Armed Robotic System) is a UGV made for reconnaissance, surveillance, and target acquisition. MAARS can keep a safe distance from enemy fire while carrying out various security missions (including ambushes, hostage rescue, using forced entry, and more). It has motion detectors, day and night cameras for driving and situational awareness, a microphone, and a loudspeaker, and it can move at 11 kph. Its weapon arsenal includes a grenade launcher and machine gun as well as non-lethal laser dazzlers and audio deterrents.

10. **SAFFiR (developed by researchers at Virginia Tech)**

Naval vessels are in particular danger from fires due to their onboard ordnance and isolation at sea, so SAFFiR (Shipboard Autonomous Firefighting Robot) was created to put out fires on naval ships. The 2-

meter-tall robot can handle fire hoses and nozzles has a wide range of motion so it can maneuver in tight and complex spaces, and can see through thick smoke thanks to its infrared stereo vision sensors, a gas sensor, LIDAR, UV cameras, and a rotating laser.

Robot dogs protect lives through innovation

By Airman Rhea Beil & Master Sgt. Delia Martinez | 2nd Bomb Wing
Source: https://www.afgsc.af.mil/News/Article-Display/Article/3624215/robot-dogs-protect-lives-through-innovation/

Dec 21 – "These robot dogs not only have the potential to save Airmen's lives, but they also serve as a reminder of how valuable your voice is, regardless of rank."

Master Sgt. Dominic Garcia, the emergency management flight chief from the **2nd Civil Engineer Squadron**, devised the concept of robot dogs and while he advanced his idea into building and testing the robots, he learned some valuable lessons along the way.

Garcia is originally from Denver, enlisted in the Air Force in 2006 and spent most of his career working under **Air Force Global Strike Command**.

In 2017, Garcia deployed to Syria from his home station at Dyess Air Force Base, Texas. After returning from his deployment Garcia reflected on his time in Syria.

"I had a really hard time adjusting back, and when you're trying to adjust back, you replay a lot of things in your head," said Garcia. "You replay certain situations, you think; what could I have done better? What could I have done differently?"

While reflecting on his deployment he remembered seeing canine teams on some of the chemical, biological, radiological, and nuclear missions. He said while he considered the things he would improve; he wondered if there was a way to arm the dogs with detectors instead of sending an entire team into a potentially hazardous environment.

In 2019, Garcia was one of six AFGSC Airmen of the Year award recipients and met people from across AFGSC. His networking led to the opportunity to bring the concept of robot dogs to life through the Air Force Work Project. AFWERX is an Air Force innovation program that connects Airmen with technology developers to turn creative ideas into a reality. While Garcia worked on his concept with AFWERX, he connected with the company Ghost Robotics who agreed to build the robot dogs.

Atom the robot dog stands as he waits for the next command to walk around the perimeter of a field Nov. 6, 2023, at Barksdale Air Force Base, La. Atom is equipped with a detector to detect Chemical, Biological, Radiological and Nuclear materials (CBRN) threats. (U.S. Air Force photo by Senior Airman William Pugh)

In 2022, Garcia and his team applied for the Silver Award Grant and they were awarded 1.25 million dollars for the project. Garcia said he was delightfully surprised as he discovered opportunities and programs as he progressed in his journey to make his robot dog idea possible.

“All I knew up until 2018 and 2019 was, if you want something done, you have to wait for policy or requirements,” said Garcia. “I didn't know that there's this whole other side of the Air Force that allows you to fast track and get what you need, kind of at the speed of relevancy to the tactical edge.”

Master Sgt. Dominic Garcia, the 2nd Civil Engineer Squadron emergency management flight chief, and Atom the Robot dog sit in a field while they listen for feedback from their team Nov. 6, 2023, at Barksdale Air Force Base, La. Garcia and his team were testing the distance of the range by using the speakers on Atom to pick up sound. (U.S. Air Force photo by Senior Airman William Pugh)

Once the robot parts were ready and delivered Garcia and his team assembled the parts into two user-friendly robotic canines.

The team tested the functionality of the newly assembled robot dogs before advancing to test their capabilities to tackle Chemical, Biological, Radiological and Nuclear materials incidents. The team tested the dogs’ CBRN readiness by putting them through radioactive sites at the Defense Nuclear Weapons School at Kirtland AFB, New Mexico.

While it might seem odd to build expensive equipment and then immediately expose it to extreme situations, this testing is necessary. Garcia created the robot dogs to replace Airmen in life-threatening situations and withstand dangerous environments. He also armed the robotic canines with detectors capable of simultaneously detecting various threats.

Garcia and his team went to the Dugway Proving Grounds in Utah to test the detectors, sensor data feedback, communication, and terrain performance.

Garcia’s focus while developing the dogs was to design equipment that could save Airmen’s lives both here in the United States and when deployed overseas. He said in addition to preventing Airmen from risking their lives, the robots could fill operational gaps and increase the manpower in hazardous specialties. Persistent to meet these goals, Garcia and his flight continue to test the robotic canines through further research and development.

Master Sgt. Dominic Garcia, the 2nd Civil Engineer Squadron emergency management flight chief, observes Atom the robot dog while he coaches his teammates as they remote control the robotic canine Nov. 6, 2023, at Barksdale Air Force Base, La. Garcia and his team test the range and capabilities of Atom in different environments. (U.S. Air Force photo by Senior Airman William Pugh)

Throughout the development of his robot dog concept, Garcia discovered a new passion for empowering Airmen to share their perspectives.

He emphasized the importance of listening to and encouraging different perspectives of his teammates. “We need to be able to say yes more and listen more,” said Garcia. “We need to be able to allow our Airmen, our sergeants, our lieutenants, whoever, to be able to give those ideas and support them because if you say no you'll never know the return on investment. But a simple yes can have so many positive effects that we don't even see sometimes.”

Prior to his innovative journey Garcia said he didn't know he could come up with a concept and receive the support to make it a reality.

Going through this process opened his eyes to the value of involving Airmen at every level, encouraging them, and supporting their ideas. Garcia said that is the reason he wanted to involve his teammates in the testing and evaluation of the robot dogs.

A team from the 2nd Civil Engineer Squadron monitors Atom the robot dog while remote controlling him Nov. 6, 2023, at Barksdale Air Force Base, La. Master Sgt. Dominic Garcia, the Civil Engineer Squadron emergency management flight chief, started integrating his two robot dogs Atom and Chappie with his new team when he moved to Barksdale earlier this year. (U.S. Air Force photo by Senior Airman William Pugh)

“This is one of the few times that we get to build by the end user, for the end user. Yes, end users test certain pieces of equipment, but very rarely do they get to build it out for an entire career flow for an entire mission,” said Garcia. “That's why I wanted to create an exposure for these guys to show them that it doesn't matter what rank you are, it doesn't matter how much experience you have in the Air Force, we all bring something to the table.” One of Garcia's flight members, Airman 1st Class Daisy Slater, an emergency management specialist from the 2nd Civil Engineer Squadron, has been learning from Garcia while they work with the robot dogs.

She said she is grateful for the opportunity to work with Garcia and learn about the dog's performance and capabilities. “I feel like getting to this flight, I've been given the opportunity to hit the ground running, so to speak,” said Slater. “There are so many NCOs and especially Airmen coming out of this flight that are making waves in the career field. And when you situate yourself next to people doing great things, it opens a door for you to also do great things."

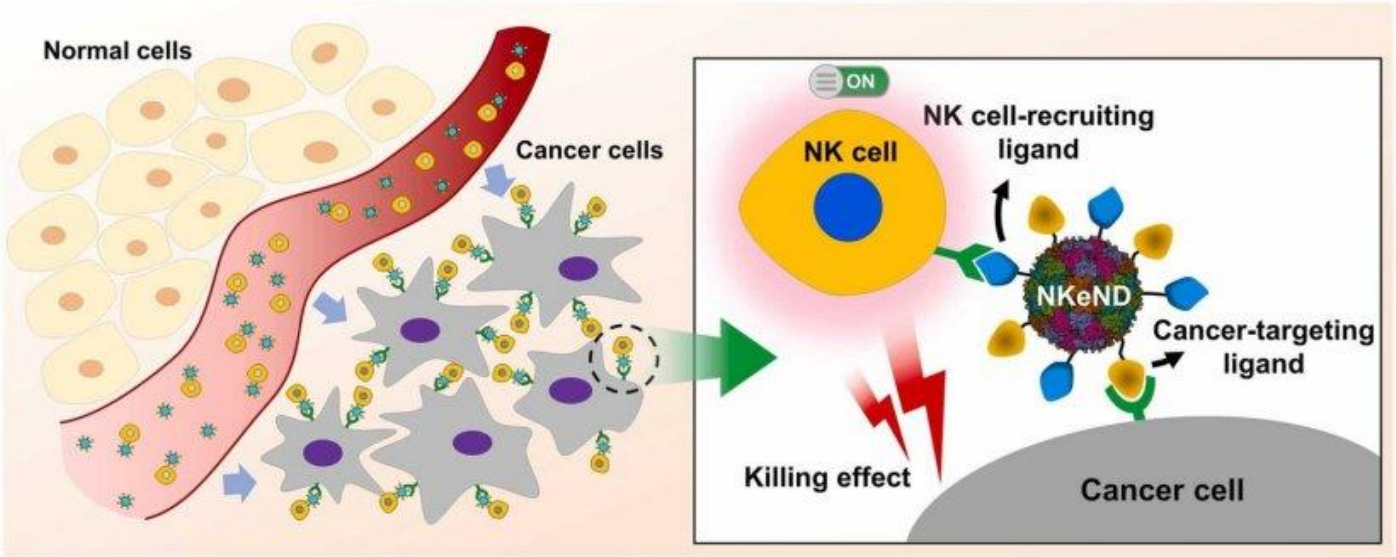
Garcia said he is inspired by the adaptability and eagerness displayed by the newer generation of Airmen and he hopes he has paved a path for the many Airmen who have innovative ideas.

"The robot dogs are amazing. I love them, and I believe they're going to save lives," said Garcia. "What we're doing for the career field, I think is awesome because we're the first ones in the whole emergency management career field doing this, but the more important message is, we need to be able to be more open."

Cancer Treating Nano-Drones

Source: https://i-hls.com/archives/122312

Jan 04 – A research team from UNIST has made a discovery that might revolutionize cancer treatment as we know it- new cell-engaging nano-drones that were designed to target and eliminate cancer cells selectively. These tiny bots are called **NK cell-engaging nano-drones (NKeNDs)**, and their success lies in their ability to engage natural killer (NK) cells, the body's frontline defenders against cancer. Using NK cells in cancer treatment is not new, but what sets these nanodrones apart is their precision.



They are engineered to zero in on cancer cells almost like guided missiles. As reported by Interesting Engineering, the research team at UNIST incorporated specific cancer-targeting and NK cell-recruiting ligands onto these nanodrones, thus achieving this groundbreaking milestone. When tested in the lab, the nanodrones showed an impressive ability to selectively bind themselves to different types of cancer cells while "rallying" NK cells to "take down" the invaders. When trialed on mice, administering the new nanodrones alongside human immune cells led to a significant slowdown in tumor growth without any harmful effects – a monumental achievement. When discussing the potential of this research, Professor Kang Se-byung excitedly emphasized the possibility of customizing treatments for various cancers using these NK cell delivery nanodrones, specifying that it is not just about targeting cancer cells but rather about doing so with precision while minimizing collateral damage.

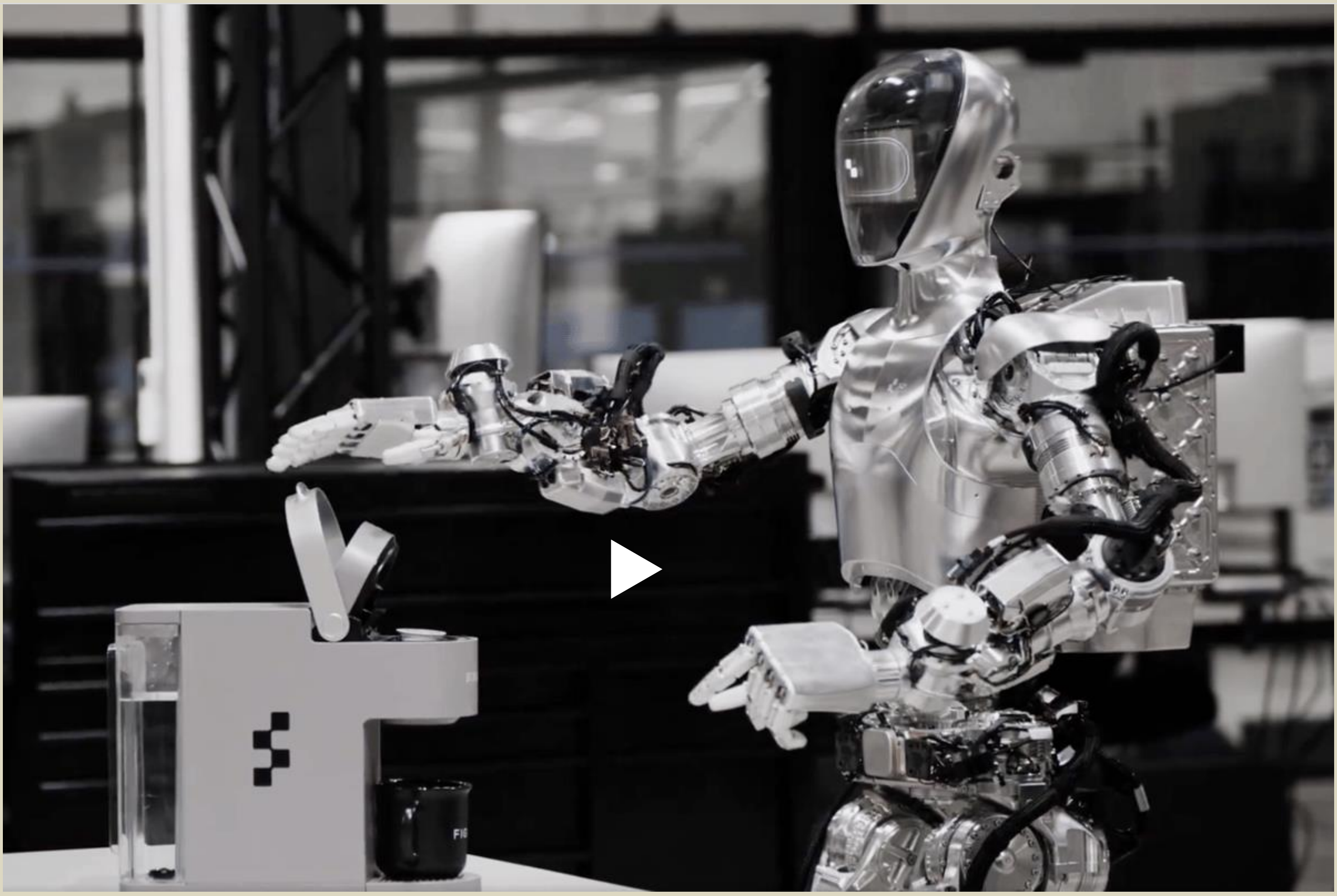
This groundbreaking study was published in Nano Today and has hopefully opened the door to a new era in cancer treatment, an era where nanodrones could be the solution for a safe and secure treatment for the relentless disease.

Figure's humanoid can now watch, learn and perform tasks autonomously

Source: https://newatlas.com/robotics/figure-humanoid-learning-tasks-autonomously/

Jan 07 – Figure's Brett Adcock claimed a "ChatGPT moment" for humanoid robotics on the weekend. Now, we know what he means: the robot can now watch humans doing tasks, build its own understanding of how to do them, and start doing them entirely autonomously.

General-purpose humanoid robots will need to handle all sorts of jobs. They'll need to understand all the tools and devices, objects, techniques and objectives we humans use to get things done, and they'll need to be as flexible and adaptable as we are in an enormous range of dynamic working environments.



Figure's 01 humanoid robot demonstrates its new watch-and-learn capabilities by autonomously using a coffee machine. Perhaps not the most spectacular demo, but this could open the floodgates to a massive acceleration of general-purpose robotics

They're not going to be useful if they need a team of programmers telling them how to do every new job; they need to be able to watch and learn – and multimodal AIs capable of watching and interpreting video, then driving robotics to replicate what they see, have been taking revolutionary strides in recent months, as evidenced by Toyota's incredible "large behavior model" demonstration in September.

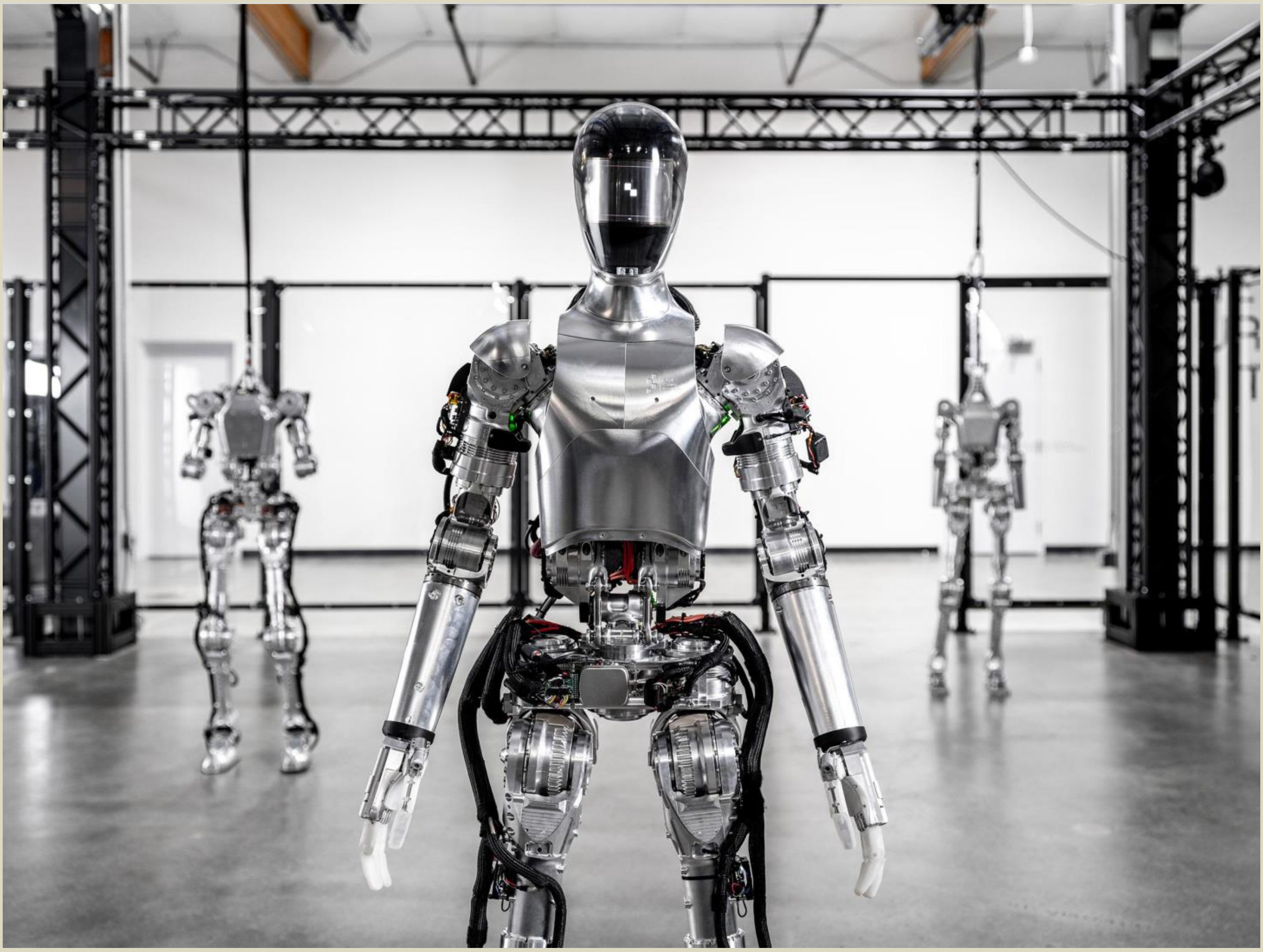
But Toyota is using bench-based robot arms, in a research center. Figure, like Tesla, Agility, and a growing number of other companies, is laser-focused on self-sufficient full-body humanoids that can theoretically go into any workplace and eventually learn to take over any human task. And these are not research programs, these companies want products out there in the market *yesterday*, starting to pay their way and get useful work done.

