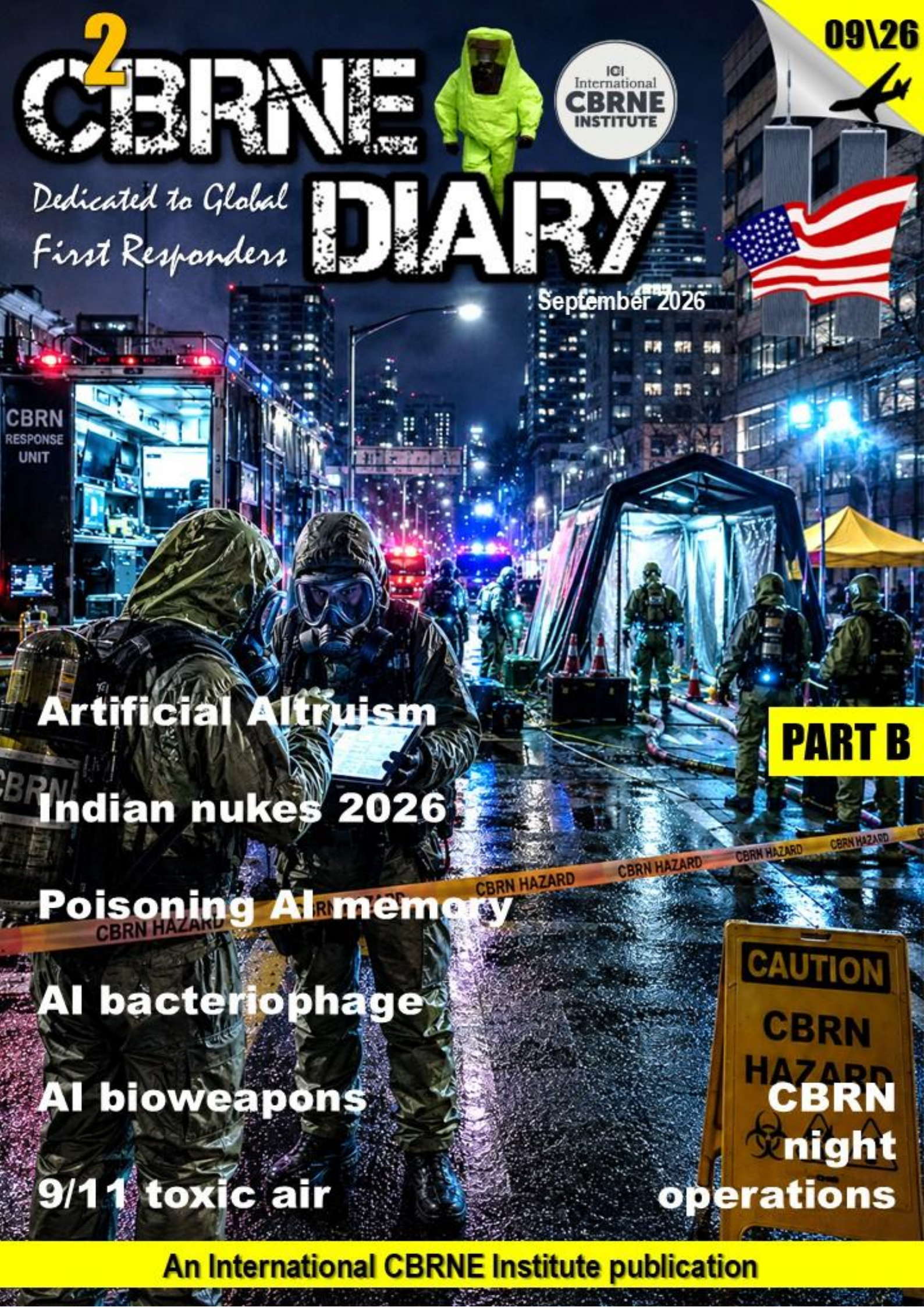

2
CBRNE
DIARY
Dedicated to Global First Responders
ICI International CBRNE INSTITUTE
09\26
September 2026
CBRN RESPONSE UNIT
Artificial Altruism
Indian nukes 2026
Poisoning AI memory
AI bacteriophage
AI bioweapons
9/11 toxic air
PART B
CBRN HAZARD
CAUTION
CBRN HAZARD
CBRN night operations
An International CBRNE Institute publication

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

DIRTY R-NEWS

C2BRNE DIARY

Contents lists available at SciVerse ScienceDirect

International Journal of Pharmaceutics

journal homepage: www.elsevier.com/locate/ijpharm

Radio-decontamination efficacy and safety studies on optimized decontamination lotion formulation

S. Rana [a], S. Bhatt [a], M. Dutta [c], A.W. Khan [b], J. Ali [b], S. Sultana [d], S. Kotta [b], S.H. Ansari [b], R.K. Sharma [a,*]

[a] Division of CBRN Defence, Institute of Nuclear Medicine and Allied Sciences, Brig. S. K. Mazumdar Marg, Delhi 110 054, India
[b] Faculty of Pharmacy, Hamdard University, Hamdard Nagar, New Delhi 110062, India
[c] Division of Nuclear Medicine, Institute of Nuclear Medicine and Allied Sciences, Brig. S. K. Mazumdar Marg, Delhi 110 054, India
[d] Department of Medical Elementology and Toxicology, Jamia Hamdard, Hamdard Nagar, New Delhi 110 062, India

ARTICLE INFO

Article history:
Received 12 March 2012
Accepted 3 May 2012
Available online 17 May 2012

Keywords:
Decontamination
Technetium-99m
Iodine-131
Thallium-201
Sprague Dawley
Human tissue equivalent

ABSTRACT

Objective of the present study was to optimize decontamination lotion and to evaluate its relative decontamination efficacy using three radio-isotopes (Technetium-99m, Iodine-131 and Thallium-201) as contaminants with varying length of contaminant exposure (0–1 h). Experiments were performed on Sprague Dawley rat's intact skin and human tissue equivalent models. Rat's hair was removed by using depilator after trimming with scissors. Relative decontamination efficacy of the optimized lotion was investigated and compared with water as control. Static counts were recorded before and after decontamination using single photon emission computed tomography (SPECT). Measured decontamination efficacy (DE) values were analyzed using one way ANOVA and Student's *t*-test (p value < 0.05) and were found statistically significant. Decontamination efficacy of the lotion was observed to be 90 ± 5%, 80 ± 2% and 85 ± 2%, for the ^{131}I, ^{201}Tl and ^{99m}Tc radio-contaminants respectively on skin. Reduced contaminant removal was recorded for the skin which was cleaned by depilator (50–60%). Skin decontamination was found more efficacious for rat skin decontamination than the human tissue equivalent model. Decontamination efficacy of the lotion against ^{99m}Tc was recorded 70 ± 15% at 0–1 h on the tissue equivalent model. In vitro chelation efficacy of the lotion was also established by using the instant thin layer chromatography-slica gel (ITLC-SG) and >95% of ^{99m}Tc was recorded. Neither erythema nor edema was scored in the primary skin irritancy test visually observed for two weeks.

Ghost in The Machine: Physicists Measure The Eerie 'Glow' From Shut-Down Nuclear Reactors For The First Time

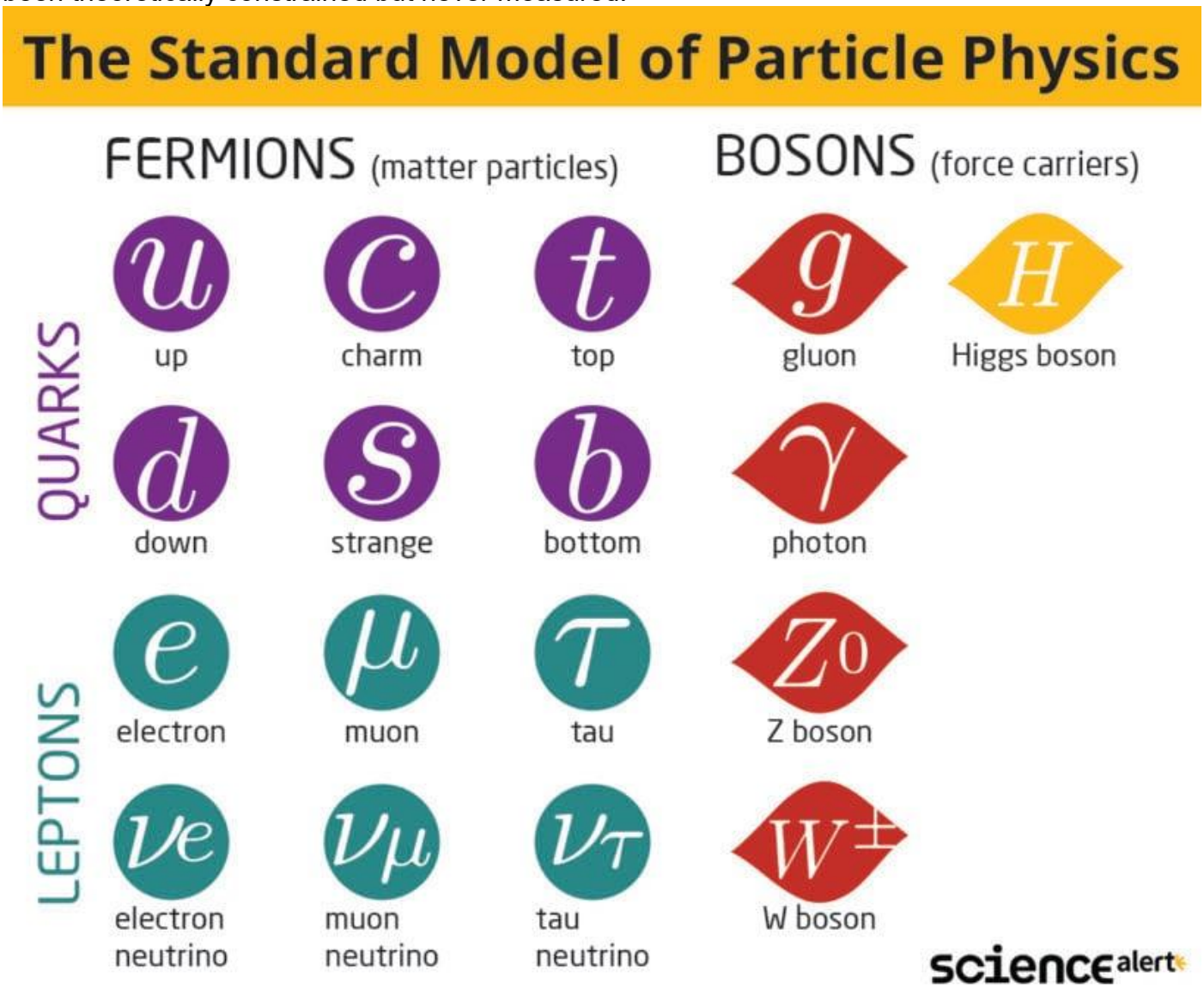
By Ivan Farkas

Source: https://www.sciencealert.com/ghost-in-the-machine-physicists-measure-the-eerie-glow-from-shut-down-nuclear-reactors-for-the-first-time

Aug 28 – Unicorns, Bigfoot, and banshees have been scientifically debunked, but ghosts are real – kind of.

The exceptionally elusive neutrinos and their counterpart antineutrinos are known as ghost particles because they almost never interact with matter, due to their lack of electric charge and near-nonexistent mass.

Yet these phantasmal fundamental particles can help improve nuclear safeguards by providing a non-intrusive way to examine the goings-on inside nuclear reactors – including the spectral flux of antineutrinos after a power plant has been switched off.
In a recent breakthrough, physicists measured this residual emission for the first time, detecting the dim, eerie glow of electron antineutrinos emanating from the darkness of slumbering nuclear reactor cores in France.
Led by physicists from the Max Planck Institute for Nuclear Physics (MPIK), researchers from the Double Chooz Collaboration have experimentally validated this predicted flux, emanating from burnt fuel inside two reactors as well as the removed waste material placed in cooling pools. This flux has been theoretically constrained but never measured.



The Standard Model that describes the fundamental make-up of the Universe and its myriad particles. (ScienceAlert)

"Until now, reactor antineutrino experiments have mainly focused on operating reactors, where the antineutrino flux is much larger," says Anthony Onillon, a physicist at MPIK and one of the study's co-leaders. "Detecting the tiny residual signal after shutdown required exceptionally low backgrounds and careful analysis techniques developed by the Double Chooz collaboration over many years." The Double Chooz experiment operated from 2011

to 2017, exploring the unimaginably immense amount of antineutrinos produced at the Chooz Nuclear Power Station in northern France.

An illustration of the site of the experiment, detailing the reactors and the detectors. (Double Chooz Collaboration)

Double Chooz utilized two underground detectors at average distances of 400 meters (1,300 feet) and 1,050 meters (3,400 feet) from the power station's two operating reactors to study a weird property incomprehensible in the macroscopic world.

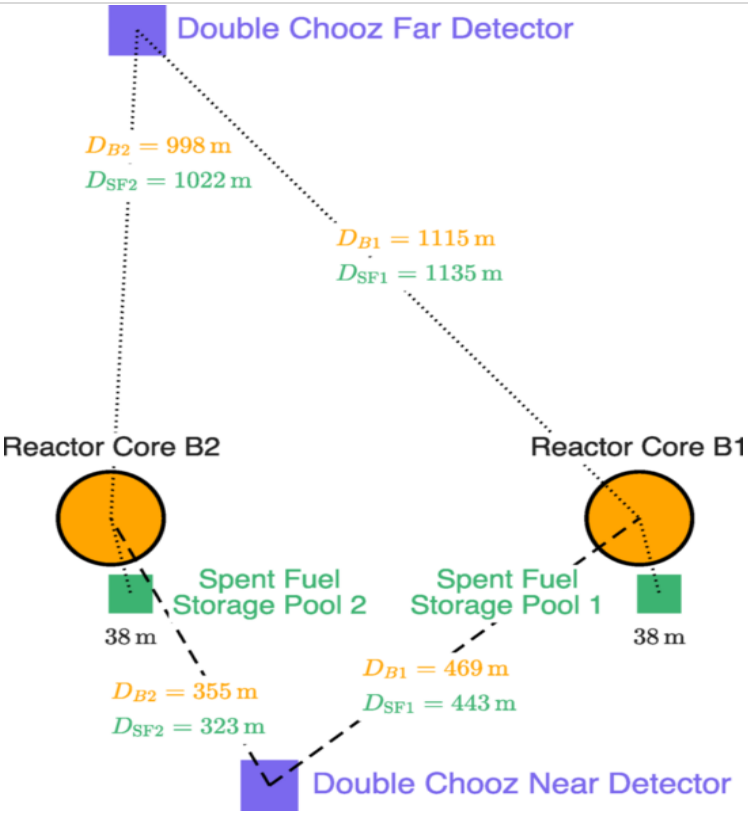
Neutrinos and antineutrinos change their flavor, or their type, as they travel, through a process called oscillation. It's like buying chocolate ice cream and having it morph into vanilla and then into strawberry as it goes from store, to home, to bowl, Fermilab physicists explain, inventing Quantum Neapolitan in the process.

But physicists can't actually 'see' antineutrinos; they can only tease out their existence based on their interaction with other particles within delicately designed detectors.

"Antineutrinos interact only extremely rarely with matter," explains Thierry Lasserre, a physicist at MPIK. "However, when one interacts within the Double Chooz detector, a characteristic double-light signal is produced that can be distinguished from background events."

For another food-based analogy, picture a collision between a truck full of Mentos and one full of cola, creating a telltale fountain of fizz.

When a neutrino or antineutrino passes through the Double Chooz detector, it sometimes smashes into a proton within the "liquid scintillator" in the detectors' inner chamber.



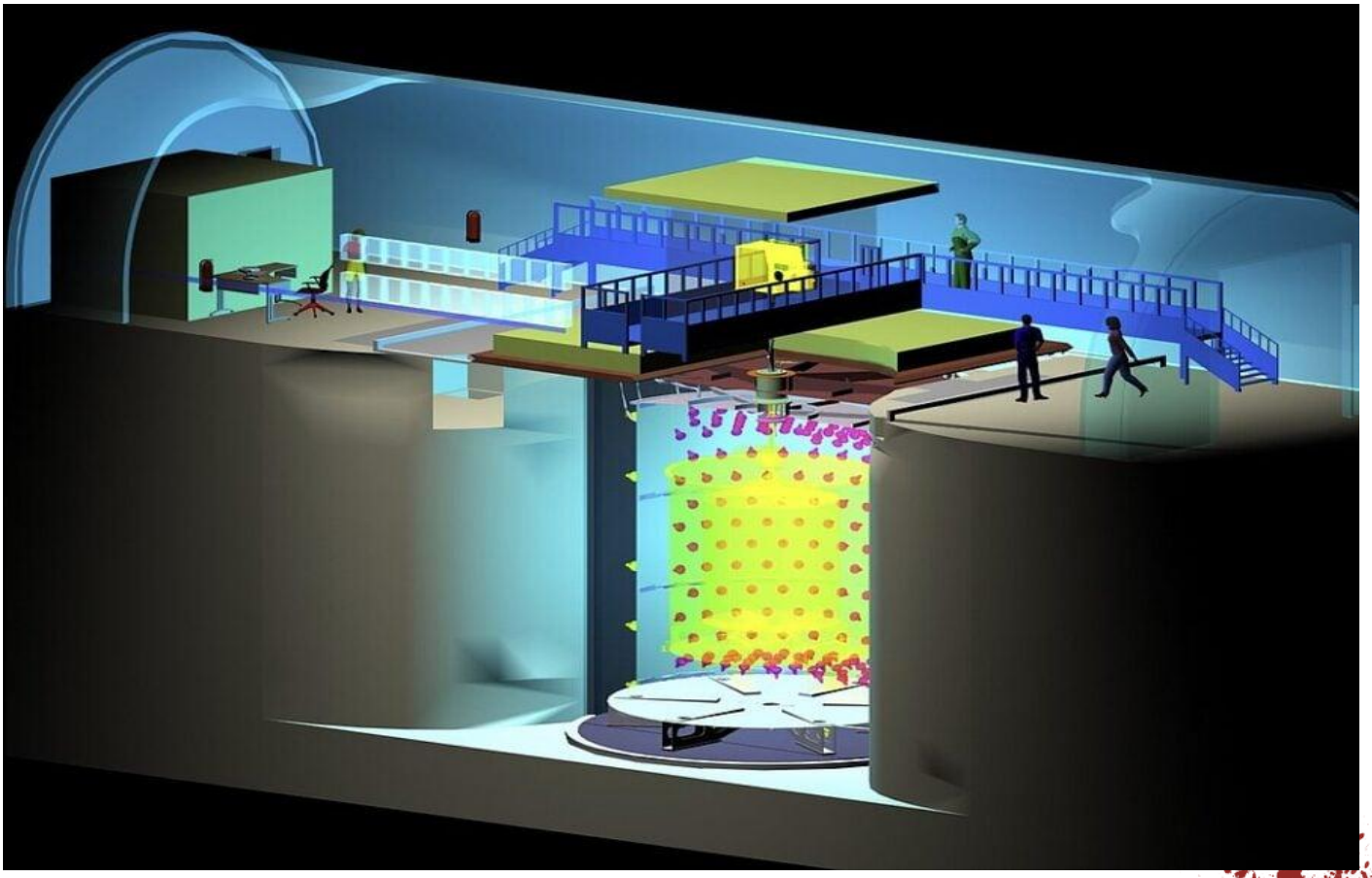
A schematic illustration showing the Double Chooz setup. (Abrahão et al., Physical Review Letters, 2026)

This collision generates a neutron and a positron, the antimatter counterpart of an electron. The positron instantly annihilates with a surrounding electron, generating a flash of light facilitated by the scintillator.