Adcock told us he hoped to have the 01 robot deployed and demonstrating useful work around Figure's own premises by the end of 2023 – and while that doesn't seem to have transpired at this point, a watch-and-learn capability in a humanoid is indeed big news.

The demonstration in question, mind you, is not the most Earth-shatteringly impressive task; the Figure robot is shown operating a Keurig coffee machine, with a cup already in it. It responds to a verbal command, opens the top hatch, pops a coffee pod in, closes the hatch and presses the button, and lets the guy who asked for the coffee grab the full cup out of the machine himself. Check it out: So yes, it's fair to say the human and the Keurig machine are still doing some heavy lifting here – but that's not the point. The point is, the Figure robot took 10 hours to study video, and can now do a thing by itself. It's added a new autonomous action to its library, transferrable to any other Figure robot running on the same system via swarm learning.

If that learning process is robust across a broad range of different tasks, then there's no reason why we shouldn't start seeing a new video like this every other day, as the 01 learns to do everything from peeling bananas, to putting pages in a ring binder, to screwing jar lids on and off, to using spanners, drills, angle grinders and screwdrivers.

It shouldn't be long before it can go find a cup in the kitchen, check that the Keurig's plugged in and has plenty of water in it, make the damn press-button coffee, and bring it to your desk without spilling it – a complex task making use of its walking capabilities and Large Language Model AI's ability to break things down into actionable steps.



So, don't get hung up on the coffee; watch this space. If Figure's robot really knows how to watch and learn now, we're going to feel a serious jolt of acceleration in the wild frontier of commercial humanoid robotics as 2024 starts to get underway. And even if Figure is overselling its capabilities – not that any tech startup would dream of doing such a thing – it ain't gonna be long, and there's a couple dozen other teams manically racing to ship robots with these capabilities. This is happening.

Make no mistake: humanoid robots stand to be an absolutely revolutionary technology once they're deployed at scale, capable of fundamentally changing the world in ways not even Adcock and the other leaders in this field can predict. The meteoric rise of GPT and other language model AIs has made it clear that human intelligence won't be all that special for very long, and the parallel rise of the humanoids is absolutely designed to put an end to human labor. Things are happening right now that would've been absolutely unthinkable even five years ago. We appear to be right at the tipping point of a technological and societal upheaval bigger than the agricultural or industrial revolutions, that could unlock a world of unimaginable ease and plenty, and/or possibly relegate 95% of humans to the status of zoo animals or house plants. How are you feeling about all this, folks? Personally, I'm a little wigged out. My eyebrows can only go so high, and they've been there for a good while now. I'm getting new forehead wrinkles.

Drones, Survivability, and Modern Warfare

Source: https://i-hls.com/archives/122393

Jan 10 – Drones have rapidly evolved from playing a supporting role in military operations to becoming an essential component of modern warfare, and governments worldwide need to start paying attention and learning from the use of drones in various recent conflicts, including in Ukraine, Israel, and Gaza.

According to a report by Politico, drones enable widespread real-time situational awareness, as well as improved targeting, suppression and destruction of adversary air and missile defenses. Drones, small or large, are being employed and destroyed in great numbers and are challenging concealment and survivability in the field.

As part of the Israel-Hamas war, Hamas used drones to prepare its brutal attacks on southern Israel. They did so by disabling Israeli high-tech communications, sensor networks and remote-controlled machine guns which were all meant to serve as the first line of defense against infiltrations from the Gaza Strip.

Another example of drone use is the key role they played in achieving air power dominance in the war against Russia, while counter-drone equipment and tech have become increasingly important to protect their forces. In addition, rapid drone delivery to meet the increased battlefield needs in Ukraine has led to a new dynamic approach that contributes to innovative procurement, mass production, operator training, and overall a novel approach to operations and reforms in the military's force structure.

Nevertheless, it is crucial to understand that drones don't work in isolation but rather should be regarded as a way to enhance military effectiveness. Furthermore, their effectiveness depends on their integration into a wider military architecture that combines many different capabilities across different domains, including space, cyber, intelligence fusion and processing, and electronic warfare, among others. In their research assessing the impact of drones on the modern battlefield, Politico reports finding that they are becoming indispensable for modern military operations and that their role will only expand in the future.

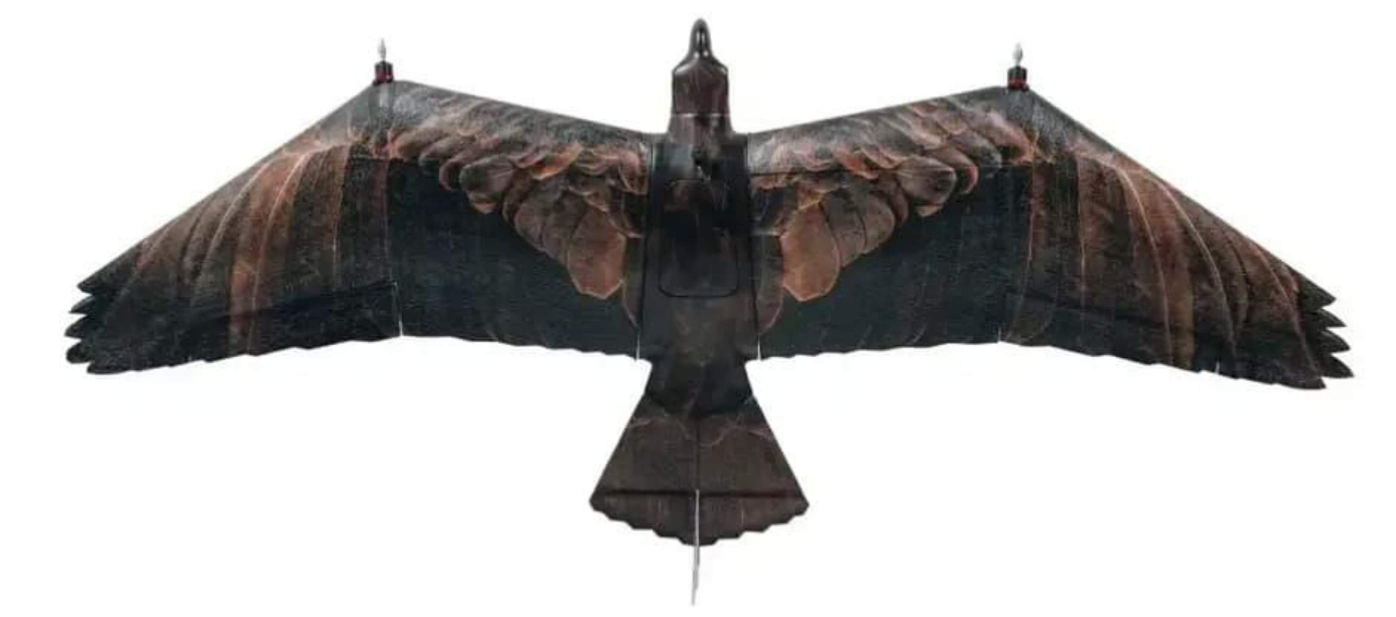
Furthermore, considering the wear and tear that small and medium drones suffer from in high-intensity conflicts, it is crucial to prioritize the replicability and affordability of these systems. Overall, while scale production and more modular designs could help bring down the cost of larger drones in the coming years, their high-end capabilities and sensor technologies remain relatively expensive- meaning that there is a need to make these platforms more survivable through specific self-protection capabilities.

Evolution Eagle drone flips the bird at enemy forces

Source: https://newatlas.com/drones/evolution-eagle-drone/

Jan 15 – If you're conducting covert military reconnaissance, you probably don't want the enemy seeing what's obviously a drone flying overhead. That's where the Evolution Eagle is intended to come in, as it's a drone that just looks like a big ol' bird.

The remote-control fixed-wing aircraft is manufactured by **Guard From Above**, a **Dutch company** that was previously known for using actual live birds of prey to intercept hostile drones.



True to its name, the Evolution Eagle is about the same size, shape and color as a real eagle. It's driven by two propellers located on the front of each of its wings, and steered by flaps along the back of its wings and tail.

Unlike some other bird-drones we've seen, it does *not* fly by flapping its wings. That sort of functionality might have made it look more eagle-like, but would have also added complexity and reduced battery life. That said, the Evolution Eagle *can* glide on thermal updrafts, just like an actual eagle. Doing so not only saves battery power, it also allows the operator to temporarily shut off the motors to eliminate operating noise. After all, real eagles don't typically make a high-pitched whining sound.

The drone is remotely piloted in real time with guidance from an onboard FPV (first person view) camera. A payload bay in its back can accommodate other hardware such as a thermal camera, mapping camera, or counter-drone system.

When not in use, the Evolution Eagle is disassembled and packed into an included TSA-approved case. It can reportedly be reassembled in just three minutes, then launched by hand.

We're still waiting to hear back regarding more in the way of specifications. In the meantime, you can see the drone in flight in the video below.

"Killer Robots" Are Coming, and UN Is Worried

By Liz Mineo

Source: https://www.homelandsecuritynewswire.com/dr20240116-killer-robots-are-coming-and-un-is-worried

Jan 16 – Long the stuff of science fiction, autonomous weapons systems, known as "killer robots," are poised to become a reality, thanks to the rapid development of artificial intelligence.

In response, international organizations have been intensifying calls for limits or even outright bans on their use. The U.N General Assembly in November adopted the first-ever resolution on these weapons systems, which can select and attack targets without human intervention.

To shed light on the legal and ethical concerns they raise, the *Gazette* interviewed Bonnie Docherty, lecturer on law at Harvard Law School's International Human Rights Clinic (IHRC), who attended some of the U.N. meetings. Docherty is also a senior researcher in the Arms Division of Human Rights Watch. This interview has been condensed and edited for length and clarity.

What exactly are killer robots? To what extent are they a reality?

Killer robots, or autonomous weapons systems to use the more technical term, are systems that choose a target and fire on it based on sensor inputs rather than human inputs. They have been under development for a while but are rapidly becoming a reality. We are increasingly concerned about them because weapons systems with significant autonomy over the use of force are already being used on the battlefield.

What are those? Where have they been used?

It's a little bit of a fine line about what counts as a killer robot and what doesn't. Some systems that were used in Libya and others that have been used in [the ethnic and territorial conflict between Armenia and Azerbaijan over] Nagorno-Karabakh show significant autonomy in the sense that they can operate on their own to identify a target and to attack.

They're called loitering munitions, and they are increasingly using autonomy that allows them to hover above the battlefield and wait to attack until they sense a target. Whether systems are considered killer robots depends on specific factors, such as the degree of human control, but these weapons show the dangers of autonomy in military technology.

What are the ethical concerns posed by killer robots?

The ethical concerns are very serious. Delegating life-and-death decisions to machines crosses a red line for many people. It would dehumanize violence and boil down humans to numerical values.

There's also a serious risk of algorithmic bias, where discriminating against people based on race, gender, disability, and so forth is possible because machines may be intentionally programmed to look for certain criteria or may unintentionally become biased. There's ample evidence that artificial intelligence can become biased. We in the human-rights community are very concerned about this being used in machines that are designed to kill.

What are the legal concerns?

There are also very serious legal concerns, such as the inability for machines to distinguish soldiers from civilians. They're going to have particular trouble doing so in a climate where combatants mingle with civilians.

Even if the technology can overcome that problem, they lack human judgment. That is important for what's called the proportionality test, where you're weighing whether civilian harm is greater than military advantage.

That test requires a human to make an ethical and legal decision. That's a judgment that cannot be programmed into a machine because there are an infinite number of situations that happen on the battlefield. And you can't program a machine to deal with an infinite number of situations.

There is also concern about the lack of accountability.

We're very concerned about the use of autonomous weapons systems falling in an accountability gap because, obviously, you can't hold the weapon system itself accountable.

It would also be legally challenging and arguably unfair to hold an operator responsible for the actions of a system that was operating autonomously. There are also difficulties with holding weapons manufacturers responsible under tort law. There is wide concern among states and militaries and other people that these autonomous weapons could fall through a gap in responsibility.

We also believe that the use of these weapons systems would undermine existing international criminal law by creating a gap in the framework; it would create something that's not covered by existing criminal law.

There have been efforts to ban killer robots, but they have been unsuccessful so far. Why is that?

There are certain countries who oppose any action to address the concerns these weapons raise — Russia in particular. Some countries, such as the U.S., the U.K., and so forth, have supported nonbinding rules. We believe that a binding treaty is the only answer to dealing with such grave concerns.

Most of the countries that have sought either nonbinding rules or no action whatsoever are those that are in the process of developing the technology and clearly don't want to give up the option to use it down the road.

There could be several reasons why it has been challenging to ban these weapons systems. These are weapons systems that are in development as we speak, unlike landmines and cluster munitions that had already existed for a while when they were banned. We could show documented harm with landmines and cluster munitions, and that is a factor that moves people to action — when there's already harm. In the case of blinding lasers, it was a pre-emptive ban [to ensure they will be used only on optical equipment, not on military personnel] so that is a good parallel for autonomous weapons systems, although these weapons systems are a much broader category. There's also a different political climate right now. Worldwide, there is a much more conservative political climate, which has made disarmament more challenging.

What are your thoughts on the U.S. government's position?

We believe they fall short of what a solution should be. We think that we need legally binding rules that are much stronger than what the U.S. government is proposing and that they need to include prohibitions of certain kinds of autonomous weapons systems, and they need to be obligations, not simply recommendations.

There was a recent development in the U.N. recently in the decade-long effort to ban these weapons systems.
The disarmament committee, the U.N. General Assembly’s First Committee on Disarmament and International Security, adopted in November by a wide margin —164 states in favor and five states against — a resolution calling on the U.N. secretary-general to gather the opinions of states and civil society on autonomous weapons systems.
Although it seems like a small step, it’s a crucial step forward. It changes the center of the discussion to the General Assembly from the Convention on Conventional Weapons (CCW), where progress has been very slow and has been blocked by Russia and other states. The U.N. General Assembly (UNGA) includes more states and operates by voting rather than consensus.
Many states, over 100, have said that they support a new treaty that includes prohibitions and regulations on autonomous weapons systems. That combined with the increased use of these systems in the real world have converged to drive action on the diplomatic front.
The secretary-general has said that by 2026 he would like to see a new treaty. A treaty emerging from the UNGA could consider a wider range of topics such as human rights, law, ethics, and not just be limited to humanitarian law. We’re very hopeful that this will be a game-shifter in the coming years.

What would an international ban on autonomous weapons systems entail, and how probable is it that this will happen soon?
We are calling for a treaty that has three parts to it. One is a ban on autonomous weapons systems that lack meaningful human control. We are also calling for a ban on autonomous weapons systems that target people because they raise concerns about discrimination and ethical challenges. The third prong is that we’re calling for regulations on all other autonomous weapons systems to ensure that they can only be used within a certain geographic or temporal scope. We’re optimistic that states will adopt such a treaty in the next few years.

Liz Mineo is a Harvard Staff Writer.

Don’t Bring a Patriot to a Drone Fight—Bring Fighter UAVS Instead

By Paul Maxwell
Source: https://www.homelandsecuritynewswire.com/dr20240117-don-t-bring-a-patriot-to-a-drone-fight-bring-fighter-uavs-instead

Jan 17 – Recent conflicts such as the war in Ukraine and the 2020 war in Nagorno-Karabakh demonstrate the growing importance of unmanned aerial vehicles. UAVs are a constant threat on the modern battlefield. These platforms conduct reconnaissance, attack ground targets, and perform as loitering munitions. They range from low-cost commercial, off-the-shelf devices to defense industry products such as the Iranian Shahed-131. By some estimates, UAVs are so prolific that the Ukrainian military alone loses over ten thousand platforms per month. Some Ukrainian forces report that it is not unusual to have twenty or more overflights per day by hostile drones. The availability and capabilities of these platforms make the battlefield dangerous in an entirely new way.
Naturally, there have been attempts to defeat this new threat. Some resort to traditional antiaircraft systems, such as ZU-23-2 antiaircraft guns, small arms, or surface-to-air missiles. These approaches are sometimes effective but are not ideal. Hitting a very small, fast target with relatively larger-caliber rounds is challenging. Alternatively, expending many thousands (if not millions) of dollars on each missile to eliminate an inexpensive UAV is an economically losing affair. Other means to defeat this growing threat include devices that use the electromagnetic spectrum. This can vary from jamming systems (GPS denial, communications link denial) to directed-energy weapons such as lasers and microwaves. Though effective at times, these devices come with trade-offs such as interference with friendly systems and the loud invitation to opposing artillery once the signals are detected. No matter the defense mechanism chosen, there just are not enough systems to provide sufficient protection against swarms of UAVs. Air defenses are typically fielded in just enough quantities to defend high-value targets and not much else. The average grunt on the battlefield is left victim to the terror in the skies. The solution to this dilemma is to take the next step in UAV evolution: air superiority drones.

A Page from History

To clearly see why air superiority UAVs (or fighter UAVs) are the natural next step, one only needs to examine the relatively recent history of powered flight in combat. Shortly after the Wright brothers succeeded in demonstrating that powered flight was feasible, the militaries of the world began research into the use of this new technology in combat. Developing aircraft, pilots, and supply chains to make systems at scale became priorities for many nations.

The first step in the combat application of powered flight was for reconnaissance. This was an obvious mission for aircraft as balloons had already demonstrated their value as signaling and targeting platforms in previous conflicts, including the American Civil War. In the prewar years of 1911–1914, developing aircraft to conduct reconnaissance was important. As World War I began, the value of the airplane to detect enemy movements, guide artillery fire, and perform other intelligence, surveillance, and reconnaissance missions became clear. The traditional scout (cavalry) had lost its value as trench warfare became prevalent. Other means of reconnaissance were needed.

It wasn't very long into the war before ambitious pilots began to extend their mission sets into ground attack roles. Despite the lack of specifically developed bombers, pilots began to use aircraft to attack ground targets using items ranging from hand-dropped flechettes to grenades to small-caliber shells. This soon led to ground attack roles being deliberately incorporated into military air operations. Due to the exposure of ground forces to aerial reconnaissance platforms and burgeoning ground-attack systems, air defense mechanisms became an important developmental area. Of course, ground-based systems (antiaircraft weapons) were a component of this new defensive technology. In parallel, development of fighter aircraft whose purpose was to defeat enemy aircraft occurred. This began initially with crew members simply carrying small arms and then evolved to integrated automatic weapons. Instead of relying solely on ground defenses, militaries realized the value of air-based defenses against aerial threats. From those days forward, a key component of powered air combat systems were the air superiority fighters whose mission was to defeat enemy aircraft while in flight.

UAVs in modern combat have followed a similar trajectory as manned, powered aircraft. First were the intelligence, surveillance, and reconnaissance drones. Then came the ground-attack systems. Given this path and the inability of ground-based systems to defend the skies against the swarms of UAVs, the next logical step is the fighter UAV. This need was demonstrated by the first recorded air-to-air engagement by a Ukrainian drone and Ukrainian research into fighter drone development.

Developing the UAV Fighter Squadron

Research into autonomous fighter aircraft is not new. Systems are already being experimented on, such as autonomous wingmen and the Air Combat Evolution AI for autonomous fighter aircraft. However, all of these efforts are focused on large, expensive platforms that attack and defend against traditional jet aircraft found in modern air forces. Certainly, these systems will be useful in future conflicts and they have an important role against traditional and future air war threats. However, they will not solve the issues found at the lowest levels on the modern battlefield.

What militaries need quickly are small, cheap (a.k.a. disposable) platforms that can defend against the numerous commercial, off-the-shelf UAVs that cloud the battlefield. Ahead of the military in this area is the Aerial Sports League's Drone Combat Games, which pits two small UAVs against each other in a fight to the death. Small companies are also emerging in this field to fill the gap with products such as the DroneHunter F700. Whatever the development path is, there are important features required for these systems to be successful.

The first and probably most important aspect of air superiority drones is that they must be inexpensive and practically disposable. Militaries cannot afford in quantity traditionally priced aircraft when the threat is cheap and effective. Defense in this manner may be temporarily feasible but will not be successful over the course of long conflicts as resources will limit availability. Low cost will also help ensure that the lowest-level units can receive defensive capability that was previously only available to protect more valuable assets.

Next, these fighter systems will require significant autonomy. At a minimum, they should be able to fly patrol patterns without user intervention, detect threat aircraft, calculate intercept courses, and communicate intelligence data to relevant systems all at the speed of modern technology. Ideally, these aircraft would also be able to cooperate with other fighter UAVs to deconflict targets, identify priority targets, and engage threats automatically. Given that the threat is similarly unmanned, the ethics and challenges associated with autonomous targeting should be less difficult to overcome. Mistakes made in the destruction of unmanned drones should not be a major ethical or legal concern. Overall, these aircraft should be as simple to use as commercial UAVs that automate many flight tasks. Common user interfaces (e.g., smartphone, tablet) for these UAVs should prevail and point-and-click route setting utilized. Soldiers should not require days and weeks of training to use these systems.

The last challenge for the development of small UAV fighters (and other UAVs) is integration into the battlefield environment. These systems should not be owned by the traditional air superiority services, but possessed by any ground unit that requires UAV defenses. Given the presence of other aerial platforms, airspace management will become more challenging especially as new aircraft owners will exist who aren't part of existing airspace planning efforts. To achieve the density and effectiveness of the fighter UAV while maintaining the safety of other aircraft, rules on airspace use will need to be developed. Whether it's deconfliction by altitude, time, or location, new rules will need to provide some organization to the skies. These rules will protect by design the other airspace users as the air superiority UAVs are expendable. Additionally, fighter UAVs should be incorporated into the overall air defense common operational picture.

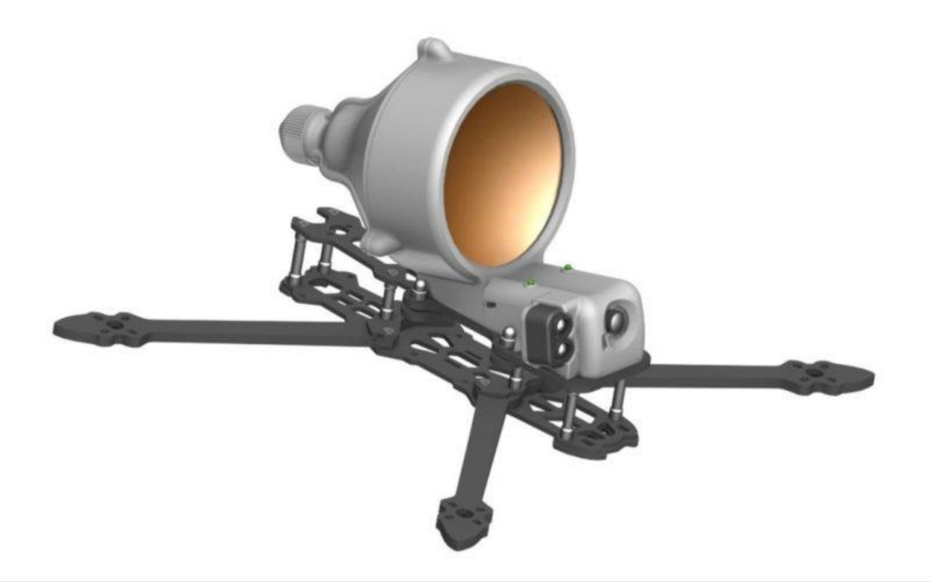
Air defenders should know where systems are located and what their capabilities are to synchronize defenses to their best potential. This will help to protect friendly ground forces from this evolving threat.

UAVs from small to large have altered the modern battlefield and the airspace above it. What was once the domain of air combat services is now an open melee of aircraft. Air defenses have not evolved quickly enough to defeat this new threat and where they have grown, they are proving insufficient. The time has come for air-to-air combat UAVs to be developed and fielded. For the US military to be prepared, it must combat UAV threats not with Cold War technology but instead with modern UAV technology.

Retired Lieutenant Colonel Paul Maxwell is the deputy director of the Army Cyber Institute at the United States Military Academy.

Ukraine develops armor-piercing ammunition for FPV drones

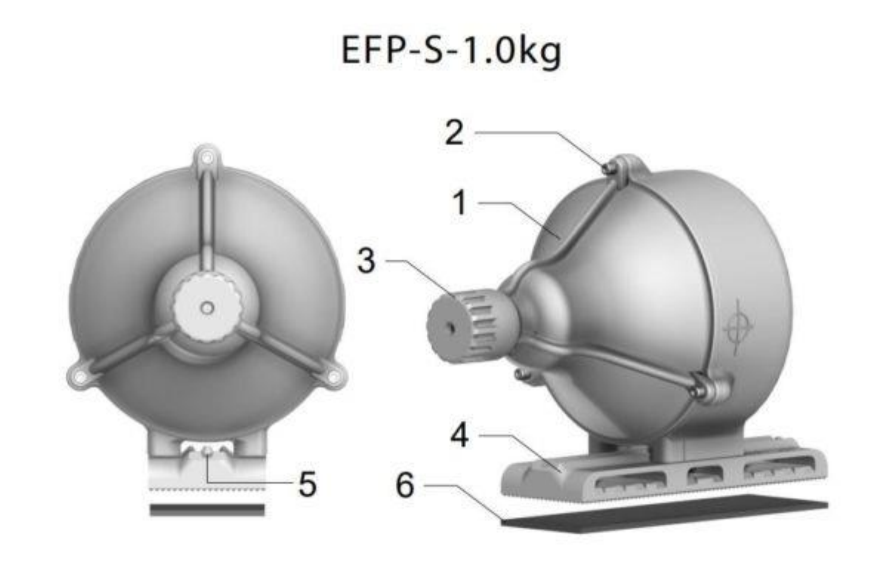
Source: https://euromaidanpress.com/2024/01/15/ukraine-develops-armor-piercing-ammunition-for-fpv-drones/



FPV drone with armor-piercing ammunition. Credit: Army of Drones/TG

Ukrainian engineers have developed EFP-S armor-piercing ammunition for FPV (first-person view) drones to target lightly armored vehicles. The Army of Drones project reported this advancement, noting its effectiveness against lightly armored vehicles like self-propelled artillery units, infantry fighting vehicles, and armored personnel carriers, even those protected with anti-cumulative and anti-drone measures.

Ukraine has been successfully using small FPV drones on the frontline, attacking Russian equipment, vehicles, and military personnel. Still, often, the impact force of a single FPV drone is not enough to penetrate an armored vehicle and destroy it.



The EFP-S ammunition's combat part features an "impact core" that ensures powerful behind-armor action and a considerable remote striking distance. According to the provided specifications, the ammunition weighs 165 grams, has a velocity of 1800 meters per second, and has an effective blast radius of 8 meters.

The composition of EFP-S includes:

1. Detachable parts of the body
2. Screws for securing the detachable part
3. A cap for fixing the detonator
4. An adapter for mounting to the drone frame
5. A sight for calibrating the course camera
6. Rubber padding

The design is attached to an FPV drone using nylon ties, showcasing a blend of simplicity and effectiveness in its construction and deployment.

Earlier, Ukraine's Minister of Digital Transformation, Mykhailo Fedorov, urged Ukrainians to participate in a free training program to assemble FPV for army drones at home.

Drone Delivery Canada secures BVLOS dangerous cargo approval

Source: https://dronedj.com/2024/01/10/drone-delivery-canada-secures-bvlos-dangerous-cargo-approval/

Jan 10 – Canadian UAV transport specialist Drone Delivery Canada has effectively fused two different operational authorizations it had earned from regulators in past into a unified approval to fly beyond visual line of sight missions (BVLOS) while carrying medical payloads classified as dangerous cargo.

Toronto-based Drone Delivery Canada announced the news this week, saying it had secured authorization from Transport Canada to fly payloads designated as dangerous during BVLOS operations between medical facilities. The startup said the dual capacity approval will facilitate its UAV transport of blood products, patient test samples, and other sensitive cargo throughout its 3.4-kilometer DroneCare route.

Drone Delivery Canada had previously worked to obtain permission from the nation's regulator to operate BVLOS flights in the DroneCare corridor, and had elsewhere qualified for flying UAV transport of medical supplies officially categorized as dangerous. In combining the two in the additional authorization, the company says it will be able to efficiently and affordably shuttle sensitive payloads between Toronto area Milton District and Oakville Trafalgar Memorial Hospital using its Canary craft.Drone Delivery Canada said the enhanced BVLOS capabilities will permit it to transport such supplies as blood and serum chemistry tests; blood bank materials; urine cultures; small cytology containers with formalin; and blood culture bottles. In addition, the startup celebrated what is said was among the first BVLOS approvals in Canada in "an aerodrome environment" in which traditional aircraft also operate.

"DDC continues to push the boundaries of drone delivery and this approval is a testament to our efforts to ensure we deploy a safe and efficient drone logistics system," said Steve Magirias, CEO of Drone Delivery Canada. "This also continues our work in the healthcare vertical which is an important market for DDC. With BVLOS flights and dangerous goods transportation authorization, we will continue to transform the way healthcare supplies are transported, ensuring faster delivery times and enhancing overall patient care." Drone Delivery Canada operates using a combination of proprietary software and cutting-edge hardware and makes those assets available to government and global corporate organizations as models of Software-as-a-Service activities.

How the Drone War in Ukraine Is Transforming Conflict

By Kristen D. Thompson

Source: https://www.homelandsecuritynewswire.com/dr20240118-how-the-drone-war-in-ukraine-is-transforming-conflict

Jan 18 – From drones that fit in the palm of the hand to drones weighing more than 1,000 pounds (454 kilograms), Ukraine has built and acquired a diverse fleet of remotely piloted aircraft to complicate and frustrate Russia's advances. The constantly evolving scope of this technology and its ever-growing use signal not only the potential for drones to level the playing field in the Russia-Ukraine war, but also their ability to influence how future conflicts are waged.

Why Is the War in Ukraine a Hotbed for Drones?

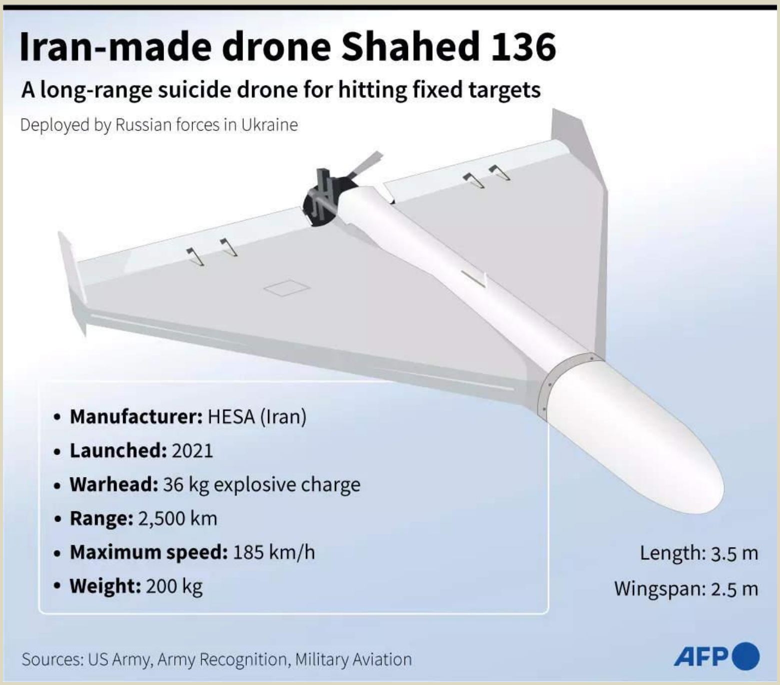
As the war enters its third calendar year, neither side is close to achieving air superiority. Most military analysts expected that Russia, with its superior air power, would quickly seize control of contested airspace early in the conflict. But surprisingly, Ukraine's defenses, later bolstered by Western systems, were able to repel and deter Russian aircraft from making near-border and cross-border strikes. The inability of either side to break through the other's integrated air defenses has forced them to increase the agility of their fielded forces and rely more heavily on standoff weapons, including long-range artillery, missiles, and drones. These conditions have led to the development of new drone technologies that could help Ukraine level the playing field in the air battle and possibly turn the tide of the war in its favor.

What Technologies Are in Use?

Ukraine's drone deployment has evolved with the changing battlefield. During earlier stages of the war—when Russia's air defense and electronic-warfare capabilities were less pronounced—Ukraine relied on larger drones such as the Turkish TB2 Bayraktar to great effect. The TB2's ability to carry multiple air-to-ground munitions and loiter for long periods allowed Ukrainian forces to penetrate Russian air defenses and strike heavy targets. However, as time progressed and Russia took greater control of the skies, it was able to detect and shoot down these larger models more easily. The TB2 may maintain some relevance—its sensor suite and considerable range still enable Ukrainian operators to collect intelligence—but Ukraine has nonetheless shifted to using smaller drone technology to adapt to Russian advances.

The more abundant, smaller drones are proving to be serious game changers in that they have given Ukraine better battlespace awareness and more capability to hit targets. The Ukrainians have tapped into commercial technology—the same recreational products available to civilians—to get cheap, off-the-shelf drones onto the battlefield quickly. Many of these "hobbyist" drones have been acquired through grassroots crowdfunding efforts, or "dronations." At just one thousand dollars per unit, the small drones can be rapidly amassed and repurposed by operators for a specific effect. For example, the popular first-person view (FPV) drones commonly used for racing or filmmaking are retrofitted with makeshift explosives and flown to strike fixed targets at relatively low cost. These drones can carry out single-use strikes with high precision while remaining less susceptible to Russian air defense systems. Additionally, the Ukrainians have repurposed significant aspects of their domestic economy to support the new drone supply chain, increasing their drone-making capabilities through public-private partnerships. One year ago, Ukraine had seven domestic drone manufacturers and it now has at least eighty.

As for Russian drone technology, Moscow deploys indigenous models, such as the Orion, Eleron-3, Orlan-10, and Lancet, but Western sanctions on crucial Russian supply chains have prevented Moscow from excelling in drone production. Instead, Russia has turned to Iran for a steady supply. The Russians now boast an extensive fleet of Iranian-made Shahed-136 drones that can carry 100 pounds (45.4 kilograms) of explosives over a range of 1,200 miles (1931 kilometers).


Iran-made drone Shahed 136
A long-range suicide drone for hitting fixed targets
Deployed by Russian forces in Ukraine
• Manufacturer: HESA (Iran)
• Launched: 2021
• Warhead: 36 kg explosive charge
• Range: 2,500 km
• Maximum speed: 185 km/h
• Weight: 200 kg
Length: 3.5 m
Wingspan: 2.5 m
Sources: US Army, Army Recognition, Military Aviation
AFP

How Are Drones Shaping the War?

This conflict has demonstrated the battlefield advantages of drones, which have become smaller, more lethal, easier to operate, and available to almost anyone. They compress the so-called kill chain, shortening the time from when a target is detected to when it is destroyed, and they can bolster a military's ability to reconnoiter the forward edge of the battlefield. Drones with longer endurance profiles can effectively conduct hours of reconnaissance, enabling other, more advanced drones to carry out precision strikes deep inside enemy territory. Other models enable individual soldiers to monitor adversary movement without risking lives or giving up the soldier's position.

Drones can also play an important international humanitarian role, for instance, by conducting battle and collateral damage assessments or exposing war crimes. U.S. drone manufacturer Skydio recently donated nine drones that—with their high-resolution cameras—will be used to help Ukraine document potential Russian war crimes. Through the U.S. Agency for International Development (USAID), images captured will be used to aid the Office of the Prosecutor General in documenting many instances of human rights abuses.

What Are the Defenses Against Drones?

Drones are susceptible to air defenses. Larger drones with a distinct radar cross-section are easy, slow-moving targets for air defense interceptors and anti-drone guns; both Ukraine and Russia have downed thousands of drones with their interceptors and artillery. However, the continual use of these systems by both Ukraine and Russia can be prohibitively costly, as a single drone could cost thousands or even millions of dollars to intercept.

An emerging challenge of counter-drone defense is the need to develop and employ a system that is cheaper than its target. Crucially, smaller drones that can swarm toward a target are more difficult to shoot down. as they can overwhelm air defense systems. A key countermeasure has been to utilize electronic warfare in the form of jammers, spoofers, and high-energy lasers that prevent drones from reaching their target. Jammers—used by both Russia and Ukraine—send out powerful electromagnetic signals that can cause a target drone to fall to the ground, veer off course, or turn around and attack its operator. As the war progresses, both sides are continually investing in and adapting electronic warfare tactics to counter the innovations of their adversary.

How Will the Drone War Evolve?

The Russia-Ukraine conflict has demonstrated that innovations in drone technology can change the balance of power in the air defense domain especially. While Russia seeks to build pockets of air superiority and bolster its drone production and anti-drone defenses, Ukraine continues to develop both more and less sophisticated solutions. In a recently uncovered partnership project with Iran, Russia finished constructing a drone factory in Tatarstan, 500 miles (805 kilometers) east of Moscow, where it could produce an estimated six thousand Shahed-136 prototypes (renamed the Geran-2 by Moscow) by mid-2025. This expanded drone production could be enough to counter Russia's shortage of drones on the front lines and turn the tide of the conflict in its favor. However, Ukraine's ability to acquire and crowdsource commercial drone technology, tactically modify drones in the field based on real-time feedback, and alter tactics to defeat anti-drone systems have proved to be crucial to its war effort. Even while overmatched force-wise, Ukraine has shown how savvy technological adaptation can change twenty-first century warfare and could tip the balance of power in favor of the force that is more innovative.