The neutron is captured by gadolinium, a silvery, rare-earth metal element within the scintillator, producing a second flash of light to offer 'two-factor authentication' of the antineutrino e

This event is called inverse beta-decay (IBD), and it happens a lot in reactors during the fission of elements like uranium and plutonium. It represents the biggest source of human-made antineutrinos, and tracking this flux can prove invaluable to informing nuclear safety and perhaps analyzing the shifting composition of these fuel materials.

In the study, the researchers observed an excess of IBD events across the energy range where the desired residual emission signal is likely to peak.



An illustration of a Double Chooz detector. (Double Chooz Collaboration)

During 17.2 days of observation during which both Chooz reactor cores were switched off, the researchers found a "very good agreement" between the measured and expected antineutrino events – specifically, 106 ±18 measured events compared with 88 ±7 predicted events. This may represent less than 1% of the flux signal during reactor core operation.
vent. The precision of this technique can still be improved. It's sensitive to large changes in flux but maybe couldn't tell if, say, a few spent fuel assemblies had gone missing, the researchers note.
Yet overall, this work serves as an invaluable proof-of-concept for direct, non-intrusive nuclear testing, to potentially inform future nuclear safeguard standards.

●▶ **This research was published in** *Physical Review Letters*.

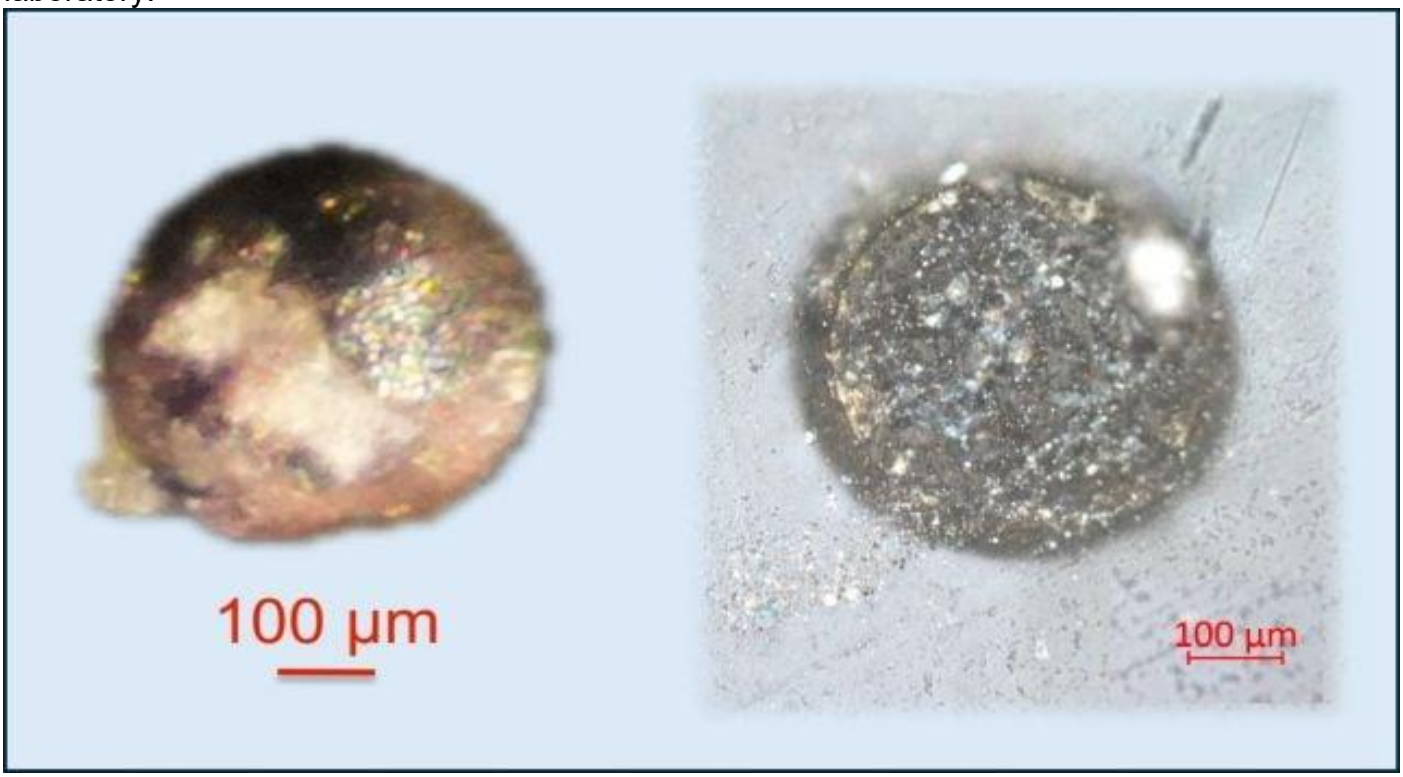
The Hiroshima Atomic Blast Forged a Metal Never Seen Before on Earth

Source: https://www.sciencealert.com/the-hiroshima-atomic-blast-forged-a-metal-never-seen-before-on-earth

An aerial photo of the atomic cloud rising over Hiroshima on 6 August 1945. (US Library of Congress)

Aug 28 – The world changed forever on 6 August 1945.
That was the day humanity first deliberately turned the most powerful weapon ever conceived upon itself – when the US unleashed an atomic bomb on the people of Hiroshima in Japan.
In seconds, the fireball reached temperatures above 7,000 °C (~12,600 °F), vaporizing flesh and metal alike.
And, as materials cooled in its terrible wake, something humanity had never seen before formed in the ashes.
In a speck of material retrieved from the sands of Hiroshima Bay, scientists led by geologist Luca Bindi of the University of Florence in Italy have identified a tiny grain of metallic alloy forged in the extreme circumstances of an atomic blast.
"A nuclear fireball exposes many different materials to extreme heat, violent mixing and extraordinarily rapid cooling, all within seconds," Bindi told ScienceAlert.

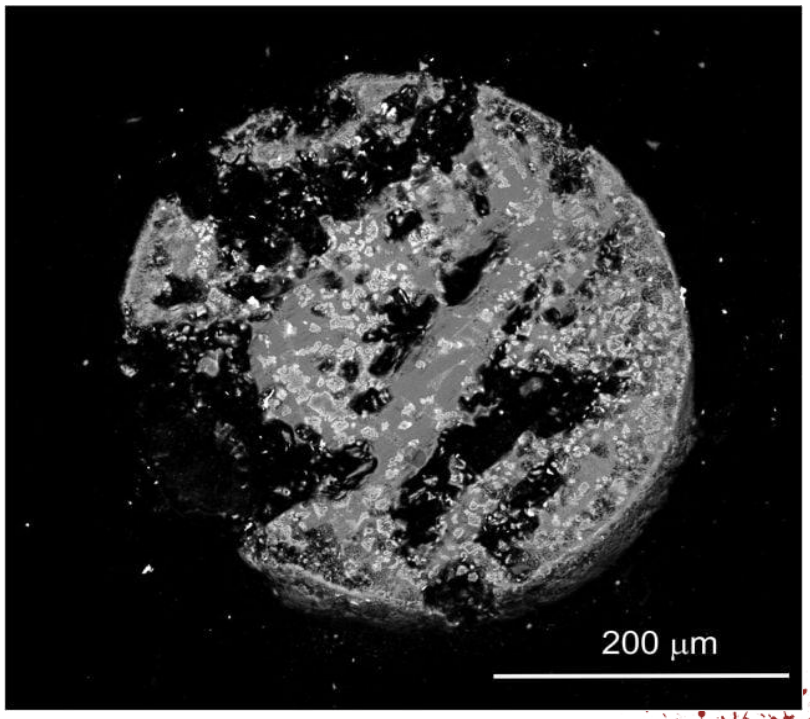
"In effect, it performs an enormous number of uncontrolled materials experiments at once, sampling combinations and structures that would take researchers years to explore deliberately in a laboratory."



The tiny spherule of hiroshimaite that contained the new alloy. (Bindi et al., *Sci. Adv.*, 2026)

The 15-kiloton blast when the bomb known as Little Boy detonated over Hiroshima left behind many scars. Some are well known, like the shadows of victims etched on stone and concrete; others are more subtle.

Among the latter are microscopic particles of fallout debris known as hiroshimaites – tiny globs of glassy material formed as vaporized and molten matter was scrambled together and rapidly cooled during the airburst event.