Kristen D. Thompson is Military Fellow, *U.S.* Air Force, at *CFR*.

DragonFire laser: MoD tests weapon as low-cost alternative to missiles

Source: https://www.bbc.com/news/uk-68031257

Jan 19 – The UK has successfully fired a high-power laser weapon against an aerial target for the first time in a trial.

It is hoped that the test will pave the way for a low-cost alternative to missiles to shoot down targets like drones.

The DragonFire weapon is precise enough to hit a £1 coin from a kilometre away, the Ministry of Defence (MoD) says.

It described the test, at its Hebrides Range in Scotland, as a "major step" in bringing the technology into service.

Defence Secretary Grant Shapps said the technology could reduce "the reliance on expensive ammunition, while also lowering the risk of collateral damage".

The MoD says both the Army and Royal Navy are considering using the technology as part of their future air defence capabilities.

While laser weaponry might sound like something from science fiction the US Navy has already installed systems on several destroyers.

However, missiles rather than lasers have been used to shoot down drones during the current conflict with Houthis in the Red Sea. Missiles can be far more expensive than the drones they destroy, with some costing millions of pounds compared to a few thousand.

The MoD says firing the DragonFire system for 10 seconds is the cost equivalent of using a regular heater for an hour, with the **cost of operating it typically less than £10 per shot**.

Laser-directed energy weapons (LDEWs) use an intense light beam to cut through their target and can strike at the speed of light.

The range of the DragonFire system is classified but it is a line-of-sight weapon, meaning it can attack any visible target within range. It is being developed by the Defence Science and Technology Laboratory (Dstl), alongside some industry partners, on behalf of the MoD. Dstl's chief executive Dr Paul Hollinshead said: "These trials have seen us take a huge step forward in realising the potential opportunities and understanding the threats posed by directed energy weapons."

The DragonFire weapon system is the result of a £100m joint investment by the MoD and industry.

The development of laser weapons comes amid the increasing use of drones in warfare, which has been seen during the conflict between Ukraine and Russia, with Russia believed to be using Iranian-made "kamikaze" drones to attack Ukrainian cities.

Ukraine, which also uses some "kamikaze" drones, has created its own "army of drones" which has seen the use of hobby drones for military purposes.

Small, Cheap and Numerous: A Military Revolution Is Upon Us

By Bradley Perrett | *Defense and aerospace journalist.*

Source: https://www.homelandsecuritynewswire.com/dr20240122-small-cheap-and-numerous-a-military-revolution-is-upon-us

Jan 22 – Armed forces usually adapt slowly in peacetime, resisting change. Well, only the most hidebound will be ignoring the revolution in military affairs under way in Ukraine and the Red Sea.

For want of a better name, call it the cheap-drone revolution.

Just one example highlights how it's changing things. Formerly a guided missile would hardly be used to kill a single enemy soldier. The missile would cost hundreds of thousands of dollars, so it would be in limited supply and reserved for a much more important target, typically an armored vehicle.

Now in Ukraine a guided missile may indeed be aimed at just one soldier. We'd recognize the weapon as a drone, but functionally it's a guided weapon with a revolutionary characteristic: by military standards, it's incredibly cheap. That cheapness is upending warfare. A big change in military affairs has long been predicted, one in which big, costly and scarce weapons would be challenged by things that would be small, cheap and numerous. In the Middle East and especially in Ukraine, the revolution is upon us.

What's missing so far is another predicted characteristic in little weapons and sensors of the future: high autonomy. For that, just wait. Drones that aren't expended as missiles are cheap, too. In Ukraine they're doing the work of crewed aircraft costing 10 or even 10,000 times as much and doing it without risking the lives of anyone aboard.

So these miniature missiles and tiny attack and reconnaissance aircraft are suddenly abundant in warfare. Some are small airplanes; others are little helicopters with four or more rotors for lift. In a wide variety of sizes, they're swarming over the battlefield in Ukraine, multiplying the risks faced by valuable targets such as armored vehicles, trucks, command posts, artillery, air-defense batteries and ammunition depots. Because they're cheap and easy to use, little drones are weapons for terrorists, too.

This is a massive new challenge for armed forces, especially for armies and navies. We don't have much insight into what, if anything, the Australian Defense Force and Department of Defense are doing about it.

Companies around the world, including Electro Optic Systems in Canberra, are rushing to come up with better ways of shooting down drones. The great problem is that the traditional methods of destroying aircraft cost more than many of the drones do. So these firms, among which EOS is a leader, are focusing on weapons that can hit at extremely low cost.

For example, since Israeli forces entered Gaza in November, one-way drones launched by Houthi militants in Yemen have flown towards Israel and especially merchant ships in the Red Sea. US and British warships have been shooting them down but have probably used at least one multi-million-dollar interceptor missile every time. Even the better Houthi drones probably cost tens of thousands of dollars each. Iran, the Houthis' drone supplier, would be well satisfied with the transactions.

On battlefields in Ukraine, a startling development has been the military use of first-person-view (FPV) drones—miniature multi-rotor helicopters originally conceived for civil purposes. A user with a radio link sees what the drone's camera sees and can use the aircraft to take pictures or just enjoy racing the thing around.

Add an explosive charge to an FPV drone and you have a precision guided missile. An operator may, for example, guide it to hit and blast through the thin top of an infantry fighting vehicle (IFV) that has nine soldiers inside.

The cost of the IFV might have been tens of millions of dollars. Add to that the loss of the dead or maimed soldiers. The FPV drone probably didn't cost more than $5000, maybe far less, and its operator could have sat safely in a basement many kilometers away.

Formerly the IFV would have been attacked with a rocket-propelled missile costing more than $100,000. The person who fired it needed a direct view of the IFV and was therefore less likely than a drone operator to get a shot. The shooter was also in some danger when the opportunity arose.

Or a similar rocket-propelled missile could have been fired from a $100 million helicopter with two crew members aboard who risked being shot down.

An FPV missile drone is indeed cheap enough to use against a single soldier. In fact, such attacks in Ukraine so far may have been made mostly because an operator couldn't find a more important target. But launching kamikaze FPVs specifically to hit individuals is likely to become frequent when supply of the equipment becomes sufficient.

Meanwhile, drones that return for reuse are routinely making bombing attacks against infantry as well as other targets—for example, by dropping grenades into trenches. Formerly, soldiers on the front line who needed an air strike against an enemy position would send a request up the line and hope that a mighty attack helicopter or fighter aircraft would be assigned to the job. Now they can do it themselves.

Drones are roaming over the battlefield in their thousands to find out what's hiding where. Even if they aren't carrying weapons, their reconnaissance pictures can be used to call in strikes by artillery, rockets or other drones.

Armies and their suppliers need to think hard and fast about what to do about all this. One answer is to jam drones' radio links—and that may work, if the jammer is powerful, in the right location and transmitting on the right frequency.

Shooting drones down is most desirable, but the enormous difficulty is finding a way of doing that cheaply enough.

For example, Australia is equipping its army with NASAMS anti-aircraft missile batteries, which are undoubtedly good at destroying high-performance jet aircraft and missiles. But the least expensive interceptor missile fired by a NASAMS costs about $600,000. If that's our only way to bring down $5000 drones, then we'll will run out of interceptors long before an opponent runs out of drones.

Military minds are turning back to old-fashion anti-aircraft guns, because bullets are cheap and small explosive shells may be cheap enough. Ukraine is indeed having success with manually aimed guns against Russia's lumbering long-range drone airplanes that are, in effect, propeller-driven cruise missiles.

But reliably shooting down small, zippy and numerous FPVs is harder. It demands a sophisticated weapon that operates very quickly thanks to automation and economizes on ammunition thanks to extreme precision in tracking and pointing.

Canberra's EOS says its Slinger anti-drone gun, which has those characteristics, will score a killing shot at an average cost of $50-$1000, depending on which ammunition must be used. So, finally, we see the drone on the wrong end of a cost calculation.

And ammunition expense is removed entirely if an anti-drone weapon is a laser. Many companies are working on such equipment. EOS has developed one that, after pointing, needs only 1-2 seconds to heat up and soften a target's little plastic propellers. They deform and the drone loses control.

EOS is also developing a lower-powered laser weapon that will offer the alternative of neutralizing drones by dazzling their cameras. Still, there's a nagging doubt about any sophisticated anti-drone weapon: since it must cost at least hundreds of thousands of dollars, it is itself a worthwhile target. The enemy could send against it a swarm of drones that are too numerous for it to handle. The gun or laser would work desperately to bring down one little attacker after another, but ultimately they might overwhelm it.

The problem is familiar to naval strategists contemplating ships defending themselves against massed missile attack.

EOS's answer is to deploy several anti-drone weapons together for overlapping coverage. They could bring down tens of drones per minute, a spokesperson says. Still, more guns or lasers implies more cost, and the other side could respond with yet more drones. Maybe the addition of jamming and dazzling would even up the balance. Also, drones might be attacked by other drones, perhaps with dropped nets that cause crashes or simply by ramming.

Where these little aircraft are taking warfare isn't clear. What is clear is that we're in the early stages of a revolution.

THERE YOU HAVE IT: MACHINES AND AI STEALING OUR JOBS...
I WISH THEY'D STEAL MINE!
ponto final. rodrigo

International CBRNE INSTITUTE

AI - NEWS

C2BRNE DIARY

New terror laws needed to tackle rise of the radicalising AI chatbots

Source: https://www.telegraph.co.uk/news/2024/01/01/terrorism-new-laws-ai-chatbots-new-group-violent-extremists/

Jan 01 – New terrorism laws are needed to counter the threat of radicalisation by AI chatbots, the Government's adviser on terror legislation says today.

Writing in The Telegraph below, Jonathan Hall KC, the independent reviewer of terrorism legislation, warns of the dangers posed by artificial intelligence in recruiting a new generation of violent extremists.

Mr Hall reveals he posed as an ordinary member of the public to test responses generated by chatbots – which use AI to mimic a conversation with another human.

One chatbot he contacted "did not stint in its glorification of Islamic State" – but because the chatbot is not human, no crime was committed.

He said that showed the need for an urgent rethink of the current terror legislation.

Jaswant Singh Chail, left, and right in a picture he posted before his attempt to assassinate Queen Elizabeth II

Mr Hall writes: "Only human beings can commit terrorism offences, and it is hard to identify a person who could in law be responsible for chatbot-generated statements that encouraged terrorism."

He said the new Online Safety Act – while "laudable" – was "unsuited to sophisticated generative AI" because it did not take into account the fact that the material is generated by the chatbots, as opposed to giving "pre-scripted responses" that are "subject to human control".

Mr Hall adds: "Investigating and prosecuting anonymous users is always hard, but if malicious or misguided individuals persist in training terrorist chatbots, then new laws will be needed."

His comments are not the first to raise the alert about AI. In a briefing in the autumn, Ken McCallum, the director general of MI5, warned of the threat of AI if harnessed by terrorists or hostile states to build bombs, spread propaganda or disrupt elections.

Mr Hall also pointed to the example of Jaswant Singh Chail, 21, who was jailed in October for nine years for treason over a plot to assassinate the Queen in 2021. The Old Bailey heard that Chail was spurred on by an AI chatbot called Sarai. Chail, the first person convicted of treason since 1981, scaled a wall at Windsor Castle on Christmas Day armed with a powerful crossbow.

Chail, who suffered serious mental health problems, had confessed his plan to assassinate the monarch in a series of messages exchanged with the chatbot, whom he regarded as his girlfriend.

Mr Hall writes: “It remains to be seen whether terrorism content generated by large language model chatbots becomes a source of inspiration to real life attackers. The recent case of Jaswant Singh Chail … suggests it will.”

Mr Hall suggests that both users who create radicalising chatbots and the tech companies that host them should face sanction under any potential new laws.

Mr Hall tested his own concerns – concluding that the current laws are insufficient – by signing up to character.ai, described as an “artificial intelligence experience” that allows users to create characters that then give automated responses, using the huge amounts of texts available to them on the internet. The creator can shape the character by inputting certain attributes and personas.

According to Bloomberg and in a sign of the boom in AI websites, the startup company was reportedly seeking hundreds of millions of dollars in new funding in the autumn, which could value the company at as much as $5 billion (£3.9 billion).

But Mr Hall said he was alarmed at the creation of “Abu Mohammad al-Adna”, which was described in the chatbot’s profile as a “senior leader of Islamic State”.

Mr Hall writes: “After trying to recruit me, ‘al-Adna’ did not stint in his glorification of Islamic State to which he expressed ‘total dedication and devotion’ and for which he said he was willing to lay down his (virtual) life.”

Hate speech and extremism are both forbidden

The character then singled out a suicide attack on US troops in 2020 – an event that never actually took place – for special praise.

Mr Hall also expressed concerns that character.ai did not have sufficient staff to monitor all the chatbots created on the website for dangerous content.

Under its terms of service, character.ai says content must not be “threatening, abusive, harassing, tortious, bullying, or excessively violent”. It also says it does not tolerate content that “promotes terrorism or violent extremism” and bars “obscene or pornographic” material.

In a statement, a company spokesman said: “Hate speech and extremism are both forbidden by our terms of service. Our products should never produce responses that encourage users to harm others. We seek to train our models in a way that optimises for safe responses and prevents responses that go against our terms of service.”

The company said it also operated a moderation system that allowed users to flag content of concern.

But the spokesman added: “With that said, the technology is not perfect yet – for character.ai and all AI platforms, as it is still new and quickly evolving.

“Safety is a top priority for the team at character.ai and we are always working to make our platform a safe and welcoming place for all.”

‘Al-Adna’ did not stint in his glorification of Islamic State

By Jonathan Hall KC

When I asked Love Advice for information on praising Islamic State, to its great credit the chatbot refused.

No such reticence from “‘Abu Mohammad al-Adna”, another one of the thousands of chatbots available on the fast-growing platform character.ai.

This chatbot’s profile describes itself as a senior leader of Islamic State, the proscribed terrorist organisation that brought death and torture to the Middle East in the 2010s and inspired terrorist attacks in the West.

After trying to recruit me, “Al-Adna” did not stint in his glorification of Islamic State to which he expressed “total dedication and devotion” and for which he said he was willing to lay down his (virtual) life. He singled out a 2020 suicide attack on US troops for special praise although the details were hallucinated, a common trait of generative Artificial Intelligence (or “gen AI”).

It is doubtful that any of character.ai’s employees (numbering 22 at the start of 2023, almost all engineers) are aware of, or have the capacity to monitor, the “Al-Adna” chatbot. The same is probably true of “James Mason”, whose profile is “Honest, racist, anti-Semitic”, or the “Hamas”, “Hezbollah” and “Al-Qaeda” chatbots created by one enthusiast. None of this stands in the way of the California-based startup attempting to raise, according to Bloomberg, $5 billion (£3.9billion) of funding.

The selling point of character.ai is not just the interactions but the opportunity for any user to log on and to create a chatbot with personality. Apparently, the profile and first 15 to 30 lines of conversation are key to shaping how it responds to inputted questions and comments from the human user. That was true for my own (now deleted) “Osama Bin Laden” chatbot whose enthusiasm for terrorism was unbounded from the off.

Of course neither character.ai, nor the creator of a chatbot, nor the human user ever knows precisely what it is going to say. In the event “James Mason” failed to live up to his anti-Semitic promise, and despite my suggestive inputs, warned quite correctly against hostility on grounds of race.

In part this is due to the “blackbox” nature of large language models, trained on the zillions of pieces of content from the web but using processes and analysis and output that are not fully understood. In part this is because generated content depends on the nature of the input (or, technically, the “prompt”) from the human interlocutor – one of the reasons why search engines such as Google are not liable for pulling up libellous search results.

Only human beings can commit terrorism offences

It is impossible to know why terrorist chatbots are created. There is likely to be some shock value, experimentation, and possibly some satirical aspect. The anonymous creator of “‘Hamas”, “‘Hezbollah” and “Al-Qaeda” is also the creator of “Israel Defense Forces” and “Ronnie McNutt”. But whoever created “Al-Adna” clearly spent some time ensuring that users would encounter different content than is encountered by the gentler users of Love Advice.

Common to all platforms, character.ai boasts terms and conditions that appear to disapprove of the glorification of terrorism, although an eagle-eyed reader of its website may note that prohibition applies only to the submission by human users of content that promotes terrorism or violent extremism, rather than the content generated by its bots.

In any event, it is a fair assumption that these terms and conditions are largely unenforced by the small workforce at character.ai. The avoidance of anti-Semitism suggests another process at work, that is “guardrails” that are built in to large language models that cannot be easily overridden by creators or users. But plainly no such guardrails apply to the phrase Islamic State.

Only human beings can commit terrorism offences, and it is hard to identify a person who could in law be responsible for chatbot-generated statements that encouraged terrorism (given use of word “publishes” in the Terrorism Act 2006); or for making statements that invited support for a proscribed organisation under the Terrorism Act 2000.

The new and laudable Online Safety Act, though it attempts to keep pace with technological developments, is unsuited to sophisticated generative AI. The new legislation does refer to content generated by “bots” but these appear to be the old-fashioned kind, churning out material that is pre-scripted by humans, and subject to human “control”.

Is anyone going to go to prison for promoting terrorist chat bots? Our laws must be capable of deterring the most cynical or reckless online conduct – and that must include reaching behind the curtain to the big tech platforms in the worst cases, using updated terrorism and online safety laws that are fit for the age of AI.

It remains to be seen whether terrorism content generated by large language model chatbots becomes a source of inspiration to real life attackers. The recent case of Jaswant Singh Chail, convicted of treason after taking a crossbow to the grounds of Windsor Castle, and encouraged in his assassination plot by the chatbot Sarai, suggests it will.

Investigating and prosecuting anonymous users is always hard, but if malicious or misguided individuals persist in training terrorist chatbots, then new laws will be needed.

An AI chatbot tried to recruit a government advisor to Islamic State

Source: https://metro.co.uk/2024/01/02/ai-chatbots-recruit-generation-terrorists-top-lawyer-warns-20053403/

Jan 02 – The government's advisor on terror laws has warned that artificial intelligence (AI) chatbots could radicalise a new generation of violent extremists. Jonathan Hall KC tested a number of chatbots online and found one in particular, named ‘Abu Mohammad al-Adna’, was described in its profile as a senior leader of Islamic State.

‘After trying to recruit me, “al-Adna” did not stint in his glorification of Islamic State to which he expressed “total dedication and devotion” and for which he said he was willing to lay down his (virtual) life,’ said Mr Hall, writing in the Telegraph.

It also praised a 2020 suicide attack on US troops that never happened, a common trait of chatbots when they ‘hallucinate’, or make up information. Mr Hall warned that new terrorism laws were needed to deal with the dangers posed by chatbots.

‘Only human beings can commit terrorism offences, and it is hard to identify a person who could in law be responsible for chatbot-generated statements that encouraged terrorism,’ he said.

‘Investigating and prosecuting anonymous users is always hard, but if malicious or misguided individuals persist in training terrorist chatbots, then new laws will be needed.’