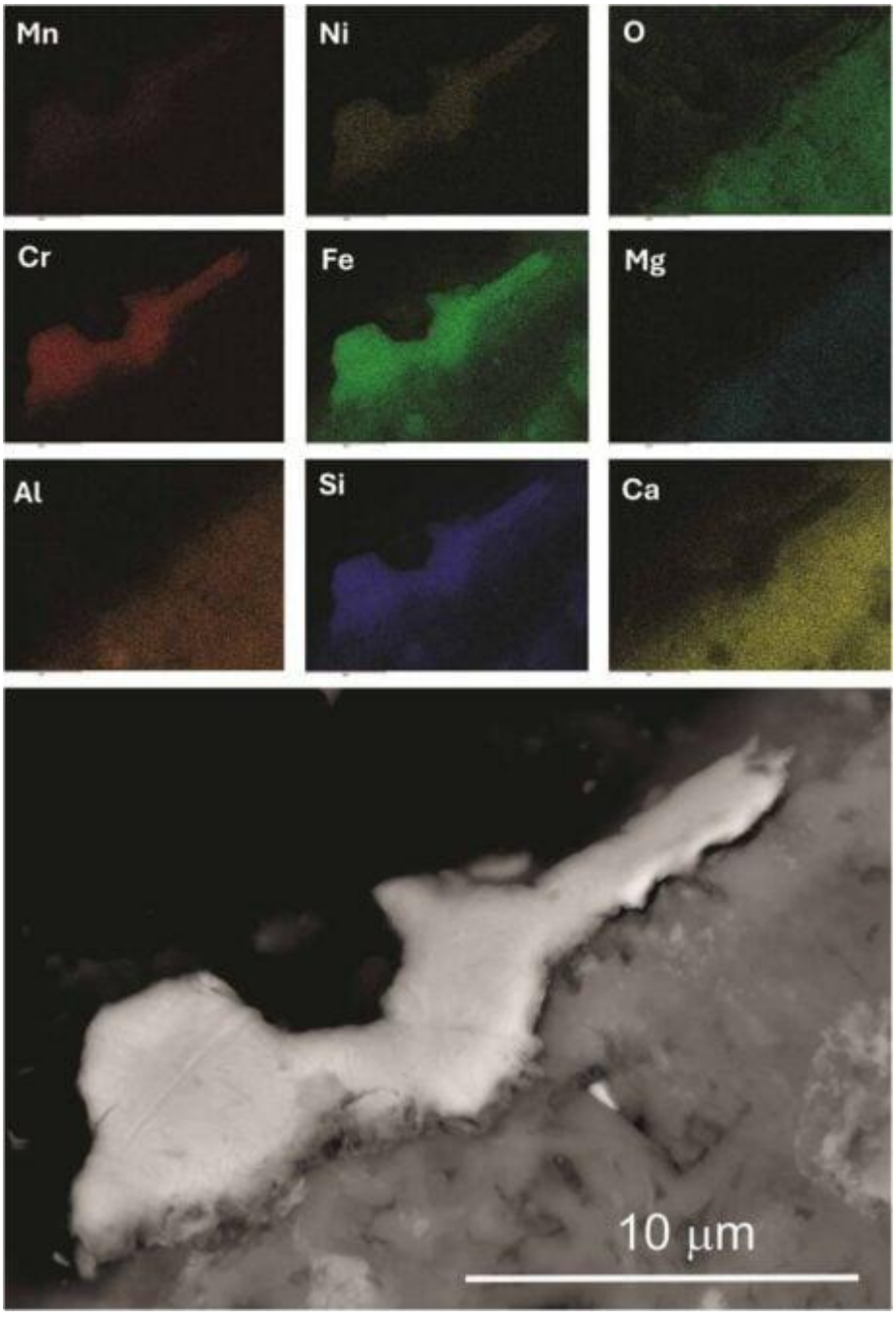


An SEM cross-section of the whole hiroshimaite spherule, with metallic material scattered through the glass. (Bindi et al., *Sci. Adv.*, 2026)

These particles contain a physical record of the fireball. Different materials were all swept up and mixed together in conditions and combinations that wouldn't normally occur, even under artificial manufacturing conditions.

"Metals, glass, soil, and building materials are vaporized and mixed at very high temperature, creating chemical combinations that would rarely occur under normal conditions," Bindi explained.

"As the fireball expands, the material condenses and cools so quickly that unusual atomic arrangements can be frozen in place before they transform into simpler, more stable structures."
Previous work had already demonstrated that Hiroshima fallout products contain unusual condensates that form under those extreme but fleeting temperature conditions.
Bindi and his colleagues were broadly searching for unusual metallic phases preserved in the fallout when they undertook a study of 34 samples of hiroshimaite, using a variety of high-resolution techniques to probe the microscopic composition and structure of each tiny glob.

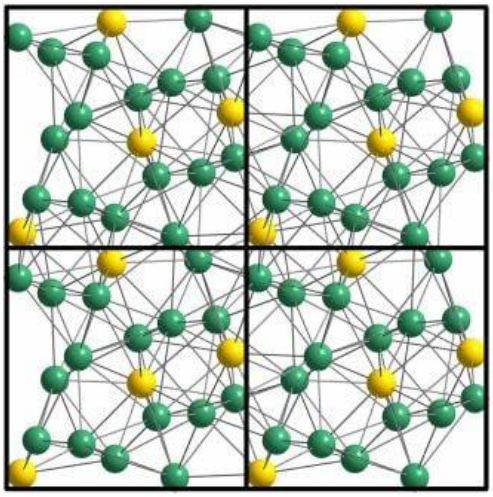


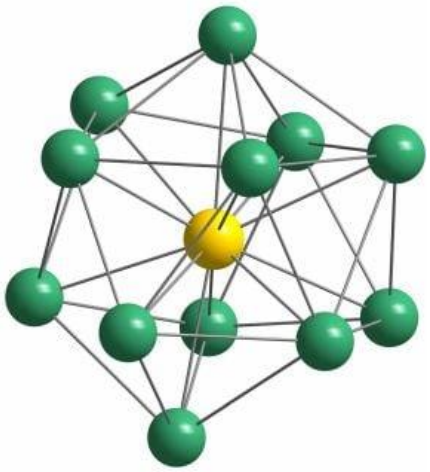
SEM X-ray maps of the elements in the grain. (Bindi et al., *Sci. Adv.*, 2026)

One of those samples proved particularly interesting. Embedded within its glassy matrix were numerous microscopic fragments of iron-chromium alloy.
Most of those metallic fragments were more or less as expected for the context.
But one stood out.
"The first clue came from the chemical analyses: one grain contained much more silicon than the surrounding Fe–Cr-rich metal particles," Bindi said.

The grain is only about 10 micrometers across and, as electron-microprobe analysis revealed, contains predominantly iron, plus chromium, silicon, nickel, molybdenum, manganese, and aluminum. But it wasn't just the mix of elements that made it so peculiar.
The researchers selected four grains for a much closer look – their tiny oddball, and three others about the same size. Using fine needles, they carefully extracted the grains by hand from the polished sample, then used a technique called single-crystal X-ray diffraction to determine the way the atoms were arranged inside each one.
The three comparison grains had the simple body-centered cubic structure expected for ordinary steel. The oddball did not. That was the decisive observation. "The

novelty," Bindi explained, "lies in that specific combination of chemistry and crystal structure, which does not match known industrial alloys or previously reported blast products."
An alloy isn't defined only by its ingredients; how those atoms are arranged matters too. Two materials containing broadly similar elements can have very different properties depending on their crystal structures. That's why the combination of chemistry and structure defined the new alloy's novelty.





The unexpectedly complex atomic structure of the new alloy. (Bindi et al., *Sci. Adv.*, 2026)

X-ray diffraction revealed that instead of the simple body-centered cubic arrangement found in the comparison grains, the atoms in the silicon-rich grain occupy a much more complex, highly ordered cubic arrangement called an $AlAu_4$-type structure, derived from the beta-manganese structure. The researchers believe that it formed under the intense conditions of the nuclear blast – it condensed from a metallic vapor and then cooled extraordinarily quickly. Under more normal circumstances, the condensed blob would form a simpler structure as it cooled more slowly. Instead, the alloy was trapped in a far more complicated configuration before it could relax into something more stable. And that might not be all that unusual for nuclear fallout. Earlier this year, another team led by Bindi revealed a never-before-seen clathrate in the debris of the Trinity test conducted in July 1945. "These discoveries suggest that historic blast debris may contain an entire population of rare metastable phases, many of them hidden in grains only a few micrometers across and therefore easy to overlook," Bindi said. That means the debris left in the ashes of nuclear explosions may contain a microscopic library of materials we don't yet know exist, forged under conditions so extreme and fleeting that they would be difficult to reproduce deliberately. But it is important not to forget how they were created – the profound poignancy of discovering a previously unknown material inside the debris of one of humanity's greatest tragedies.
"That tension is always present," Bindi said.
"Scientifically, the material is extraordinary, but it cannot be separated from the human catastrophe that created it; the work must therefore be approached with humility, respect and a clear awareness that scientific knowledge here comes from the remains of immense suffering."

●▶ **The findings have been published in** *Science Advances*.

Abstract

Background: In radiological emergencies with radionuclide incorporation, decorporation treatment is particularly effective if started early. Treating all people potentially contaminated ("urgent treatment") may require large antidote stockpiles. An efficacious way to reduce antidote requirements is by using radioactivity screening equipment. We analyzed the suitability of such equipment for triage purposes and determined the most efficient mix of screening units and antidote daily doses.

Methods: The committed effective doses corresponding to activities within the detection limits of monitoring portals and mobile whole-body counters were used to assess their usefulness as triage tools. To determine the optimal resource mix, we departed from a large-scale scenario (60,000 victims) and based on purchase prices of antidotes and screening equipment in Germany, we calculated efficiencies of different combinations of medical countermeasure resources by data envelopment analysis. Cost-effectiveness was expressed as the costs per life year saved and compared to risk reduction opportunities in other sectors of society as well as the values of a statistical life.

Results: Monitoring portals are adequate instruments for a sensitive triage after cesium-137 exposure with a high screening throughput. For the detection of americium-241 whole-body counters with a lower daily screening capacity per unit are needed. Assuming that 1% of the potentially contaminated patients actually need decorporation treatment, an efficient resource mix includes 6 monitoring portals and 25 mobile whole-body counters. The optimum mix depends on price discounts and in particular the fraction of victims actually needing treatment. The cost-effectiveness of preparedness for a " dirty bomb" attack is less than for common health care, but costs for a life year saved are less than for many risk-reduction interventions in the environmental sector.

Conclusion: To achieve economic efficiency a high daily screening capacity is of major importance to substantially decrease the required amount of antidote doses. Among the determinants of the number of equipment units needed, the fraction of the potentially contaminated victims that actually needs treatment is the most difficult to assess. Judging cost-effectiveness of the preparedness for "dirty bomb" attacks is an issue of principle that must be dealt with by political leaders.

Map Shows US Allies Hosting Nuclear Weapons as Feud Emerges in NATO Country

By Tom O'Connor | Deputy Editor, National Security and Foreign Policy
Source: https://www.newsweek.com/map-us-allies-hosting-nuclear-weapons-feud-poland-nato-12380619

Aug 29 – Only nine nations in the world are known to possess their own nuclear weapons programs, three of which—the United States, the United Kingdom and France—are members of the NATO alliance.

But five more NATO states host U.S. nuclear weapons on their soil in line with the bloc's nuclear sharing program, an arrangement developed in the 1950s in a bid to counter the Soviet Union's conventional military superiority in Europe in the event that the Cold War erupted into full-scale conflict.

Today, these countries include Belgium, Germany, Italy, the Netherlands and Turkey. Each maintains a stockpile of B61 gravity bombs that can be fitted to a variety of aircraft deployed among NATO members, including variants of the F-15, F-16 and F-35 fighter aircraft, as well as the European Panavia Tornado.

nd as European nations once again worry about potential escalation from Moscow as the Russia-Ukraine war enters a dangerous new phase, another NATO member, Poland, has entered into a fierce debate over whether or not to bring U.S. weapons of mass destruction onto its territory.