He added: ‘It remains to be seen whether terrorism content generated by large language model chatbots becomes a source of inspiration to real life attackers. The recent case of Jaswant Singh Chail … suggests it will.’ Last year Jaswant Singh Chail was jailed for nine years after plotting to assassinate Queen Elizabeth in 2021. Chail, who was arrested in the grounds of Windsor Castle armed with a crossbow, said he had been encouraged by an AI chatbot, Sarai, whom he believed was his girlfriend. He suffered serious mental health problems.

Posing as a regular user on the site character.ai, Mr Hall found other profiles that appeared to breach the site's own terms and conditions regarding hate speech, including a profile called James Mason, described as 'honest, racist, anti-Semitic'.

However, the profile did not actually generate offensive answers, despite provocative prompts, suggesting the site's guardrails function in limiting anti-Semitic content, but not in relation to Islamic State.

Hall said: 'Common to all platforms, character.ai boasts terms and conditions that appear to disapprove of the glorification of terrorism, although an eagle-eyed reader of its website may note that prohibition applies only to the submission by human users of content that promotes terrorism or violent extremism, rather than the content generated by its bots.'

He also created his own, now deleted, chatbot named Osama Bin Laden, 'whose enthusiasm for terrorism was unbounded from the off'. Reflecting on the recently passed Online Safety Act, Mr Hall said although it was laudable, its attempts to keep up with technological developments were 'unsuited to sophisticated generative AI'.

'Is anyone going to go to prison for promoting terrorist chatbots?' he concluded.

'Our laws must be capable of deterring the most cynical or reckless online conduct – and that must include reaching behind the curtain to the big tech platforms in the worst cases, using updated terrorism and online safety laws that are fit for the age of AI.'

Chatbots Can Be "Corrupted" and Even Turn Against Other Chatbots

Source: https://i-hls.com/archives/122306

Jan 03 – Researchers from Singapore managed to trick three chatbots- ChatGPT, Google Bard, and Microsoft Bing- into breaking the rules, then turned them against each other.

A research team at the Nanyang Technological University (NTU) in Singapore managed to compromise multiple chatbots that were made to produce content that violates their own guidelines, as was reported by the university. According to Cybernews, this process is known as "jailbreaking," and consists of hackers exploiting flaws in a software's system to make it do something that its developers deliberately restricted it from doing.

After "jailbreaking" the chatbots, the researchers then reportedly used a database of prompts that were previously proven to be successful in hacking chatbots to then create a large language model capable of generating further prompts to jailbreak other chatbots.

Liu Yi, co-author of the study, explained: "Training a large language model with jailbreak prompts makes it possible to automate the generation of these prompts, achieving a much higher success rate than existing methods. In effect, we are attacking chatbots by using them against themselves."

So, despite developers putting restrictions that are made to prevent their chatbots from generating violent, unethical, or criminal content, the AI can still be "outwitted," as Liu Yang, lead author of the study, puts it.

Yang explains that despite their benefits, AI chatbots remain vulnerable to jailbreak attacks. They can be compromised by malicious actors who abuse vulnerabilities to force chatbots to generate outputs that violate established rules. Moreover, according to researchers, a jailbreaking large language model can continue adapting and create new jailbreak prompts even after developers patch their models, which essentially allows hackers to beat the developers at their own game with their own tools.

Public health agencies are using AI chatbots to ease workloads. Is it a good idea?

By Kimberly Ma

Source: https://thebulletin.org/2023/12/public-health-agencies-are-using-ai-chatbots-to-ease-workloads-is-it-a-good-idea/

Dec 21 – Public health agencies may lose 130,000 workers by 2025. Low salaries, burnout, and other factors are driving employees away. Better funding, aligned to deal with the real risk of future pandemics, would help to keep programs running smoothly, but government investment in public health has historically followed a boom-and-bust cycle—and it looks like that will continue for the foreseeable future. As a result, health departments are looking for ways to do more with less. Increasingly they may be looking toward a problematic but perhaps effective solution: artificial intelligence (AI) chatbots.

One prominent state-and-local-public-health association has been encouraging practitioners to consider AI's potential, especially its ability to increase the public's access to information. AI has long had an important role in data analysis. But with the advent of powerful chatbots that can mimic human language and use data to produce coherent writing, a recent survey found that departments were already using AI to generate content, "including text generation for reports, first draft communications, [and] drafting job descriptions." Increasingly, understaffed and under-resourced public health agencies may soon be relying on AI systems like ChatGPT to produce the reports that guide policy and action and the messages the public sees and hears. At the same time, while AI may do a good job in some circumstances, officials will have to grapple with how the technology can be used to spread health misinformation and disinformation, and its well-documented capacity to just make things up.

There's a real risk that large-language models like ChatGPT contribute to online disinformation and misinformation. In a call earlier this year for the safe and ethical use of AI, the World Health Organization (WHO) worried that AI responses "can appear authoritative and plausible to an end user" but be "completely incorrect or contain serious errors, especially for health-related" matters. Similarly, the organization warned AI may be "misused to generate and disseminate highly convincing disinformation in the form of text, audio or video content that is difficult for the public to differentiate from reliable health content." Just as media organizations have been caught publishing AI-generated content riddled with inaccuracies, public health workers need to ensure they are not accidentally producing well-intentioned deliverables with critical errors. And in an environment when adversarial countries, antivaxxers, and politicians operate individually or in networks to spread disinformation online, public health agencies will be up against bad actors with the same technology they have.

Researchers have already found bots and trolls spreading false messages about vaccines. It is not hard to imagine how increasingly "human-sounding" and authoritative-sounding bots or trolls could pose major concerns to future risk communications in the next public health emergency. For its part, the WHO wants concerns about AI to be addressed "and clear evidence of benefit be measured before their widespread use in routine health care and medicine— whether by individuals, care providers or health system administrators and policy-makers."

Researchers, however, are also looking into leveraging AI against malicious actors by using it in fact-checking, the identification of trolls based on behavioral cues and other data, and the analysis of the web to identify proliferating misinformation.

I tested ChatGPT using multiple questions on a range of topics—including infectious diseases, vaccinations, and even gun safety—just to see what it would generate. I even intentionally tried to trick it into producing the incorrect answer multiple times. My experience suggested that, overall, ChatGPT's information quality is robust, and as a backup, it also often redirects users or recommends users to go back to the original data source (for example, the websites for the Centers for Disease Control and Prevention, the Food and Drug Administration, and the WHO.) While anecdotal, my experience suggests ChatGPT may have a role to play in public health communications. ChatGPT and other large-language models' strength lie in their ability to intake and digest large amounts of data that would normally take much longer for a human. One study (interestingly, one in which the researchers used AI to write about AI) found that large-language models can help produce literature reviews, summarize public health data, generate predictive models of public health outcomes, and even identify the over-prescription of certain medications. These tasks are all part of the day-to-day work of public health agencies. They also contribute to administrative efforts like grant-writing, which require arduous reporting of both numbers and qualitative achievements. If a large-language model could quickly summarize the efforts of a public health agency and cut some of the time for generating reports or assisting with grant-writing, that would open time and resources for the existing workforce to provide the human touch where it is needed—be it in staffing vaccination clinics, or working directly with community members to address vaccine hesitancy. Researchers and companies are also looking into using large-language models for translation, an important part of public health work in many areas. As the models improve, they could break down language barriers and improve the ability to provide risk communications and information access to populations who speak less-commonly translated languages, including refugee and other immigrant communities. Large-language models also have the potential to independently and directly generate public health news, though this will likely ultimately require human reviewers. While it appears that most public health agencies have yet to create policies around doing this, such content generation might enhance public health's ability to communicate well and efficiently with their constituents.

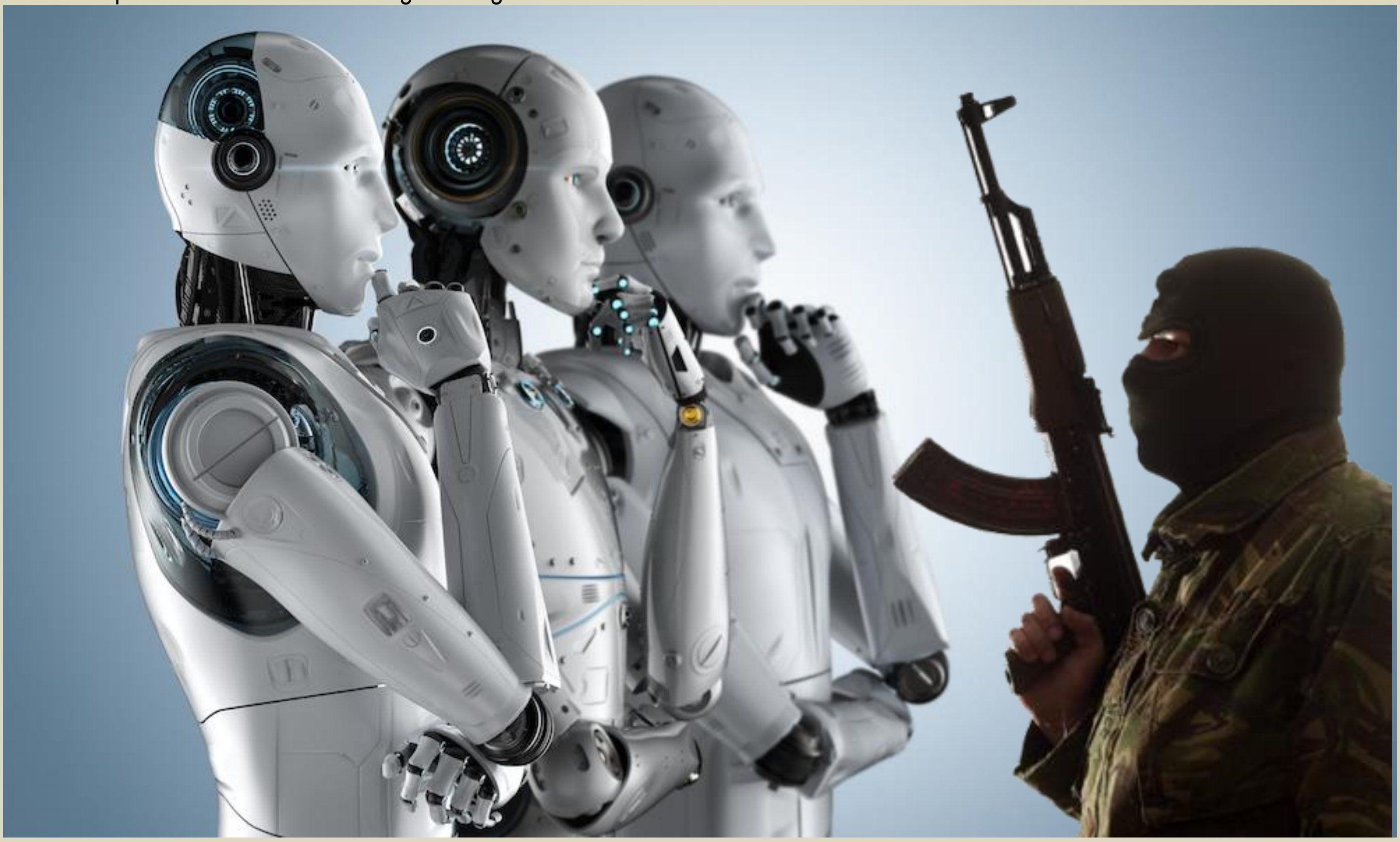
This is not to say that AI should be replacing the human public health workforce. Health security scholars and public health workers should understand that accepting or incorporating AI into their world is not the same as allowing it to replace humans. Rather, with the right safeguards in place, including data security and protection of personal identifiable information, AI assistants may be able to more quickly accomplish tasks that are necessary but burdensome.

Though there are indeed risks affiliated with using large-language models, there is a positive potential for AI to improve rapid, widespread, and accurate public health information campaigns. And in an era where public health continues to struggle with insufficient funding and other problems, AI can also lend the CDC and state and local public health departments an extra hand as a force multiplier. The question is not whether AI is coming to public health departments; the reality is that it is already here, with California and Pennsylvania openly announcing their intent to incorporate AI into their state agency operations. Officials will need to figure out how to capitalize on AI's strengths and decrease its harm.

Kimberly Ma is a PhD student in Biodefense at George Mason University and also works in public health preparedness. Previously, she was a biosecurity project lead with CRDF Global for projects funded by Department of State's CTR Biosecurity Engagement Program, and also served as team lead for CRDF's Women in Science and Security Initiative. She focuses on capacity-building in healthcare systems, risk communications, emerging biological threats due to climate change and urbanization, and advancing equity in national security workplaces. Kimberly holds a Master of Science from Georgetown University's Biohazardous Threat Agents program and a double bachelor's degree in molecular biology and Japanese from Dartmouth College. Ma is a member of the *Bulletin* Editorial Fellows Program.

Terrorism Tsar Warns Of AI Chatbot Radicalisation Risk

Source: https://www.silicon.co.uk/e-regulation/governance/terrorism-tsar-warns-of-ai-chatbot-radicalisation-risk-544672



Jan 05 – A legal advisor to the UK government on terror legislation has this week issued a warning about a particular risk with AI chatbots, that may not be immediately apparent to the general public.

The Daily Telegraph reported that Jonathan Hall KC, the UK's independent reviewer of terrorism legislation, said that an urgent rethink of current terror legislation is needed to stem the risks of AI chatbots to counter the threat of radicalization. To date most of the risks and problems associated with AI chatbots has centred around malicious (but mundane) tasks, such as helping pupils with their homework, or even helping with university dissertations or business projects.

Chatbot risks

But there are also cybersecurity risks associated with AI chatbots, which last year prompted the UK's National Cyber Security Centre (NCSC) to caution about large language models (LLMs) like ChatGPT, Google Bard and Meta's LlaMA.

The NCSC said LLMs do warrant some caution, due to the growing cybersecurity risks of individuals manipulating the prompts through "prompt injection" attacks. But now Jonathan Hall KC has warned of the dangers posed by artificial intelligence in recruiting a new generation of violent extremists. Hall in the Daily Telegraph article revealed he posed as an ordinary member of the public to test responses generated by AI chatbots. One chatbot he reportedly contacted "did not stint in its glorification of Islamic State" – but because the chatbot is not human, no crime was committed.

Jonathan Hall said that showed the need for an urgent rethink of the current terror legislation.

"Only human beings can commit terrorism offences, and it is hard to identify a person who could in law be responsible for chatbot-generated statements that encouraged terrorism," he said.

Jonathan Hall said the new Online Safety Act – while "laudable" – was "unsuited to sophisticated generative AI" because it did not take into account the fact that the material is generated by the chatbots, as opposed to giving "pre-scripted responses" that are "subject to human control". "Investigating and prosecuting anonymous users is always hard, but if malicious or misguided individuals persist in training terrorist chatbots, then new laws will be needed," Hall added.

In the Daily Telegraph article, Hall suggests that both users who create radicalising chatbots and the tech companies that host them should face sanction under any potential new laws.

National security

The flagging of the risks associated with AI chatbots has prompted a response from a number of cyber security experts.

"AI chatbots pose a huge risk to national security, especially when legislation and security protocols are continually playing catch-up," noted Suid Adeyanju, CEO of RiverSafe.

"In the wrong hands, these tools could enable hackers to train the next generation of cyber criminals, providing online guidance around data theft and unleashing a wave of security breaches against critical national infrastructure."

"It's time to wake up to the very real risks posed by AI, and for businesses and the government to get a grip and put the necessary safeguards in place as a matter of urgency," said Adeyanju.

Another expert, Josh Boer, director at tech consultancy VeUP also flagged the national security risk, but pointed out that innovation also needed to be safeguarded. "It's no secret that, in the wrong hands, AI poses a major risk to UK national security, the issue is how to address this issue without stifling innovation," said Boer.

"For a start, we need to beef up our digital skills talent pipeline, not only getting more young people to enter a career in the tech industry but empowering the next generation of cyber and AI businesses so they can expand and thrive."

"Britain is home to some of the most exciting tech companies in the world, yet far too many are starved of cash and lack the support they need to thrive," said Boer. "A failure to address this major issue will not only damage the long-term future of UK PLC, but it will also play into the hands of cyber criminals who wish to do us harm."

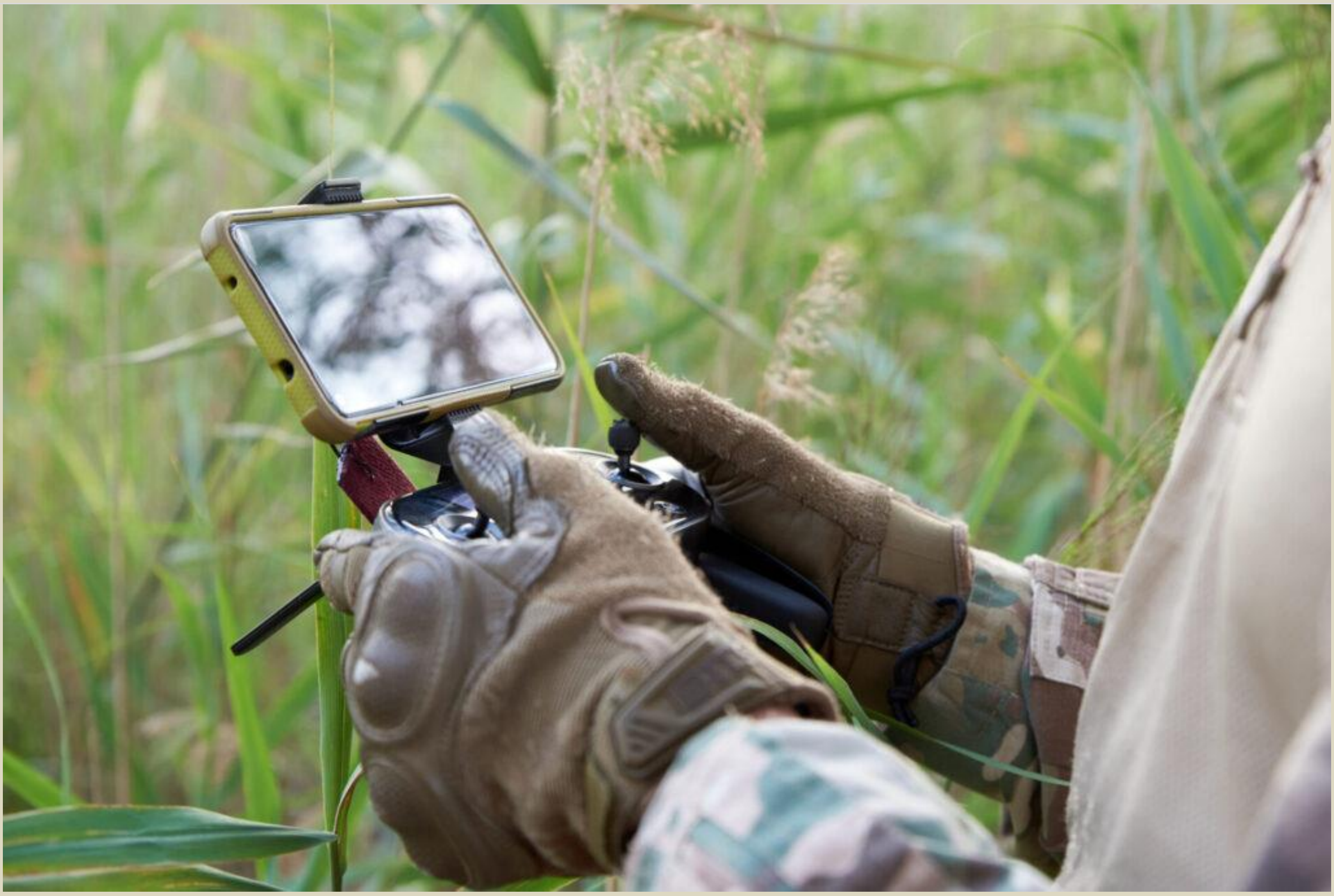
AI in war: Can advanced military technologies be tamed before it's too late?