Following a meeting with Elbridge Colby, U.S. under secretary of defense for policy, on Thursday, Polish Deputy Defense Minister Pawel Zalewski was asked by reporters if Warsaw would seek to join the NATO nuclear sharing program. He responded, "No. I would like to say this very clearly and openly: Poland does not want nuclear warheads on its territory."

The comments, however, prompted a wave of criticism from figures aligned with President Karol Nawrocki, who leads the right-wing populist Law and Justice opposition party. On Friday, Nawrocki's International Policy Bureau chief, Marcin Przydacz, slammed Zalewski's remarks as "bizarre, absurd and completely inconsistent with what Poland has been saying so far and what the policy of the Polish state is."

"Poland also wants to have the presence of warheads on its territory," Przydacz said. "Today, there is no such infrastructure, but if we join the [nuclear-sharing] program, such infrastructure will have to be built."

Why Poland? Why Now?

Long overshadowed by traditional European powers such as France, Germany and the U.K., Poland has increasingly emerged as a military leader on the continent since becoming the first country to break with the communist Eastern Bloc in 1989, two years before the fall of the Soviet Union.

Poland now commands the third-largest army in NATO, behind only the U.S. and Turkey. It also devotes the largest share of its GDP to defense among allies, at 4.3 percent.

But Warsaw's impressive build-up has not left it immune to the spillover effects of the war in Ukraine, which Poland borders directly, along with Russia's Kaliningrad exclave and Moscow's ally, Belarus. Drones and missiles have crossed into Polish territory on several occasions since the beginning of the conflict in February 2022, most notably an incident last September in which Russia was blamed for the incursion of 19 drones onto Polish territory.

This year may prove even more precarious for Poland as the Kremlin looks to increase the pressure on NATO to counter slowing gains in Ukraine and Kyiv's costly campaign of long-range attacks against Russian gas infrastructure. Reports that Moscow may be planning to escalate in the form of a new mobilization or even operations on NATO soil were further fueled by a surprise visit by the CIA chief to the Russian capital earlier this week.

While Kremlin spokesperson Dmitry Peskov dismissed such speculation on Thursday as having "no basis in reality," officials in Warsaw remain on high alert. Foreign Minister and Deputy Prime Minister Radek Sikorski warned last month that Russia may pursue a "false flag operation" to justify direct action against a NATO member.

Some analysts argue the presence of U.S. nuclear weapons on Polish territory may fortify deterrence in light of growing tensions.

"Involving Poland in nuclear sharing would help convince Russia that the U.S. and NATO are seriously thinking about responding with nuclear weapons to nuclear attack on the Alliance's eastern flank," Artur Kacprzyk, an analyst at the Polish Institute of International Affairs' International Security Program, told *Newsweek*.

He argued that NATO's nuclear-sharing program's message of unity was undermined by the fact that no nations along the alliance's eastern flank directly across from Russia participated. Poland, in particular, he said, was "firmly in the crosshairs" of Russian Iskander short-range ballistic missile systems deployed to Kaliningrad and Belarus.

"Deploying nuclear weapons in Poland would be a particularly strong political signal from the U.S. and NATO, while also offering additional options for using U.S. nuclear bombs in Europe," Kacprzyk said. "When stationed closer to

Russia they could be to strike deeper and faster, with lesser warning time for Russian air defense."

At What Cost?

Among the primary reasons that Kacprzyk argued nuclear deterrence remained relevant even in an age of hybrid warfare tactics increasingly being attributed to Moscow was that "Russia relies on nuclear weapons as a cover for aggression," and has only "doubled down on nuclear intimidation" since the beginning of the war in Ukraine.

Yet the public rift that has recently emerged among senior Polish officials indicates a lack of consensus on how far the nation was willing to go to shore up its defense.

Lukasz Kulesa, deputy head of research at the Polish Institute of International Affairs, acknowledged that Poland's full entry into the NATO nuclear-sharing pact would inevitably have consequences.

"Of course, Russia would criticize such a move and present it as 'proof' of U.S. and NATO's aggressive intensions," Kulesa told *Newsweek*.

"Internally at NATO, some members states may question whether such forward deployment would not be too escalatory towards Russia, and whether it would be operationally justified," Kulesa said. "After all, it would bring U.S. nuclear weapons within the range of more Russian missiles."

That only five of the alliance's non-nuclear member states participate in the nuclear sharing arrangement speaks to its complexity. Canada and Greece previously participated but withdrew, while Denmark and Norway have explicitly opposed the deployment of nuclear weapons on their soil. Spain's 1982 entry into NATO prohibits nuclear weapons from being hosted on its territory, and France, which has its own arsenal, is the only NATO member that does not participate in the alliance's broader nuclear planning group.

Given the controversy surrounding the decision, a "less ambitious" and "less risky" option Kulesa identified would "involve certifying Polish F-35s and pilots for the nuclear mission but without the actual deployment on Polish soil," thus potentially constituting "a good compromise at this point."

But despite the debate playing out in Warsaw, he saw "broad support in Poland among the main political parties for joining 'directly' NATO's nuclear mission."

"The question seems to be more about what's feasible at this point—most importantly, what the Trump administration is willing to offer or agree to."

Would the United States use nuclear weapons against Iran?

By Murray Hunter

Source: https://www.thevibes.com/articles/opinion/126793/would-the-united-states-use-nuclear-weapons-against-iran

Sep 01 – Nuclear weapons have long stood as the ultimate deterrent in great-power relations, embodied in the doctrine of mutually assured destruction (MAD). The concept holds that any nuclear exchange between major powers would ensure the annihilation of both sides, making deliberate first use irrational.

The Doomsday Clock, maintained by the Bulletin of the Atomic Scientists, tracks how close humanity stands to catastrophe from nuclear risks and other existential threats.

Only once have nuclear weapons been employed in war by the United States against Japan in 1945.

The human and moral consequences of Hiroshima and Nagasaki were so severe that a powerful taboo against their use took hold, even as arsenals expanded dramatically during the Cold War.

That taboo has held through decades of conventional conflicts.

Nuclear options were never seriously contemplated in Korea, Vietnam, the Gulf Wars, or other U.S. military engagements. Yet recent discussion surrounding the ongoing U.S.-Iran conflict has revived speculation about tactical nuclear weapons.

The irony is absurd, where initial US and Israeli actions against Iran were framed in significant part as efforts to prevent Tehran from acquiring its own nuclear capability.

In an interview with podcaster Tucker Carlson, former National Counterterrorism Centre director and presidential counterterrorism adviser Joe Kent addressed the possibility directly.

Kent, who resigned earlier in 2026 over disagreements with the administration's Iran policy, argued that if Washington remains committed to removing Iran's leadership and compelling total surrender, conventional options are running short.

A full-scale ground invasion, he said, is "not feasible whatsoever" given Iran's size, terrain, and population.

Playing out the logic of regime change long enough, Kent claimed, leads relatively quickly to consideration of weapons of mass destruction.

Kent described a hypothetical limited nuclear strike against deeply buried uranium enrichment facilities in Iran's mountainous regions as one possible path under discussion in extreme scenarios. "We would be fools to think that this couldn't happen here, in this current scenario, especially as the [Trump] administration scrambles for a way out," Kent stated.

President Donald Trump has issued stark public warnings. In April, he declared that Iran's "whole civilisation will die" absent compliance with U.S. demands.

He has repeatedly spoken of the capacity to obliterate civilian infrastructure, such as power plants, bridges, and more.

Carlson and others have interpreted such language as implicitly raising the nuclear threshold, arguing that destruction of a civilisation on that scale would be difficult to achieve solely with conventional means.

Kent's remarks came against a backdrop of reported strains on US precision munitions and interceptor stockpiles after months of strikes. The administration has suspended certain waves of attacks, with media accounts citing depletion of high-end munitions.

Trump and senior officials have firmly denied shortages, insisting ample inventories remain.

In an apparent tactical shift, Trump recently announced a "crushing economic operation" against Iran, labelling it "Economic D-Day."

Treasury Secretary Scott Bessent followed with expansive new sanctions targeting nearly 60 entities, individuals, and vessels across jurisdictions, including many linked to China.

The stated goal is to render Iran an economic outcast by punishing any actors facilitating its financial networks or money laundering, with threats of removal from the US dollar system.

These developments illustrate the limits of pure military pressure. Iran's geography, air defences, dispersed and hardened facilities, and ability to retaliate through proxies, ballistic missiles, and disruption of the Strait of Hormuz have complicated efforts to force rapid political collapse from the air. Economic isolation seeks to achieve what bombing has not yet delivered. Yet the persistence of maximalist political aims, total surrender and leadership change keeps extreme military options theoretically on the table in some analysts' minds. Serious institutional, strategic, and normative barriers remain against nuclear first use. The United States maintains a vast conventional advantage and has historically treated nuclear weapons as a last resort for existential threats, not tools for regime change against a non-nuclear state.

Escalation risks are enormous: any nuclear employment could shatter the global non-proliferation regime, invite retaliation or proliferation by others, alienate allies, and produce long-term humanitarian and environmental catastrophe.

Domestic political costs would be severe. Even tactical or limited strikes against underground targets would cross a threshold unbroken

since 1945 and invite unpredictable second- and third-order effects.

Kent's comments and Trump's rhetoric highlight genuine frustration over stalled objectives and the high costs of prolonged conflict. They do not constitute official policy or an imminent decision. The administration's pivot toward intensified sanctions suggests a preference for non-nuclear leverage at present. Whether economic pressure can compel the desired political outcome remains uncertain. What is clear is that introducing nuclear weapons into the equation would represent a profound break with decades of restraint, one whose consequences would extend far beyond Iran and reshape international security for generations. The historical record and the logic of deterrence counsel extreme caution.

In contrast, the Russian State Duma International Affairs Committee Chairman Leonid Slutsky recently told Tucker Carlson that Moscow could have employed tactical nuclear weapons against Ukraine long ago to secure a decisive military victory, yet deliberately chose not to do so.