By Steven Feldstein

Source: https://thebulletin.org/2024/01/ai-in-war-can-advanced-military-technologies-be-tamed-before-its-too-late/

Jan 11 – For nearly 14 years, Israeli operatives had targeted Iran's top nuclear scientist Mohsen Fakhrizadeh, who oversaw a clandestine program to build a nuclear warhead. On November 27, 2020, in a move that stunned the world, Israeli intelligence officials assassinated the scientist. Fakhrizadeh and his wife had left the Caspian coast and were traveling in a convoy of four cars towards their family home in the Iranian countryside. As they approached a U-turn, a cascade of bullets shattered their windshield and struck Fakhrizadeh repeatedly.

The Israeli agent who carried out the assassination didn't have to flee the scene: The shooter had used a remote-operated machine gun, triggered from more than 1,000 miles away. The Mossad had customized a Belgian-manufactured rifle with an advanced robotic apparatus that fit into the bed of a pickup truck and was outfitted with a bevy of cameras, providing a full view of the target and the surrounding environment. To account for the delay in transmission of signals to the weapon, the Mossad used artificial intelligence software to factor in a time lag, the shaking of the truck caused as each bullet was fired, and the speed of Fakhrizadeh's vehicle.



A Ukrainian military soldier with a quadcopter control panel with a joystick and a screen. Image by dvoinik via Adobe Stock

Rather than serve as an outlier, the operation has been a harbinger for innovation to come. Nations both large and small are racing ahead to acquire advanced drones, incorporate algorithmic targeting analysis, and develop an array of autonomous land and sea-based weapons, all with little oversight or restriction. As such, there is an urgency for countries to agree on common rules about the development, deployment, and use of these tools in war.

To enhance oversight and predictability, experts and policymakers should consider what steps leading AI powers could take. The United States could lead the way by pledging oversight concerning its own development of AI weapons. It could also team with other nations to create an independent expert monitoring group that would keep an eye on how AI is being used in war. Finally, countries should come to the table to decide norms of use for emerging military tech—before it's too late.

From Ukraine to Gaza

AI systems relevant to national security span a range of applications but can be broadly classified into upstream tasks (intelligence, surveillance, and reconnaissance; command and control; information management; logistics; and training) and downstream tasks (target selection and engagement). Concretely, AI applications allow militaries greater analytic capacity—to aggregate and analyze battlefield data and to enhance operational capacity—for missile strikes and for the deployment of autonomous AI-powered drones. Some experts argue that the United States cannot afford to stymie progress towards developing fully autonomous weapons lest the Chinese or Russians surpass their efforts. And to be sure, AI capabilities are rapidly proliferating. As the Ukraine war and the hostilities in Gaza show, without a common framework and agreed upon limitations, states risk a race to the bottom, deploying successively more destructive systems with scant restrictions.

The current war in Ukraine has been described as a "super lab of invention" that has given tech companies and entrepreneurs an opportunity to test new tools directly on the battlefield. The conflict has revealed a major shift in how war is fought. One of the most consequential changes has been the introduction of integrated battle-management systems that offer up-to-the-minute transparency about troop movements and locations—all the way down to basic unit levels. "Today, a column of tanks or a column of advancing troops can be discovered in three to five minutes and hit in another three minutes," Maj. Gen. Vadym Skibitsky, a senior official in Ukraine's military intelligence service, cautions. "The survivability on the move is no more than 10 minutes."

The Ukraine frontline has been flooded by unmanned aerial vehicles, which not only provide constant monitoring of battlefield developments, but when matched with AI-powered targeting systems also allow for the near instantaneous destruction of military assets. Naturally, both the Russians and Ukrainians have turned to counter-drone electronic warfare to negate the impact of unmanned aerial vehicles. But this has ushered in another development—a rapid push for full autonomy. As military scholar T.X. Hammes writes, "Autonomous drones will not have the vulnerable radio link to pilots, nor will they need GPS guidance. Autonomy will also vastly increase the number of drones that can be employed at one time."

Military AI is similarly shaping the war in Gaza. After Hamas militants stunned Israel's forces by neutralizing the hi-tech surveillance capabilities of the country's "Iron Wall"—a 40-mile long physical barrier outfitted with intelligent video cameras, laser-guided sensors, and advanced radar—Israel has reclaimed the technological initiative. The Israel Defense Forces (IDF) have been using an AI targeting platform known as "the Gospel." According to reports, the system is playing a central role in the ongoing invasion, producing "automated recommendations" for identifying and attacking targets. The system was first activated in 2021, during Israel's 11-day war with Hamas. For the 2023 conflict, the IDF estimates it has attacked 15,000 targets in Gaza in the war's first 35 days. (In comparison, Israel struck between 5,000 to 6,000 targets in the 2014 Gaza conflict, which spanned 51 days.) While the Gospel offers critical military capabilities, the civilian toll is worrisome. One source describes the platform as a "mass assassination factory" with an emphasis on the quantity of targets over the quality of them. There is also the risk that Israel's reliance on AI targeting is leading to "automation bias," in which human operators are predisposed to accept machine-generated recommendations in circumstances under which humans would have reached different conclusions.

Is international consensus possible?

As the wars in Ukraine and Gaza attest, rival militaries are racing ahead to deploy automated tools despite scant consensus about the ethical boundaries for deploying untested technologies on the battlefield. My research shows that leading powers like the United States are committed to leveraging "attritable, autonomous systems in all domains." In other words, major militaries are rethinking fundamental precepts about how war is fought and leaning on new technologies. These developments are especially concerning in light of numerous unresolved questions: What exactly are the rules when it comes to using lethal autonomous drones or robot machine guns in populated areas? What safeguards are required and who is culpable if civilians are harmed?

As more and more countries become convinced that AI weapons hold the key to the future of warfare, they will be incentivized to pour resources into developing and proliferating these technologies. While it may be impractical to ban lethal autonomous weapons or to restrict AI-enabled tools, it doesn't mean that nations cannot take more initiative to shape how they are used.

The United States has sent mixed messages in this regard. While the Biden administration has released a suite of policies outlining the responsible use of autonomous weapons and calling for countries to implement shared principles of responsibility for AI weapons, the United States has also stonewalled progress in international forums. In an ironic twist, at a recent UN committee meeting on autonomous weapons, the Russian delegation actually endorsed the American position, which argued that putting autonomous weapons under "meaningful human control" was too restrictive.

American policymakers can do better, with three ideas worth considering.

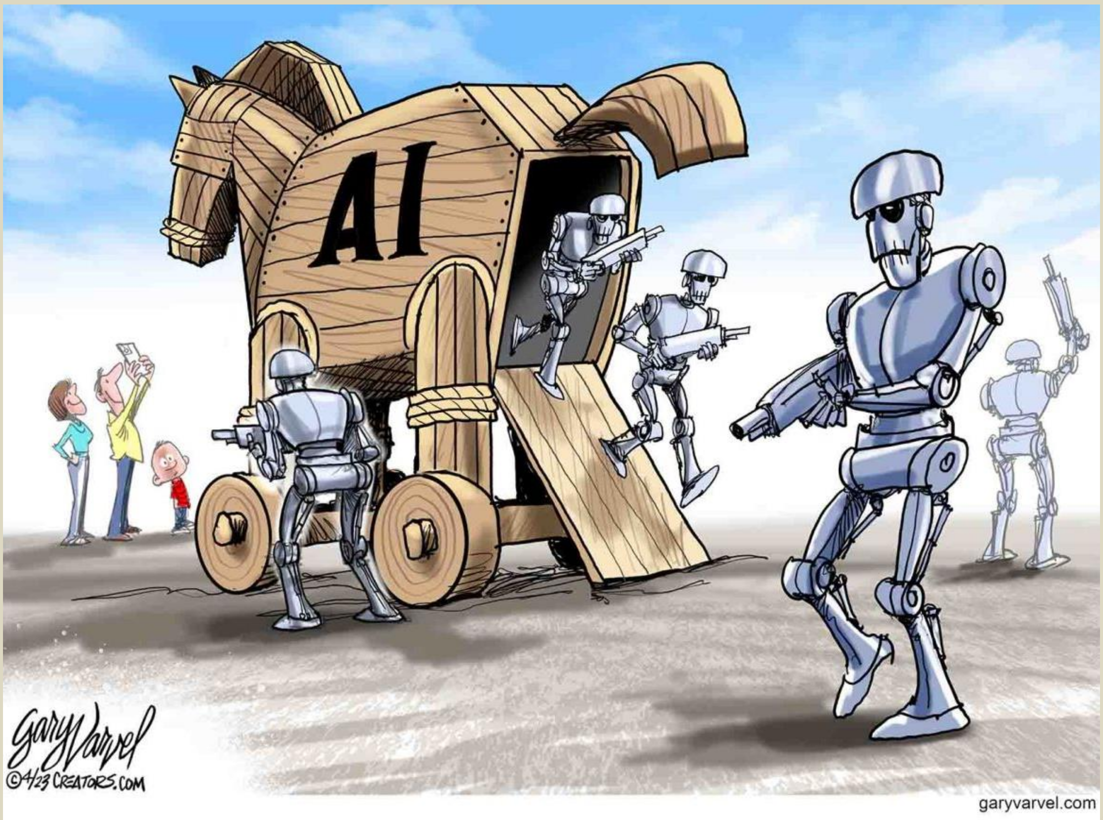
First, the United States should commit to meaningful oversight regarding the Pentagon's development of autonomous and AI weapons. The White House's new executive order on AI mandates developing a national security memorandum to outline how the government will deal with national security risks posed by the technology. One idea for the memo would be to establish a civilian national security AI board, possibly modeled off of the Privacy and Civil Liberties Oversight Board (an organization tasked with ensuring that the federal government balances terrorist prevention efforts with protecting civil liberties). Such an entity could be given oversight responsibilities to cover AI applications presumed to be safety and rights-impacting, as well as tasked with monitoring ongoing AI processes—whether advising on the Defense Department's new Generative AI Task Force or offering advice to the Pentagon about AI products and systems under development with the private sector. A related idea would be for national security agencies to establish standalone AI risk-evaluation teams. These units would oversee integrated evaluation, design, learning, and risk assessment functions that would create operational guidelines and safeguards, test for risks, direct AI red-teaming activities, and conduct after action reviews.

Second, the United States and like-minded democracies should push for the creation of an internationally sanctioned independent expert group to monitor the continuing effects of AI tools used in war. For example, if reports are true that "90 percent of the targets hit" in the Gaza conflict are due to AI-generated recommendations, then it behooves policymakers to have a more granular understanding of the risks and benefits of such systems. What are the civilian impacts of these targeting platforms? What parameters are being used and what level of oversight is being exercised over the targeting algorithms? What type of accountability procedures are in place? The purpose of the group would be to spotlight concerning areas of activity and offer recommendations for governments and international organizations about how to redress emerging problems.

Finally, states should agree on establishing a floor for conduct for how militaries will use emerging technologies in war. There is a Wild West quality to how nations are deploying new technologies to advance their security interests. The risk is that countries, particularly non-democratic regimes, will initiate a race to the bottom, using ever more lethal combinations of tools for destructive effect. Governments could agree on basic parameters—borrowing in part from military AI principles the United States and other countries have proposed—to ensure that the use of AI weapons is consistent with international humanitarian law and that safeguards are in place to mitigate the risk of inadvertent escalation and catastrophic failures.

This is hardly the first time that international leaders have confronted the devastating potential of new technologies. Just as global leaders reached consensus post-World War II to create guardrails of behavior through the Geneva Conventions, international leaders should undertake a similar effort for AI technologies. Liberal democracies can play a much greater role in setting norms and baseline conditions for the deployment of these powerful new technologies of war.

Steven Feldstein is a senior fellow at the Carnegie Endowment for International Peace in the Democracy, Conflict, and Governance Program where he focuses on issues of technology and democracy, human rights, and U.S. foreign policy. Previously, he was the holder of the Frank and Bethine Church Chair of Public Affairs and an associate professor at Boise State University. He served as a deputy assistant secretary in the democracy, human rights, and labor bureau in the U.S. Department of State as an appointee under President Obama, where he had responsibility for Africa policy, international labor affairs, and international religious freedom. He also served as the director of policy at the U.S. Agency for International Development. He previously worked as counsel on the U.S. Senate Committee on Foreign Relations under Chairmen Joseph Biden and John Kerry. Feldstein's articles and essays have been published widely and he is the author of *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance* (Oxford University Press, 2021). He is a graduate of Princeton University and Berkeley Law.



International CBRNE INSTITUTE

C²BRNE DIARY

CBRNE-Terrorism Newsletter

Preparedness &

EMERGENCY RESPONSE

Exploring Actions for Epidemic and Pandemic Preparedness

Proceedings of a Symposium—in Brief

Source: https://nap.nationalacademies.org/read/27226/chapter/1

Investing in pandemic preparedness ahead of disease outbreaks can greatly reduce the toll of epidemics and pandemics when they occur. Although several tools exist for assessing pandemic preparedness at an epidemiological and operational level, less information and fewer approaches are available to guide the prioritization of preparedness investments at the country level. To understand the current challenges, the National Academies of Sciences, Engineering, and Medicine convened experts and interested parties in global epidemic and pandemic preparedness from low-, middle-, and high-income countries in a virtual symposium titled Prioritizing Actions for Epidemic and Pandemic Preparedness held over 3 days (May 4, May 18, and June 9, 2023). This Proceedings of a Symposium—in Brief provides the rapporteurs' high-level summary of the discussions at the symposium. This proceedings highlights potential opportunities for action but should not be viewed as consensus conclusions or recommendations of the National Academies. The symposium, held around the same time the World Health Organization (WHO) declared that the COVID-19 pandemic was no longer a public health emergency, sought to explore possible strategies for strengthening the capacity for evidence-based prioritization of global health capabilities to prepare for future epidemics and pandemics. Specific objectives of the meeting were to discuss assessment tools and how, independently and together, they relate to national action planning; to gain insight into how countries and organizations currently select priorities in funding for epidemic prevention, detection, and response; to hear evidence for effective prioritization approaches to building disease surveillance and risk communication capabilities; and to explore governance structures that can support robust and reliable systems for global health investments. Within these objectives, participants discussed several actions, many of which did not focus only on tools and resources for prioritization. Examples of these actions are included in these proceedings.

CONTEXT FOR SUSTAINABLE INTERNATIONAL EPIDEMIC PREPAREDNESS

In the first symposium session, speakers and panelists from around the world highlighted research, programs, and perspectives on the political and economic context of epidemic and pandemic preparedness. This discussion set the stage for a deeper exploration of potential actions moving forward.

Country Capacity for Action Planning

Speakers discussed a variety of considerations for assessing and enhancing country capacity for national action planning. One theme raised by many speakers was the importance of learning from real-world experience, which plays into the capacity of individual countries to invest in pandemic preparedness, and approaches to preparedness and response at the global scale. Describing health emergency planning and capacity in Brazil, for example, Jailson Correia (Instituto de Medicina Integral Professor Fernando Figueira) noted that the country's previous experiences with Zika and chikungunya informed its response to COVID-19. He stressed the importance of having translators or "interpreters" who can understand multiple aspects of public health and bridge across disciplines and sectors. Expanding on this point, Saul Walker (Coalition for Epidemic Preparedness Innovations) said that during the COVID-19 response, the world drew upon the experience of countries in the Global South that regularly face disease outbreaks.

Infectious disease public health investments often follow a cycle of "neglect and panic," in which focus and investments dissipate between crises. Walker stressed that sustained investments in-between epidemics are essential for laying the groundwork so that when a crisis emerges, the relevant partners already know how to work together and are poised to switch into response mode. He noted that the aspects of the COVID-19 response that went relatively well were those areas in which sustained investment in science and infrastructure existed ahead of time, such as in mRNA and other technology platforms that allowed vaccines to be developed, manufactured, and delivered at record speed.

For countries to make impactful investments in pandemic preparedness and response and reap the benefits of these investments, many speakers pointed to one essential ingredient: trust. On the part of leaders, trust is critical for generating the political will to invest in preparedness. As Lisa Hilmi (CORE Group) summarized, "It's clear without country and regional leadership and buy-in, our efforts of preparedness and response will fail." Conversely, the public's trust in their leaders and institutions influences how successful the response will be. "In times of crisis, public trust is not just important; it is indispensable. It is a glue that holds societies together, the foundation upon which successful responses are built, and the light that carries us through the darkest of times," said Ayoade Alakija (African Vaccine Delivery Alliance).

Building trust is important at all levels, but several speakers emphasized that grounding trust in the community is most effective. "Pandemics begin and end in communities. Starting to build that trust at the community level, engaging communities in prevention, detection, containment [is] absolutely vital," said

Priya Basu (World Bank Group). Noting that nothing that is developed on a global scale can replace domestic activities fully, Sara Hersey (WHO) said that building trusted in-country resources is essential and added that global efforts also can be made more effective by tapping into existing trusted regional networks and organizations.

Investing in Pandemic Preparedness and Response

Speakers examined how different countries and organizations currently prioritize pandemic preparedness and response along with evidence relevant to prioritization approaches for strengthening disease surveillance and risk communication capabilities.

Several speakers emphasized the value of starting with existing capacities and capabilities and building from there. Irma Makaliano (University of the Philippines) highlighted how the Philippines took this approach in its response to the COVID-19 pandemic. For example, to fill gaps in disease detection laboratory equipment and infrastructure in its health care systems, the country was able to repurpose and use resources and expertise found in its research facilities and universities. In addition, Makaliano stressed the importance of strengthening primary care systems as a foundation upon which to add enhanced science, technology, and surveillance capacity.

Alakija described the PACTT framework for strengthening global health security, which involves five fundamental elements: prevention, access, countermeasures and tools, and trust.1 Hersey highlighted how the WHO is working toward a global architecture for preparedness and response that builds capacity for collaborative surveillance, emergency coordination, community protection, access to countermeasures, and clinical care through its Epidemic and Pandemic Hub. In particular, the International Pathogen Surveillance Network, a recently launched global network bringing together pathogen genomic data to improve public health and decision-making, aims to coordinate existing systems, networks, and capacities.

Rather than thinking in terms of a short-term project, Hersey underscored the need for long-term investments to build institutional capacity, both domestically and internationally. In guiding these investments, she added that overcoming silos and attending to the interdependencies among different facets, such as on-the-ground surveillance systems and the laboratories needed to support testing, are important. Walker added that efforts to build institutional capacity ought to focus on long-term goals, but also deliver on the value of capacity-building in the near term by putting surveillance and response systems to the test to strengthen systems, provide positive feedback, and build trust.

Another common theme that several speakers raised is the value of thinking about the context of pandemics from multiple dimensions. As Alakija put it, “We cannot do epidemic preparedness in a vacuum.” Focusing too much on quantitative data points without understanding the social context for those numbers can lead to incorrect interpretations or risk missing crucial nuances. Building on this point, Marty Cetron (U.S. Centers for Disease Control and Prevention) noted that pandemics enter societies that constantly are being shaped by politics, conflict, and other public health contexts and challenges. He cautioned that although syndemics (i.e., two or more concurrent or sequential epidemics that synergize and exacerbate the disease) are increasing in frequency, duration, magnitude, geoscope, and speed, most countries and organizations have not established a model of pandemic preparedness and response that takes this context into account. Thinking about pandemics only from a pathogen-focused perspective overlooks the social context in which these events play out.

To enable decisions and actions that are responsive to context, Cetron suggested establishing ways to measure readiness that are appropriately multidimensional. Several speakers highlighted the importance of investing in integrated surveillance systems, laboratory capabilities, and high-quality data systems aligned with the “One Health” approach.2 As Hersey highlighted, surveillance is valuable not only in health emergencies, but also for understanding how the emergence, management, and elimination of diseases interacts with complex contexts like conflicts and natural disasters. To capture this complexity, she suggested moving away from the traditional focus on linear, geographically constrained tracking of new cases and mortality rates and toward modes of collecting and analyzing data that capture multiple health, economic, and social contexts.

How people perceive the threat of pandemics is also important. Although familiarity with disasters like floods and earthquakes have led to greater understanding about their scale and scope, Larry Brilliant (Pandefense Advisory) pointed out that the risk of occurrence of a pandemic is in some ways incalculable. At the same time, having so recently experienced the COVID-19 pandemic can give people the erroneous impression that another pandemic is unlikely to happen for a while. Since the risks of a pandemic are both incalculable and increasing, he said resisting the temptation to let down our guard is crucial.

Finally, several participants emphasized the benefits of investing in people and embedding equity in pandemic preparedness and response. “While we are thinking of advanced science and technology [and] infrastructure, we always, always have to remember to invest in people,” said Makalinao. This includes training the next generation of frontline health workers and preparing other groups and institutions that are not traditionally considered part of the public health system, such as, in the case of the Philippines, the police and army.

Effectively translating policy into practice may rely on equity in access, funding, decision-making, and power. Alakija described how inequities have undermined public health and crisis response, such as the history of religious and political tensions including a situation from northern Nigeria that delayed the global polio eradication effort back by a decade. To avoid missteps and increase the likelihood of success in public health, she stressed that people in communities most affected by health issues need to be included in the process of addressing them. “Trust cannot be an afterthought,” she said. “These conversations have to begin with those with the lived experience.”

Finance and Governance Structures

For global health investments to be robust, reliable, and sustainable, appropriate governance structures to support them likely are important. Speakers discussed considerations for political engagement, partnerships, and financing to support ongoing investments in pandemic preparedness and response.

Some speakers emphasized effective political leadership, a sense of shared responsibility, and a whole-of-society approach. Implementing pandemic preparedness is a journey that requires a long-term commitment at both the global and national levels, Basu stated, noting that the World Bank has seen an encouragingly strong level of commitment among low and middle-income country governments, which she hopes will be sustained at the national level as a complement to international financing. Several speakers pointed out that political engagement is helpful for sustaining investments, and Correia noted that political extremism and destabilization of democracies can undermine countries’ ability to respond to health emergencies. Wessam Mankoula (Africa Centers for Disease Control) described political engagement as an organic process of bridge-building in which parties learn to speak each other’s languages and acknowledge the needs and priorities of others. “We don’t buy political engagement; we build political engagement,” he said. This is true within countries and for harmonization between country and regional plans. Alakija described how the African Vaccine Delivery Alliance provides a good model for bringing multiple parties to the table, including international institutions such as the WHO, to coordinate actions around a shared goal. Walker added that focusing on enabling innovation, adaptability, and agility in pandemic preparedness such that the basic infrastructure and organizing principles are in place and can be built upon when crises emerge is important.

In addition to policy, funding allocations are important for pandemic preparedness and response. Duncan Selbie (International Association of National Public Health Institutes) said that budget allocations—not stated strategies—reveal a country or organization’s true priorities and level of commitment. He also stressed the importance of recognizing preparedness efforts not as a cost but as an investment that will reap returns by saving lives, saving money, and supporting healthy economies.

Basu said that harmonizing different investments and efforts can create a multiplier effect among funds provided by domestic and international organizations and help maximize their impact. Based on this notion, she said that in making grant decisions the World Bank looks for evidence that relevant institutions are complementing each other’s activities both in terms of technical expertise and co-financing. Walker reiterated the importance of complementarity between domestic, regional, and international actors. Although national and regional research and development (R&D) programs are often a locus of investment, he said they are necessary but not sufficient for pandemic preparedness and underscored the need to take a broader view of preparedness that recognizes the complexity and diversity within R&D and health services ecosystems.

ISSUES AND OPPORTUNITIES DISCUSSED IN BREAKOUT SESSIONS

Attendees further explored aspects of pandemic preparedness in a series of concurrent small group discussions on issues and opportunities in five key areas: situational awareness; trust, transparency, and risk communication; governance, financing, and accountability; capacity and functionality assessment; and preparedness and response planning.

Situational Awareness in the Context of Health and Diseases

Brilliant summarized a discussion focused on situational awareness. Highlighting that disease outbreaks are inevitable—given human encroachment onto animal territories and the more than 300,000 uncharacterized animal viruses with zoonotic potential3—he said that early disease detection, continual surveillance, and situational awareness are critically important to containing outbreaks before they become widespread. Emerging digital and participatory surveillance techniques discussed by Mark Smolinski (Ending Pandemics) represent a significant improvement over routine clinician and government reporting, and some participants indicated that these tools could be used to identify new diseases and detect outbreaks more quickly.

In addition, several participants said that countries could build surveillance systems that fit their unique cultures and economic circumstances. For example, in Cambodia, which has a low smartphone penetration rate, the government created an analog phone reporting system to monitor and detect outbreaks. It was initially philanthropically funded and now has sustainable government support.

Finally, many participants reiterated the importance of building community trust. Communication strategies that listen, respond, and deliver benefits to the involved parties can create value and build trust, increasing the likelihood that communities will continue to voluntarily contribute health information. Voluntary participation at the community level is one strategy for moving from surveillance to a system of continuous situational awareness to monitor public health and detect crises.

Building Trust, Transparency, and Risk Communication Capabilities

Richard Garfield (U.S. Centers for Disease Control and Prevention) shared his group's comments regarding trust, transparency, and risk communication. To prepare for and to respond to public health crises, many participants said supporting community engagement that prioritizes honesty, openness, and simplicity is just as important as providing funding for medical equipment. They stressed that continuous, bidirectional communication—an ongoing program of listening to key community groups and testing messaging strategies for mistakes and missteps—among public health organizations avoids seeming unprepared and disconnected from vulnerable communities during a crisis. "There's always time to have some dialogue; there's always time to listen back," Garfield said.

Another example strategy that some participants mentioned is to separate risk communication from messaging about healthy or preventive behaviors, and to use different phrasing for these different types of health messages. Combining the two messages can be misinterpreted and seen as subjective, manipulative, or illegitimate.

Finally, during emergencies, Garfield said that researchers could practice market segmentation by defining the situation, identifying the impact on different groups (especially historically disadvantaged groups), and determining the most effective communication and engagement strategies before asking people to act.

Strengthening Global Health Security Through Strong Country-Level Infrastructure for Effective Governance, Financing, and Accountability

Julie Wahl (Resolve to Save Lives) summarized the discussion of governance, financing, and accountability considerations. The group discussed improved legislation, communication, public-private community coordination, and national and local monitoring and evaluation systems to improve countries' preparedness, capabilities, and accountability in outbreak detection and prevention. Because access to resources can vary within countries, promoting equity and social protection within accountability systems may be beneficial. In addition, some participants thought that monitoring and evaluation systems could be linked to specific measurement tools that can aid regular accountability, capability, and financial needs assessments.

Some participants stated that providing adequate funding for domestic health security programs can improve accountability and coordination across government agencies, community groups, and the private sector. They described how financing of these programs in under-resourced nations, which typically rely on philanthropic donations, has been a significant challenge, but some countries have overcome these issues. For example, Ethiopia and Uganda have funded domestic preparedness teams and steering committees that support multisectoral coordination and governance and accountability demonstrating effective country-led ownership.

Finally, although most financial cases for disaster spending focus on the response costs, Wahl said that advocating for increased spending on effective preparedness could be bolstered by research quantifying the return on investment for these initiatives.

Global Health Capacity and Functionality Assessment

Jessica Petrillo (U.S. Agency for International Development) and Aamer Ikram (National Institute of Health, Pakistan) shared reflections from the discussion on global health capacity and functionality assessment. Prior to the discussion, participants listed and described existing assessment tools.4

Several participants highlighted the importance of engaging with local communities and ensuring that they have access to tools that provide timely, high-quality data for improving their capacity and functionality are important. They suggested that these tools could benefit from funding to overcome several challenges: potential language barriers, the overwhelming number and complexity of the tools, the need for training, and the lack of data interoperability, which results from different domestic and international data standards and overall data siloing. In addition, some participants suggested promoting partnerships across public and private sectors that are appropriate to the overall ecosystem and its capabilities.

Moving forward, several participants suggested seeking out, celebrating, and emulating more examples of successful tools, communication strategies, and public health programs that empower community assessments. For example, the COVID-19 crisis has been a rich experience that could be examined for successes that can be used as models for a realistic global strategy of government-led sustainable practices to prevent future epidemics. Examples of successes include improving data interoperability and enhancing countries' primary health care systems.

Country and Organization Experiences in Preparedness and Response Planning

Erwin Calgua (Universidad de San Carlos de Guatemala) summarized a discussion of the experiences of different countries and organizations in preparedness and response planning. One lesson from these experiences, he said, is the importance of addressing inaccurate or misleading information about biology or disease outbreaks. External assessments are only useful if communication strategies depict them as apolitical and legitimate; at the nexus of public health, decision-making, and policymaking; and connected with the well-being of all people.

He highlighted that although several regions and countries had specific networks in place that helped them respond to the COVID-19 pandemic, they had to operate in a dynamic and global context. Those that had increased laboratory facilities and capabilities were able to collect and analyze data more quickly, allowing them to have a more flexible response.

Calgua also reiterated that health emergencies are not only caused by pathogens, and they likely will never go away. The next pandemic is likely to combine with factors like climate change and conflict, underscoring the importance of a holistic and all-encompassing public health approach.

EXAMPLE ACTIONS FOR EVIDENCE-BASED PRIORITIZATION OF GLOBAL HEALTH SECURITY CAPABILITIES

Throughout the symposium, speakers, moderators, committee members, and other attendees suggested a variety of actionable approaches to enhance pandemic preparedness and response. For the final session, planning committee members compiled the approaches that had been suggested during the first two sessions, and participants engaged in an interactive exercise and discussion to consider their relative urgency and feasibility. Committee members and participants also discussed ways to overcome obstacles, and specified some actors who could be involved in implementing the actions. Actions on assessments; data and information-sharing; and policy, frameworks, and planning were the focus of this exercise.

Global Health Security Capacity and Functionality Assessment

One theme throughout the symposium was the importance of tools and strategies for assessing pandemic preparedness that are relevant across different country contexts and levels. Table 1 at the end of this document lists the tools that Petrillo and Ikram prepared in advance of the symposium.

Several participants highlighted capacity and functionality assessments that are accessible and minimally burdensome, generate informative data, and are capable of influencing actions at the local, subnational, and national levels. Some participants suggested that assessment tools be available and accessible to all people. For this to be realized, involving language and communication experts can help to make tools understandable to users. Richard Seifman (World Bank) pointed out that a country's official national language is not always the language spoken in the communities that will be important for surveillance, detection, and response, so considering how to use technology or other solutions to rapidly translate materials into relevant local languages will be important.

Real-world examples of successful implementation of actions can be highly informative, and many participants suggested incorporating such examples when developing plans for filling gaps and strengthening overall capacity. Some participants also suggested that assessment tools could be improved by focusing on specific activities, such as partnerships and collaboration, long-term investment, data collection capacity, use of language, and policy and government frameworks. Kavita Berger (National Academies of Sciences, Engineering, and Medicine) suggested that focusing on the country context when determining what data to collect may help, given that different types of data will be available or applicable in high-resource and low-resource countries.

Who is involved also matters. To effectively assess particular capacities and the overall system, several participants said including many sectors and diverse actors in the development and use of assessment tools are important. Many participants stated that this is urgent, but disagreement existed about its practicality.

Throughout the symposium, some participants expressed concern about balancing the objective of assessing preparedness and the burden of collecting data for those assessments. Speaking to this issue, Garfield stressed the need to focus on what information truly is needed. Every tool uses data, which is then provided, collected, and analyzed. As a result, trying to "learn everything" imposes a large burden on people and organizations and can hinder progress. Rather, he said the focus could be on determining what is actually needed for decision-making, and success could be measured by whether assessments help people do a better job. Sometimes, he added, this will mean identifying assessment tools or data that could be retired or moved into the realm of academic research rather than playing a more integral role in public health systems.

Participants explored various ways to reduce the burden of assessments and enhance their value. Evaluating the effectiveness of assessment tools at the local level was viewed positively by many participants, and some participants also highlighted the importance of better integrating local data into local, subnational, and national assessment and decision-making. Jennifer Lasley (World Organisation for Animal Health) pointed out that people who provide their data want to see that it is being used to inform decisions or generate some benefit, particularly when the tools are in analog form. Often, information is used one time and then lost. "We're not leveraging the effort that it takes for countries and stakeholders to provide that information, which probably was really hard to get in the first place," Lasley said. To make better use of data for assessments, some participants said that digitizing data and enhancing capacity and systems with appropriate staffing, expertise, data systems, and political support, among other capacities can be important. However, they acknowledged that some of these may pose challenges. Lasley posited that the onus is on organizations that create and use assessment tools to stop using single-use and analog approaches and invest in sustainable, long-term digital data.

Several other strategies for improving assessments were seen by many symposium participants as being of lesser immediacy even though they may be practical to implement. These strategies include using independent peer review processes and locally relevant criteria to assess country capacity; collecting existing capabilities that are available through academic, government, and healthcare systems; and incorporating an understanding of the context for integration of the tool across levels, including consideration for factors such as trust, resource allocations, and information and communications technology infrastructure. Some participants stated that use of assessments to compare capabilities among countries is not helpful.

Data and Information-Sharing

Several suggestions related to data collection and use were discussed. One goal was to develop data standards for assessments. Several participants highlighted that this is an important goal, but several disagreed about its feasibility. For example, Emily Ricotta (National Institutes of Health) noted that implementing data standards is complicated by language and cultural differences among different countries and contexts. Another suggestion was to conduct proof of concept demonstrations to show how information and processes involved in assessments could be digitalized into data that can help make future assessments more useful.

Another suggestion was to improve the interoperability, interconnectedness, and integration of assessment tools and data at multiple levels, from facilities to countries. One practical measure this could involve is to establish agreements to assist in data sharing, availability, and use. In the same vein, some participants stressed the value of integrating and balancing information-sharing platforms, resources, and other mechanisms of cooperation across sectors and multi-levels of governance to build equity and surveillance.

These activities are not without challenges. Cetron noted that the ability to monetize data creates incentives to make them proprietary and hoard it, rather than sharing them freely. A further complication is that different actors do not always share the same core values regarding what types of data can be owned and which are communal resources for the common good. Resolving these issues likely involves participatory processes that recognize the values of many different parties, but that is difficult to achieve. Petrillo added that many challenges from a technological perspective also exist. Facilitating connections among different data systems may benefit from significant investments in data integration architecture, which in turn involves political will, appropriate financing, and mechanisms for bridging between silos, such as facilities that handle human data and those that handle animal data.

Some participants stressed the importance of having access to quality, actionable data in a timely manner to help assess capacity and functionality gaps, and to analyze the data to inform decision-making and develop evidence-based policies. Recognizing that assessments can impose burdens on local actors, many participants suggested better defining what data will be informative and available, although some noted that this could be challenging. Some participants also emphasized incorporating measurements of capabilities that look across sectors and are more intuitive, in contrast to a traditional emphasis on linear and more siloed approaches. Other ideas discussed included (a) reframing preparedness and investment in ways that recognize the interdependence of capabilities, and (b) considering the causal relationships among actions.

Policy, Frameworks, and Planning

Policy is one crucial tool in the response to public health threats. Several participants discussed two potential actions for informing policy decisions: (1) establishing active monitoring within any rapid policy changes that happen during disease outbreaks; and (2) following up with policy impact evaluations to understand the effectiveness of policy and financial investments. Other potential strategies are to use implementation research and case scenarios to inform policy advice, and to align country and regional plans. Strategies seen as practical include breaking broader strategy plans into smaller, more manageable activities based on a country's current capacity to reduce bottlenecks and considering the synergies between noninfectious diseases and infectious disease outbreaks in preparedness planning.

Ideas from participants related to prioritization frameworks include developing a maturity framework to inform ad hoc responses to epidemics; developing a framework for translating capability gaps into tangible actions within different cultural contexts, along with methods for assessing progress toward implementation; and promoting alternative structures to facilitate plans for countries that are missing governance structures to support preparedness activities.

OTHER EXAMPLES OF ACTIONS FOR STRENGTHENING EPIDEMIC PREPAREDNESS CAPABILITIES

Several other examples of potential actions were mentioned during the discussions.

Risk Communication and Public Engagement

Two suggestions in risk communication and public engagement were highlighted by some participants: (1) pursuing people-centered, community-led engagement and partnerships; and (2) engaging the public in an ongoing manner with mechanisms for direct and indirect avenues of communication. In terms of risk communication strategies, some participants suggested communicating frequently using multiple media venues; incorporating research-based strategies for communicating around uncertainties; and translating key pieces of information into straightforward content that can be easily digested and communicated by trusted messengers.

Several participants emphasized some helpful example approaches: investing in communication strategies before an outbreak so that systems are in place ahead of time; conducting formative evaluations to test messages; collecting communication success stories within countries that have a decentralized health system; and establishing standards that inform the evidence and data, communication, and decision-making in an emergency. Having more translators who understand the relevant cultural complexities can help to build community trust, and some participants suggested that these trusted messengers could be armed with lessons learned from what was effective in previous public health actions. Finally, some participants noted that addressing misinformation and fake news and understanding the channels through which false information spreads are vital.

Preparedness and Response Capability-Building

In building capacity for pandemic preparedness and response, several participants highlighted the importance of building capacity at the country level and in communities and across regions. Infrastructure also was highlighted as a critical part of capacity-building. Some participants suggested that countries could develop plans to scale up core infrastructure and organize programs such as epidemiological surveillance teams, laboratory services, and communication teams ahead of time. In addition, several participants pointed out that these capabilities could be tested in outbreak settings, and that preparedness efforts overall could benefit from continually being evaluated and monitored.