Speaking in late August 2026, Slutsky emphasised that Russia prioritizes minimizing civilian casualties and does not view nuclear arms as instruments of terror in the manner of the 1945 bombings of Hiroshima and Nagasaki.

Slutsky stated that such weapons would only be considered if Western powers supplied Ukraine with weapons of mass destruction, expressing hope that the situation would not reach that point.

This public assertion of self-imposed limits, coming from a senior Russian lawmaker, underscores how even nuclear-armed states engaged in high-stakes conventional wars have so far adhered to the post-1945 taboo against nuclear use, preferring other means despite the theoretical availability of the ultimate option.

Could US Nuclear Reactors Survive Military Hits in Saudi Arabia?

By Henry Sokolski

Source: https://nationalinterest.org/blog/middle-east-watch/could-us-nuclear-reactors-survive-military-hits-in-saudi-arabia

Sep 05 – Last Monday, Energy Secretary Chris Wright asked Congress to approve a US-Saudi civilian nuclear cooperative agreement. The clock is ticking. Ninety days hence, the United States could be exporting reactors to the Kingdom unless Congress objects to the deal. Before Congress approves such exports, though, it should examine why so few Russians are managing Iran's current nuclear energy operations. Once the war began in late February, Russia removed nearly all of its 600 staff from the Bushehr nuclear power plant. Last month, Russia cautiously increased its staff numbers, but

only to 42. Its wariness is not without cause.

On May 17, 2026, Iranian drones struck auxiliary diesel generators at the United Arab Emirates' Barakah nuclear power plant in Al Dhafra. Earlier, Iran claimed US-Israeli forces attacked in or near the Bushehr nuclear plant site four times. These strikes follow a pattern. From 1980 to 2007, Israel, the United States, Iran, and Iraq attacked reactor sites on at least 13 separate occasions. This year and last, the United States and Israel attacked Iran's nuclear fuel-making activities.

Given this history, Riyadh and Washington have to worry that nuclear facilities built in the Kingdom, which is now in a war zone, might also be hit. Saudi Arabia says it's planning to build at least one nuclear power plant, and industry experts still hope the Kingdom might build up to 16, including several small modular reactors. Riyadh is also intent on enriching uranium on its soil.

Yet, if history is any guide, all of these projects are potential military targets. Can they survive assault? It's unclear. Certain portions of the plants could be passively defended against drone attacks, much as the United Arab Emirates recently protected its major oil storage tanks with bird caging or metal "cope cages." Ukraine uses such caging to protect its large reactors against Russian drone attacks.

kraine has also hardened portions of its electrical supply system, which is essential to provide a steady supply of electricity to keep its reactors' cooling and safety systems running smoothly. This includes hardening key transformers and maintaining spare parts on hand to replace components that get hit. It has also created an electrical system repair corps to get Ukraine's power systems back up and running in a reasonable amount of time.

Ukraine, Iran, and Belarus employ active air defenses to reduce air-breathing missile threats to their nuclear plants. But none of these defenses can be counted upon to protect against ballistic missile strikes.

In the case of Westinghouse's AP-1000 reactor (which the Saudis may likely buy), the containment building and the reactor's separate spent fuel storage facility are hardened to 6,000 pounds per square inch. This is hard, but the storage facility could and should be hardened with ultra-high performance concrete, which can resist pressures up to 40,000 pounds per square inch. If the spent fuel storage building is hit and prompts a major radiological release, it could force the evacuation of hundreds of thousands or even millions of people. Such a catastrophe is conceivable: ballistic missiles with penetrating warheads can pierce concrete hardened to 30,000 pounds per square inch.

The US Research Council has also long recommended installing emergency spray water coolers within the storage pond buildings. This would prevent spent nuclear fuel fires that would otherwise occur if the storage pond is hit and consequently drained.

These are only some of the measures one might take to protect existing or planned nuclear power plants in Saudi Arabia. Ultimately, it is unclear if they will be enough to avoid the worst-case scenario—a major wartime radiological release.

So far, there has been little public discussion about how best to deal with these vulnerabilities. If the Kingdom weren't so sun-, gas-, and oil-soaked or didn't have as many geothermal prospects, building nuclear power would be imperative, even if it were risky. None of this, however, is the case, and Saudi nuclear plants also present obvious nuclear proliferation concerns.

Any serious review of the US-Saudi nuclear cooperative agreement would grapple with all of these issues. So far, our government hasn't; Congress should.

Henry Sokolski is the executive director of the Nonproliferation Policy Education Center and author of China, Russia and the Coming Cool War. He served as the deputy for nonproliferation policy at the Department of Defense from 1989 to 1993. Before that, he worked in the secretary of defense's Office of Net Assessment on strategic weapons proliferation issues.

Assad-era Syrian reactor was configured for nuclear weapons, IAEA chief says

By Stehanie Liechtenstein

Source: https://apnews.com/article/syria-nuclear-reactor-plutonium-weapons-0d72d8d543a1fe5218d21b6f13f9fbcb

Sep 07 — The Assad-era government in Syria was constructing a nuclear reactor that was configured to produce fissile material for possible use in nuclear weapons, the head of the International Atomic Energy Agency said on Monday. The "configuration" and the "technical features" of the nuclear reactor under construction in Syria during the leadership of ousted former President Bashar Assad were "very efficient in the production of fissile material that could be directly used for the fabrication of nuclear weapons," IAEA director general Rafael Grossi said.

"Of course, that was never declared, that was always denied, so, and again, intentions cannot be judged, but that was a very serious proliferation concern that we had, and this has been difficult work," he told reporters on the first day of a regular meeting of the IAEA Board of Governors, in Vienna.

Syria was believed to have operated an extensive undeclared nuclear program under Assad that included a nuclear reactor built by North Korea in eastern **Deir el-Zour province.**

Following Assad's ouster, the new government agreed to give IAEA inspectors access to suspected former nuclear sites. During a visit to Syria in August, IAEA inspectors confirmed that "the cooling infrastructure which has now been uncovered is consistent with that of a nuclear reactor." Grossi and a team of senior inspectors also visited a previously undeclared site in the country.

Inspectors had to 'tear down walls' to find hidden material

Syria notified the agency of the site's existence in a July 17 letter and invited the IAEA "to cooperate with the Syrian authorities in the inspection and verification of the site and of any nuclear material to be potentially found."

The IAEA said in its confidential report circulated to member states last Tuesday and seen by The Associated Press that this new site contained "natural uranium metal in the form of fuel rods with cladding." The agency verified the material and confirmed "**the presence of around 73 tonnes of natural uranium metal**." Grossi said when the inspectors visited the site in August they had to "tear down walls" and go through "very difficult and narrow passages" to reach the nuclear material that had been hidden. The site had "boxes scattered all over the place," he said. Grossi said that "the important thing is that this material now is under safeguards" of the IAEA, adding that agency inspectors had managed to install cameras at the location.

Syria to decide what happens next

Asked if the nuclear material will remain in Syria or be removed, Grossi said that this is "a matter that the Syrian government will have to decide." He added: "We are not requesting them to do this or to do that. For us what's important is that we know all the time where this (material) is until the last gram."

Logan Mintz, a director for nuclear materials security at the Washington-based Nuclear Threat Initiative, said that natural uranium metal is not directly usable for a nuclear weapon but it could be "diverted to a covert weapons program that further processes it into plutonium for a nuclear weapon." She said that once deemed safe to move, the material could be "transported in certified containers" to a third country

that can "safely and securely dispose it into a more chemically stable and more widely used form" for possible use in nuclear power plants.

"As with any transport of nuclear material, this movement would require robust security from theft or sabotage," she said.

World leaders are losing their terror of nuclear war

Sep 09 2026

Source: https://illuminem.com/illuminemvoices/summary-world-leaders-are-losing-their-terror-of-nuclear-war

➲ *Read the full piece on The Economist or enjoy below:*

Driving the news: In an editorial published 8 September, The Economist argues that world leaders are losing the fear of nuclear war that once restrained them, and that Putin, Trump and Xi — who control the world's most powerful arsenals — should take nuclear risk more seriously

- The argument is framed around the release of The Brink of War, a film marking the 40th anniversary of the Reykjavik summit between Ronald Reagan and Mikhail Gorbachev

The context: The piece draws on cold war precedent, arguing that shared dread of annihilation repeatedly pushed American and Soviet leaders toward restraint

What's next: New START expired on 5 February 2026, leaving the US and Russia without legally binding limits on strategic nuclear forces for the first time since the early 1970s

- Trump said the US would seek a "new, improved, and modernized" treaty, but no bilateral or multilateral negotiations are under way

- China's disarmament ambassador Shen Jian said Beijing will not join disarmament talks at this stage, maintaining that Washington and Moscow hold primary responsibility for cuts first
- US officials have signalled the country retains non-deployed capacity that could expand the arsenal

One quote: US arms control diplomacy should take "into account all Russian nuclear weapons, both novel and existing strategic systems, and address the breakout growth of Chinese nuclear weapons stockpiles" — Thomas DiNanno, US arms control official, February 2026

One stat: Russia holds an estimated 5,459 nuclear warheads and the United States 5,177, per ICAN — against the 1,550 deployed strategic warheads each that New START capped until its expiry

One stat: 60,000 nuclear warheads under the control of the two leaders meeting at Reykjavik in 1986.

Once, the fear of nuclear annihilation forced superpowers to exercise restraint. Today, the US, Russia and China seem increasingly willing to play with a threat that may leave NO winner.

Indian nuclear weapons, 2026

By Hans M. Kristensen, Matt Korda, Eliana Johns, and Mackenzie Knight-Boyle
Source: https://thebulletin.org/premium/2026-09/indian-nuclear-weapons-2026/

On April 3, 2026, India reportedly commissioned its third indigenously developed nuclear-powered ballistic missile submarine (SSBN), the INS *Aridhaman* (S4). It is noticeably longer and wider than India's first two SSBNs and is believed to be equipped with eight missile tubes—twice the number present on the *Arihant* (picture) and *Arighaat*. The fourth Arihant-class SSBN, INS *Arisudan* is scheduled for commissioning in 2027 and India is also developing its next generation of SSBNs—the S5 class. (Photo: Indian MoD; modified)

Sep 09 – India continues to modernize its nuclear weapons arsenal and operationalize its nascent triad. We estimate that India currently operates nine different nuclear-capable systems: two aircraft, six land-based ballistic missiles, and one sea-based ballistic missile. At least two more systems are in development and nearing completion and are to be fielded with the armed forces within one or a few years. We estimate that the operational forces can deliver over 160 nuclear warheads, with additional warheads having been produced for missiles in production, for a total inventory of up to 190 warheads.

Research methodology and confidence

The Indian government does not publish numbers about the size of its nuclear weapon stockpile. The analyses and estimates made in the Nuclear Notebook are therefore derived from analysis of 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.

Collecting and analyzing accurate information about India's nuclear forces is a more challenging effort than for many other nuclear-armed states. India has never disclosed the size of its nuclear stockpile, and Indian officials do not regularly comment on the capabilities of the country's nuclear arsenal. Although some official information can be derived from parliamentary inquiries, budget documents, government statements, and other sources, India generally maintains a culture of relative opacity regarding its nuclear arsenal. India has previously refused to divulge the costs of certain nuclear weapon programs, and in 2016, the Indian government added Strategic Forces Command to a list of security organizations exempt from India's Right to Information Act, thereby inhibiting journalists, researchers, and the public from getting access to critical information about India's nuclear arsenal (Government of India 2016; Sarkar 2021). In addition, in contrast to geopolitical competitors like China or Russia, the United States does not typically publish assessments of India's nuclear arsenal; one US Air Force publication that used to provide information has not been published since early 2021, and that version appeared to include information that was watered down and out of date.

While the Indian government rarely provides official statements about its nuclear arsenal, the Ministry of Defence's Defense Research and Development Organization (DRDO) often publishes informative details about the weapon systems that it is developing. These details can be found in monographs, monthly reports, and other publications. While these reports very rarely include details specifically about India's nuclear program, they sometimes offer data points about dual-capable delivery systems that can be leveraged for analysis.

In the absence of much official information from the Indian government and military and from Western governments, local news and media outlets tend to embellish details about the country's nuclear arsenal. For example, some outlets regularly claim that certain weapon systems are "nuclear-capable," despite a lack of any official evidence to that effect. Many news publications also tend to rely on anonymous "sources" for military information without indicating or providing evidence that these sources have actual familiarity with the systems that they are describing.

To that end, we prefer to rely on official sources and more cautious expert assessments—as well as commercially or freely-available satellite imagery—to analyze India's nuclear arsenal and, whenever possible, try to corroborate the credibility of any unofficial claims with multiple sources. Satellite imagery can be particularly useful in monitoring construction at military facilities, as well as identifying which types of missiles, vessels, or aircraft are present at bases. In certain cases, useful imagery about nuclear systems can also be obtained through social media posts—both from military and civilian accounts—and can be used in conjunction with satellite imagery for more concrete analysis.

Fissile material and warhead inventory estimates

India is one of only a handful of countries believed to be producing both highly enriched uranium (HEU) and weapons-grade plutonium. India's HEU production is

largely assumed to be focused on producing fuel for its growing number of nuclear-powered vessels and submarines (Frieß et al. 2024).

India's source of weapons-grade plutonium has been the aging 100-megawatt (MWt) Dhruva plutonium production reactor at the Bhabha Atomic Research Center complex near Mumbai, and until 2010 the CIRUS reactor at the same location. After more than a decade of delays, India's new 500-MWt Prototype Fast Breeder Reactor (PFBR) at the Indira Gandhi Center for Atomic Research near Kalpakkam reached first criticality in April 2026 (Department of Atomic Energy 2024, 2026). Fueled by a stockpile of reactor-grade plutonium separated from India's first-generation power reactors, the new reactor irradiates a "blanket" of uranium or thorium to produce Plutonium-239 and Uranium-233. If operated at 80% efficiency, the PFBR could hypothetically produce an estimated 140 kilograms of Plutonium-239 per year, sufficient for up to 35 nuclear warheads. Several more fast breeder reactors are planned, including two that are in pre-planning stage (FBR-1 and FBR-2) and will be located adjacent to the Prototype Fast Breeder Reactor at Kalpakkam (BHAVINI; Kumar 2018). If operated successfully, the breeder reactors could potentially increase significantly the amount of plutonium available for India's nuclear warhead stockpile.

Table 1. Indian nuclear forces, 2026.

Type / designation	No. of launchers	Year deployed	Range (km)[a]	Warheads xyield[b]	No. of warheads
Aircraft[c]	48[d]				48
Mirage 2000H	32	1985	1,850	1 × 12 kt bomb	. .
Jaguar IS	16	1981	1,600	1 × 12 kt bomb	. .
Land-based missiles	88				104[e]
Prithvi-II	24	2003	250[f]	1 × 12 kt	24
Agni-I	16	20078[g]	700+	1 × 10–40 kt	16
Agni-II	16	20119[h]	2,000+	1 × 10–40 kt	16
Agni-III	16	2018	3,200+	1 × 10–40 kt	16
Agni-IV	8	2022	3,500+	1 × 10–40 kt	8
Agni-V	8	2023	5,000+	(1–3 × 10–40 kt MIRV)[i]	24
Agni-P	. .	(2027)	1,000–2,000	(1 × 10–40 kt)[j]	. .
Sea-based missiles	1/12[k]				12
K-15 (B-05)	1/12[l]	2018	700	1 × 12 kt	12
K-4	(2/12)[m]	(2027)	3,500	1 × 10–40 kt	. .
Total stockpile	148				164
Other stored warheads					[26][n]
Total inventory	148				190

Table 1. Indian nuclear forces, 2026.

As of the beginning of 2026, the International Panel on Fissile Materials estimated India to have produced approximately 730 kilograms (plus or minus about 170 kilograms) of weapon-grade plutonium (International Panel on Fissile Material 2026). Assuming approximately 4 kilograms of plutonium per warhead, this would theoretically be sufficient for producing anywhere between 140 and 225 nuclear warheads. However, this calculation comes with some caveats due to several uncertainties. Most notably, given the uncertainty about what warhead designs India has produced (lower-yield fission-only weapons, boosted single-stage weapons, higher-yield thermonuclear-like weapons, or any combination of these designs), it is difficult to estimate how many nuclear warheads India could potentially produce in total. India's 1998 nuclear tests reliably validated a fission design, but the country's progress on boosted fission and thermonuclear weapon designs remains highly uncertain (Albright 1998; Levy 2015). Regardless of the warhead

designs, it is unlikely that India has used all its plutonium to produce warheads, and it may have kept some in reserve.
The size of India's nuclear stockpile also depends on the number and types of launchers that can deliver them, as it is unlikely that India would produce significantly more warheads than these systems can launch. Based on available public information about its nuclear-capable delivery force structure and strategy, we estimate that India may have produced around 190 nuclear warheads (see Table 1). This includes over 160 warheads for operational launchers as well as additional warheads for new missiles in production.

Nuclear doctrine

India's nuclear doctrine and strategy have historically been most focused on Pakistan, and recent border clashes are reminders that tensions between India and Pakistan constitute one of the most concerning nuclear hotspots on the planet. The two nuclear-armed countries engaged in open hostilities as recently as May 2025. After an attack by a militant group killed 26 people in Indian-administered Kashmir, hostilities escalated between the two countries (Mateen, Saini, and Singh 2026). India carried out "Operation Sindoor"—missile strikes against what it termed "terrorist infrastructure" sites in Pakistan that India claimed were involved in the militant attack. Pakistan's prime minister stated that India would "now have to pay the price," and claimed that Pakistan had shot down five Indian fighter jets. The incident escalated into the nuclear realm when it triggered a convening of Pakistan's National Command Authority, the body that oversees Pakistan's nuclear arsenal (*The Express Tribune* 2025). The scale and intensity of the action prompted some observers to call this the "worst clash in more than two decades" (Shahzad and Patel 2025). The clash followed another incident in November 2020 when Indian and Pakistani soldiers exchanged artillery and gunfire over the Line of Control, resulting in at least 22 deaths. Earlier, in February 2019, Indian fighters dropped bombs near the Pakistani town of Balakot in response to a suicide bombing conducted by a Pakistan-based militant group. In retaliation, Pakistani aircraft shot down and captured an Indian pilot before returning him a week later. The skirmish similarly prompted a convening of Pakistan's National Command Authority.
In March 2022, India accidentally launched what appeared to be a BrahMos conventional ground-launched cruise missile 124 kilometers into Pakistani territory, damaging civilian property. Pakistani officials subsequently claimed that India did not alert them using the high-level military hotline, and India did not even issue a public statement about the accident until two days later (Dawn 2022). In the absence of any de-escalation measures from India, Pakistan reportedly suspended all military and civilian aircraft for nearly six hours and placed frontline bases and strike aircraft on high alert (Sehgal 2022). If this same accidental launch had taken place during a period of heightened tensions, it is possible that the incident could have escalated into a very dangerous phase (Korda 2022). Similar incidents are likely in the future, so the risk of conflict escalation between India and Pakistan remains dangerously high.
While India's primary deterrence relationship historically has been with Pakistan, its fielding and additional development of much longer-range nuclear-capable missiles indicate that it is putting increased emphasis on its future strategic relationship with China. In November 2021, the then-Indian Chief of Defense Staff stated in a press conference that China had become India's biggest security threat (Sen 2021). Additionally, most of India's new Agni missiles have ranges that suggest China is their primary target. This posture is likely to have been reinforced after the 2017 Doklam standoff during which Chinese and Indian troops were placed on high alert over a dispute near the Bhutanese border. Tensions have remained high in subsequent years, particularly following another border skirmish in June 2020 that resulted in the deaths of both Chinese and Indian soldiers. Further casualties have been reported due to Chinese-Indian military skirmishes as recently as January 2021 (BBC 2021).