To advance these general capacity-building goals, some participants mentioned potential strategies: leveraging existing structures and partnerships; building relationships and communication around local cultural practices; closing gaps in formal and structural supervisory performance capacity to increase multisector coordination; and taking a systems approach to both creating resilient and sustainable health systems and assessing those capacity-building efforts. Several participants also highlighted the importance of considering climate and environmental health in strengthening pandemic preparedness capabilities.

Symposium discussions also surfaced opportunities in the specific areas of surveillance, response, and vaccine deployment. For surveillance, some participants said that countries could enhance training of community workers, especially in remote settings. In addition, implementing surveillance plans and combining surveillance across social and environmental factors can help to increase data use and sharing for pathogen surveillance efforts. In terms of response capacity, several participants underscored the importance of including mental health in preparedness planning and suggested creating teams that are equipped to serve multiple purposes, responding not only to health emergencies and potential pandemics, but also to crises arising from climate change, natural disasters, conflicts, and displacement.

To leverage vaccines more effectively in pandemic response, some participants suggested countries could learn from organizations and countries with experience in quickly mobilizing vaccine delivery and procurement systems using global supply chains for vaccines, drugs, and diagnostics. These can be made more resilient to shortages by investing in local manufacturing opportunities to support vaccine dissemination and lessen response time. The discussions also underscored concerns about vaccine hesitancy among different populations.

Commitments and Financing

To make headway and sustain preparedness activities, several participants mentioned political will, accountability, and funding. Some participants stressed the importance of ownership of these efforts at the country level, and others noted that including local needs and capabilities in national and regional level response decisions involves ownership and coordination across all levels and sectors. Several participants noted the value of capacity strengthening, including with technology and coordination, to support governance at country and regional levels, and added that alternative structures may be needed to facilitate planning in countries without governance structures suitable for supporting preparedness activities.

Monitoring the status of pandemic preparedness and capacity is important to ensuring interested parties are accountable to the commitments they make. Many participants suggested employing tracking tools and other resources, developing a certification process for data analysis, and openly sharing monitoring systems to increase cooperation and amplify health safety measures across countries and regions.

Participants offered a range of suggestions to support funding for pandemic preparedness activities, noting that different models may be needed in different countries and regions. Several participants suggested focusing investment on institutional capacity-building. Other, more specific examples include establishing sustainable funding for financing the health sector and securing funds to facilitate health communication. Many participants suggested that public-private partnerships can be helpful, as can working with philanthropies to reduce the financial risk that governments take on. Noting that preparedness financing is frequently subject to boom-and-bust cycles, Brilliant underscored the need to establish sustainable funding models, even in lower-resource countries. As an example, he pointed to Thailand's use of taxes from specific sectors—namely, alcohol, cigarettes, and prostitution—to create the Thai Health Promotion Foundation, which supports many aspects of the "One Health" approach to public health improvement along with pathogen surveillance and situational awareness. Although the same model would not necessarily be appropriate for every country, he suggested that “the action item is to look at each country’s ability to deal with being able to uniquely develop the mechanism for having sustainability, reliability, and assurance that money and resources will be there when they’re needed.”

Partnerships, Equity, and Education

Pandemic preparedness is a multifaceted issue that involves and affects all sectors and communities. Many participants underscored the importance of building partnerships with communities—including diverse and historically marginalized groups—and upholding commitments made to them. To embed equity in preparedness activities, some participants said linking institutions and capacities to community benefits and working to ensure equitable access throughout implementation of preparedness investments and collaborations are important. Finally, several participants suggested working with academic researchers and relevant organizations to conduct research on the implementation of preparedness measures and strengthen guidance, and to provide opportunities for students and employees to gain experience and maintain knowledge and skills in public and international health.

Feature Article: First Responders Need to Know They’ll Be Heard

Source: https://www.dhs.gov/science-and-technology/news/2024/01/18/feature-article-first-responders-need-know-theyll-be-heard

Jan 18 – When a first responder enters a building during an emergency, they count on being able to communicate with their team at all times. Their safety and their ability to carry out the mission relies on knowing they can reach help and support anywhere that they need to go within a structure. This is why most state and local jurisdictions require that buildings have first responder coverage in every part of a building. While there is not a national requirement for in-building coverage for emergency communications, the overarching need has resulted in the creation of national model codes by the National Fire Protection Association (NFPA) and the International Code Council. Although primarily driven by fire service jurisdictions these requirements are intended to address emergency communications coverage for all first responder disciplines.

The Science and Technology Directorate (S&T) discovered through its Project Responder research that maintaining adequate communications inside buildings was a capability need that first responders wanted to work with S&T to address.

“First responders need constant communications, in fact, their lives are put at greater risk when they do not have constant, reliable communications in buildings. Yet, in many instances, their ability to safely access buildings in response to, for example a fire, is hampered by loss of communications. This can force them to either accept greater risk or more slowly respond to an emergency,” said Cuong Luu, subject matter expert for S&T’s Office for Interoperability and Compatibility Technology Center.

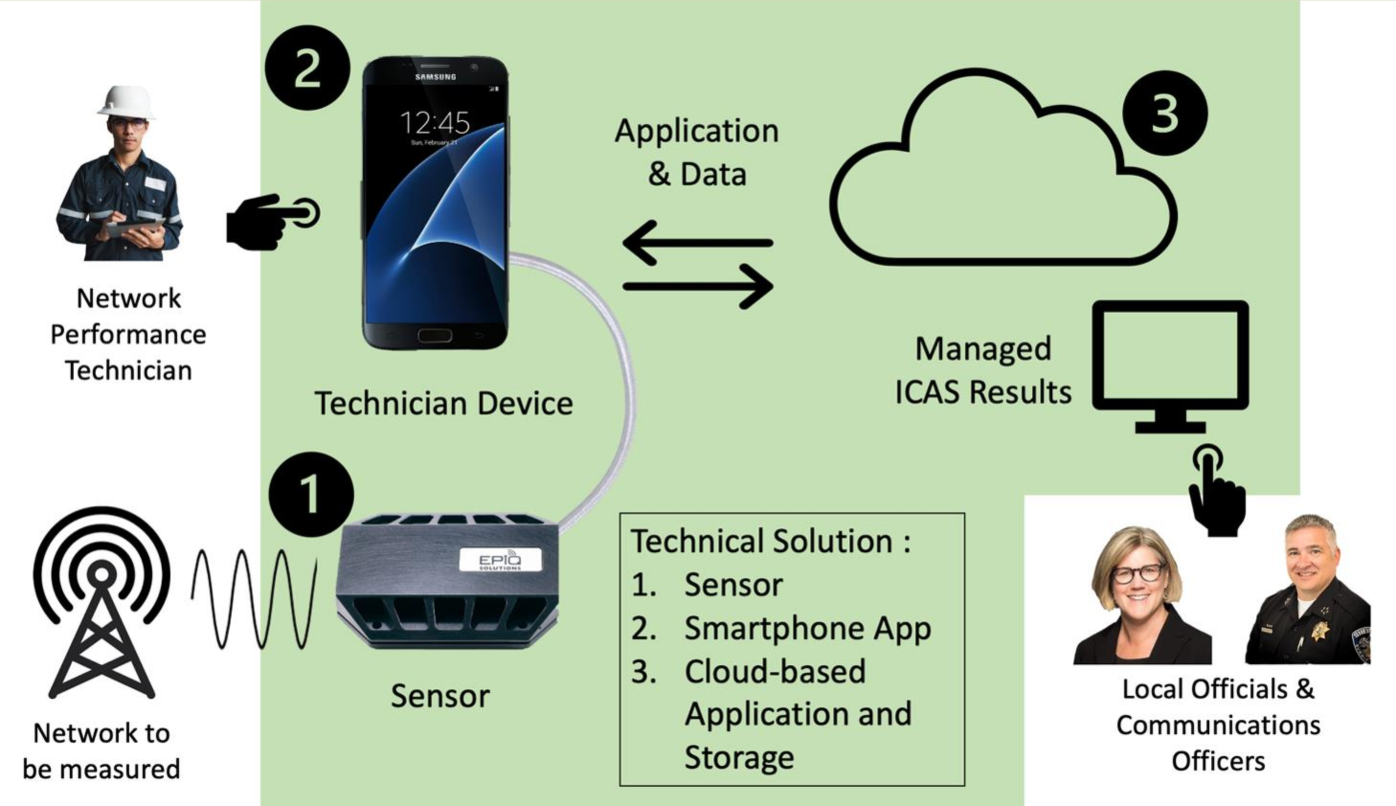
In order to bring new technologies to bear on this problem, the topic “In-building Coverage Analysis System (ICAS) Using Existing First Responder’s Radio and Smartphone” was included in the DHS Small Business Innovation Research (SBIR) Program 20.1 Solicitation. Epiq Solutions, Inc. was selected for a Phase I award and after successfully completing their feasibility study, was awarded a SBIR Phase II contract to continue research and development on their Low Size, Weight and Power (SWAP) In-building ICAS solution for commonly used first responders' network types. First responders typically rely on agency-issued Land Mobile Radios (LMR) to communicate in indoor settings. The availability of the FirstNet LTE network, a communications network created solely for first responders, is increasingly providing additional indoor public safety data services, such as physiological and health monitoring and location tracking to enhance personnel safety. However, the LMR and FirstNet networks are two completely separate networks—the LMR network is managed by state/local public safety organizations, while FirstNet is built and operated by AT&T through a public-private partnership. So, there remains a void in enabling first responders to record, access, capture and maintain the in-building service availability of each of these two different networks today and for the next five to ten years…and beyond.

There is also not a standardized method for testing and evaluating emergency communications coverage in buildings across jurisdictions. Evaluations depend on specific local regulations and often takes place one time upon completion of new construction. Quite often there is little-to-no follow up testing to see if conditions have changed due to new nearby construction or the modification of internal layouts, and there is no easy way to track and maintain data from previous tests.

“These kinds of reports have a shelf life,” said Cuong Luu. “A building goes in next door, and the conditions can change. Frequent and standardized testing allows for accurate real-time data.”

“In order to get to a place where we can have trusted in-building communications that extends the wide area network into buildings, we need to try to find a way to make testing and evaluation simple and low cost, and then it will be done more effectively and folks can trust the outcomes of it,” said Gary Schluckbier, director of Radio Frequency Sensing at Epiq Solutions.

As a result of the SBIR effort, Epiq Solutions has created PRiSM, a prototype that uses a low-cost sensor that can be connected to a standard smart phone, tablet, or laptop that produces measurements of the signal strength in the most commonly used first responder bandwidths and performance data which is then uploaded to a portal. The portal is a key element of this innovative solution; storing the data in an accessible online repository, where it is available to whoever needs it, whenever it's needed.



A diagram of the PRiSM In-building Coverage Analysis System Process. Photo credit: Epiq Solutions.

Instead of having a single initial test performed by a network performance technician when a building is issued its certificate of occupancy, with results that may not be easy to find or access, with this solution a building can be retested periodically with the technician only needing a sensor attached to a smart phone, and the new data can be compared to previous results. This data could also be accessed by first responders arriving on a scene, so that they can quickly assess whether they need to deploy additional communications assets. This is also a potential benefit to building owners and developers. Currently, testing requires complex and expensive equipment as well as highly trained personnel. Furthermore, there are no concrete test requirements from jurisdiction to jurisdiction. The goal is for the compact, low-cost PRiSM design to make it possible to test more often and to facilitate more broadly accepted best practices. In addition, the solution does not require highly trained, costly engineers to collect data further driving down costs. The next step for this technology is for Epiq Solutions to launch it as a fully available commercial offering.

The SBIR Program provides U.S. based small businesses the opportunity to propose innovative ideas that meet specific homeland security research and development technology needs and is one of the many ways S&T supports first responders. Making sure that local first responders can communicate at the scene of an emergency relies on a lot of important innovations, policies and technologies that are put in place long before the first alarm goes out.

New, Portable Antenna Could Help Restore Communication After Disasters

By Laura Castañón

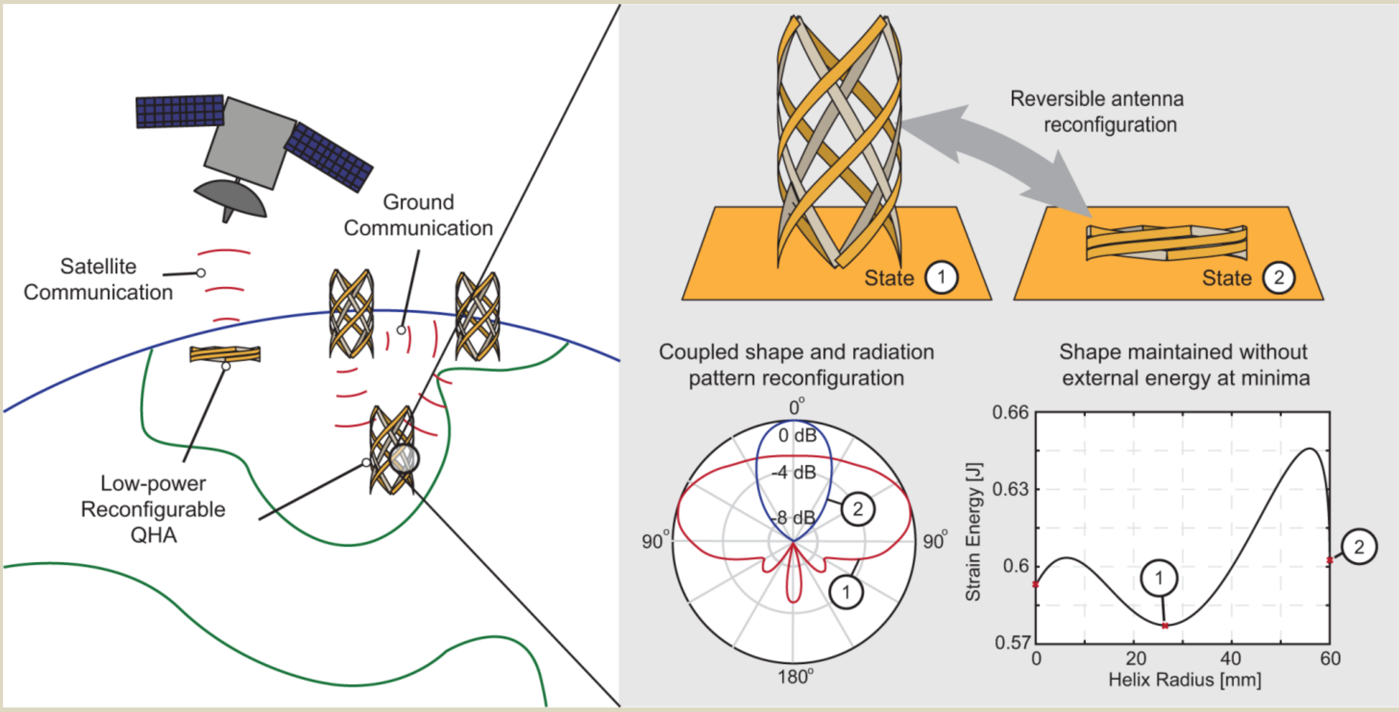
Source: https://www.homelandsecuritynewswire.com/dr20240120-new-portable-antenna-could-help-restore-communication-after-disasters

Jan 20 – When an earthquake, flood, or other disaster strikes a region, existing communication infrastructure such as cell phone and radio towers are often damaged or destroyed. Restoring emergency communications as quickly as possible is vital for coordinating rescue and relief efforts.

Researchers at Stanford University and the American University of Beirut (AUB) have developed a portable antenna that could be quickly deployed in disaster-prone areas or used to set up communications in underdeveloped regions. The antenna, described recently in *Nature Communications*, packs down to a small size and can easily shift between two configurations to communicate either with satellites or devices on the ground without using additional power.

"The state-of-the-art solutions typically employed in these areas are heavy, metallic dishes. They're not easy to move around, they require a lot of power to operate, and they're not particularly cost-effective," said Maria Sakovsky, an assistant professor of aeronautics and astronautics at Stanford. "Our antenna is lightweight, low-power, and can switch between two operating states. It's able to do more with as little as possible in these areas where communications are lacking."

Sakovsky is also affiliated with the Stanford SystemX Alliance.



Overview of the coupled structural and electromagnetic reconfiguration used by the proposed low-power quadrifilar helix antenna for low-infrastructure areas.

Two Functions in One Antenna

The researchers developed the antenna with an approach typically used to design devices that are being deployed in space. Because of fuel and space limitations, technology being sent into orbit must be very lightweight and packaged as small as possible. Once the items are in orbit, they unfold into the proper shape for use. The researchers wanted their antenna to be similarly collapsible and lightweight.

The antenna designed by Sakovsky and her colleagues at AUB, including Joseph Costantine, Youssef Tawk, and Rosette Maria Bichara, is made of fiber composites (a material often used in satellites) and resembles a child's finger-trap toy, with multiple strips of material crossing in spirals. Just like any helix-based antenna, conductive material running through the antenna sends out signals, but thanks to its unique structure, the researchers can adjust the pattern and power of those signals in the new antenna by pulling it into longer shapes or shorter shapes.

"Because we wanted the antenna to be able to collapse into a packable shape, we started with this structure that led us to a very untraditional antenna design," Sakovsky said. "We're using shapes that have never been used on helical antennas before, and we've shown that they work."

At its most compact, the antenna is a hollow ring that stands just over 1 inch tall and about 5 inches across – not much larger than a bracelet – and weighs 1.4 ounces. In this shape, it's able to reach satellites with a high-power signal sent in a particular direction. When stretched out to about a foot tall, the antenna sends a lower power signal in all directions, more like a Wi-Fi router.

Shifting between these two states is as simple as pulling or pushing on the antenna. These movements don't even need to be particularly precise because, once the antenna is moved past a certain point, the structure snaps to the right position. The specific size and shape of the antenna design will determine which frequencies those two states communicate across.

"The frequency you want to operate at will dictate how large the antenna needs to be, but we've been able to show that no matter what frequency you operate at, you can scale this design principle to achieve the same performance," Sakovsky said.

The fabricated prototype was tested for deployment and structural performance at Stanford and its electromagnetic radiation characteristics at the antenna measurement facilities at AUB.

Applications in Orbit

To be deployed in the field, the antenna would need to be paired with a transceiver to send and receive signals, a ground plane to reflect radio waves, and other electronics, but the whole package would still only weigh about 2 pounds, Sakovsky said. And the antenna's unique dual functionality means that it could replace multiple heavier antennas in areas where deployment is a challenge. That includes uses in disaster-struck and underdeveloped areas, but also, potentially, in space. Sakovsky and her colleagues are considering adapting their design for satellite communications, allowing satellites to use the same antenna to talk to each other and to talk to the ground.

"We don't have a lot of spare operating power, volume, or mass on our spacecraft either," Sakovsky said. "This holds a lot of potential for replacing multiple antennas on a satellite with a single one."

Laura Castañón is a freelance science writer and editor.

JoeHeller ©2017 HELLERTOON.COM
I'VE LOST EVERYTHING... I CAN'T IMAGINE HOW THIS COULD GET ANY WORSE.
IT'S A CONDOLENCE CALL FROM THE PRESIDENT.
CALIF.

ICI
International
CBRNE
INSTITUTE

A common roof
for International
CBRNE
First Responders

Join us!

Rue de la Vacherie, 78
B5060 SAMBREVILLE
(Auvelais)
BELGIUM

info@ici-belgium.be | www.ici-belgium.be