The expected expansion of India's nuclear forces, increasingly focused on a militarily superior China (in terms of both conventional and nuclear forces), will result in new capabilities being deployed over the next decade. This development could potentially also influence how India views the role of its nuclear weapons against Pakistan. For example, one analyst asserted in 2017 that "we may be witnessing what I call a 'decoupling' of Indian nuclear strategy between China and Pakistan. The force requirements India needs in order to credibly threaten assured retaliation against China may allow it to pursue more aggressive strategies—such as escalation dominance or a 'splendid first strike'—against Pakistan" (Narang 2017). (A so-called "splendid first strike" is an initial attack with nuclear weapons that completely disables the enemy's nuclear capability, ensuring that there will be no retaliation.) There have been no official indications that India has adopted such a strategy, however.

India has long adhered to a nuclear no-first-use policy that does not require the capability to conduct a disabling first strike. And deployment of a more mature, secure, sea-based retaliatory capability might reduce the pressure to keep land-based forces on higher alert.

The no-first-use policy was weakened somewhat by India's 2003 declaration that it could potentially use nuclear weapons in response to chemical or biological attacks; such employment would constitute nuclear first use, even if it were in retaliation. Moreover, amid the 2016 border skirmishes with Pakistan, India's then-defense minister Manohar Parrikar indicated that India should not "bind" itself to the no-first-use policy (Som 2016). The Indian government later explained that the minister's remarks represented his personal opinion, but the debate drew attention to the conditions under which India would consider using nuclear weapons. Some analysts warned that "India's NFU [no-first-use] policy is neither a stable nor a reliable predictor of how the Indian military and political leadership might actually use nuclear weapons" (Sundaram and Ramana 2018). In what seemed like a confirmation of that warning, current defense minister Rajnath Singh in August 2019 tweeted that "India has strictly adhered to this doctrine. What happens in the future depends on the circumstances" (R. Singh 2019). Despite such questions and inherent uncertainty about the conditions of India's NFU policy, it might have served to limit somewhat the scope and strategy of Indian nuclear forces for the first decades of its nuclear era.

Additionally, although India has long been thought to store its nuclear warheads separately from deployed launchers, some analysts have suggested that at least some nuclear bombs are co-located with aircraft on bases in underground bunkers for rapid mating if necessary, and that India might be moving toward "pre-mating" some warheads with ballistic missiles in canisters for a subsection of the missile force (Narang 2013). The term "pre-mating" appears to imply the warhead is not actually mated with the missile but in a near-complete status nearby so the warhead can be readied and mated on short notice if needed. Before mating, the warheads would have to be brought out from storage and prepared in a special handling facility. One potential but unconfirmed candidate for such a facility is located near Morki; another is located near Khoha.

No credible public reports confirm that India has mated warheads with land-based missiles under normal circumstances. The first canistered missile (Agni-V) is now thought to be operational, and the second one (Agni-P) is expected to become operational in a year or two. (A canistered missile is stored, transported, and launched directly from a hermetically sealed, protective container (canister) rather than being mounted exposed on an open launcher.) India's submarine fleet remains in its nascency but would have to deploy with warheads mated on the missiles to serve as a credible retaliatory capability.

Aircraft

Fighter-bombers were India's first and only nuclear strike force until 2003, when the Prithvi-II nuclear-capable ballistic missile was fielded. Despite considerable progress since then in building a diverse arsenal of land- and sea-based ballistic missiles,

aircraft continue to serve a prominent role as a flexible strike force in India's nuclear posture. We estimate that three or four squadrons of Mirage 2000H and Jaguar IS aircraft at a small number of bases are assigned nuclear strike missions against Pakistan and China.

The Mirage 2000H Vajra ("Divine Thunder"), which is likely India's primary nuclear strike aircraft, is deployed with the 1st, 7th, and possibly the 9th squadrons of the 40th Wing at Maharajpur (Gwalior) Air Force Station in northern Madhya Pradesh. We estimate that at least one or two of these squadrons have a secondary nuclear mission. Indian Mirage aircraft also occasionally operate from the Nal (Bikaner) Air Force Station in western Rajasthan, and other bases might potentially function as nuclear dispersal bases as well.

The Indian Mirage 2000H, which was originally supplied by France, is undergoing upgrades to extend its service life and enhance its capabilities to include new radar, avionics, and electronic warfare systems. India signed a $2.1 billion deal with French company Thales in 2011 to upgrade 51 Mirage 2000H aircraft to the Mirage 2000-5 standard. Although the modernization program was scheduled to be completed by the end of 2021, the program was significantly behind schedule, with only about half of the aircraft having been modernized by the expected deadline (Philip 2022). India does not have domestic manufacturing capability for the Mirage aircraft, and as French manufacturer Dassault Aviation ceased production of the aircraft, India will face difficulties in maintaining its fleet.

India's Air Force signed deals with France in 2020 and 2021 for a total of 40 Mirage 2000 aircraft that have been phased out of the French Air Force. India will use the scavenged parts to upkeep its existing Mirage squadrons (Yelwe 2024). India was also reportedly in discussions with Qatar for the purchase of 12 secondhand Mirage 2000-5 aircraft, which officials stated would be for flying operations, not spare parts (*Hindustan Times* 2024a). However, negotiations appear to have stalled in late 2024 over disagreement on pricing (Basu 2024).

The Indian Air Force also operates four squadrons of Jaguar IS/IB Shamsher ("Sword of Justice") aircraft at three bases (a fifth squadron flies the naval IM version). These include the 5th and 14th squadrons of the 7th Wing at Ambala Air Force Station in northwestern Haryana, the 16th and 27th squadrons of the 17th Wing at Gorakhpur Air Force Station in northeastern Uttar Pradesh, and the 6th and 224th squadrons of the 33rd Wing at Jamnagar Air Force Station in southwestern Gujarat. We estimate that one or two of the squadrons at Ambala and Gorakhpur (one at each base) might be assigned a secondary nuclear strike mission. Jaguar aircraft also occasionally operate from the Nal (Bikaner) Air Force Station in western Rajasthan. The Jaguar, designed jointly by France and Britain, was nuclear-capable when deployed by those countries.

The Indian Air Force has operated the Jaguar since the 1980s. Half of the Jaguars have received the so-called DARIN-III precision-attack and avionics upgrade since 2017 (Ministry of Defence 2017), but the upgrade of the second half of the inventory was scrapped in August 2019 due to its prohibitive cost and long timeline. In October 2019, India's Air Chief Marshal declared that the Indian Air Force's six Jaguar squadrons of approximately 108 fighters would begin retiring in early 2020 (Shukla 2019); however, this was pushed back, potentially to bring India closer to its goal of maintaining enough squadrons to simultaneously deter both Pakistan and China over the coming decade (Shukla 2021a). In 2023, the Indian Air Force outlined its plans for retiring the Jaguar starting in 2027–2028. Most recently, in March 2026, Indian officials reportedly outlined an updated plan to begin retiring the oldest Jaguars between 2028 and 2031. To assist in the transition, the Indian Air Force is considering life-extending the Mirage 2000 fleet. The aircraft, originally slated for retirement around 2035, may now operate until 2038 or later as new Rafale and Tejas aircraft enter service (J. Menon 2026).

India plans to replace the Jaguar in the conventional role with the indigenously produced Tejas Mark 2 (Mk-2) fighter jet currently under development (Kunde 2023). In the meantime, the Indian Ministry of Defense signed a deal with Hindustan

Aeronautics Limited (HAL) in September 2025 for 97 Tejas Mk1A Light Combat Aircraft (LCA) for the Indian Air Force (Charpentreau 2025).

In the nuclear role, the new French-produced Rafale could potentially replace the older Jaguar. India and France initially signed an agreement in 2016 for delivery of 36 Rafale aircraft (Ministry of Defence 2017). The order was considerably reduced from initial plans to buy 126 Rafales. The Rafale is used for the nuclear mission in the French Air Force, and India could potentially convert it to serve a similar role in the Indian Air Force and ultimately take over the air-based nuclear strike role in the future. The first Rafale (tail number RB-001) was formally handed over to India at a special ceremony in France in October 2019, and the full shipment of 36 aircraft was completed on schedule by April 2022 (Hindustan Times 2022). All 36 Rafales are outfitted with 13 "India-Specific Enhancements," which include new radars, cold-weather engine start-up devices, 10-hour flight data recorders, helmet-mounted display sights, and electronic warfare and friend-or-foe identification systems (Dominguez 2019).

The Rafales are being deployed in two equally sized squadrons of 18 fighters and four dual-seat trainers: one squadron (17th "Golden Arrows" Squadron) at Ambala Air Base Station, located only 220 kilometers from the Pakistani border, and the other squadron (101st "Falcons of Chamb and Akhnoor" Squadron) at Hasimara Air Force Station in West Bengal. New infrastructure developments to accommodate the planes are being constructed at both bases, and the Indian Air Force has reinstated the squadrons to active duty after they had both been decommissioned years earlier (Indian Air Force 2021). French manufacturer Dassault Aviation SA reportedly plans to construct a maintenance, repair, and overhaul (MRO) facility near the Noida International Airport in Jewar (Dassault Aviation 2024). The facility will allow India to locally manufacture future Rafale aircraft as part of Indian Prime Minister Narendra Modi's "Make In India" initiative. French engine manufacturer Safran SA also plans to build an MRO facility at Hyderabad for Rafale engines, which is expected to become operational in early 2027 (Safran 2025).

In February 2026, India's Defence Acquisition Council approved the purchase of an additional 114 Rafale fighters for the Indian Air Force, the majority of which will reportedly be manufactured in India (*Le Monde* 2026).

This followed an order in April 2025 of 26 Rafale Marine fighter jets from France to operate from India's INS *Vikrant* and INS *Vikramaditya* aircraft carriers. Deliveries will begin in 2029 and reportedly will be completed by 2030 (A. Menon 2025).

Land-based ballistic missiles

The Indian Army possesses six types of mobile land-based, nuclear-capable ballistic missiles that appear to be operational: the short-range Prithvi-II and Agni-I, the medium-range Agni-II, and the intermediate-range Agni-III, Agni-IV, and Agni V. At least one other Agni missile is in development and nearing deployment: the medium-range Agni-P. A future intercontinental-range Agni-VI missile is also rumored to be in the design stage, although its status is unclear.

It remains to be seen how many of these missile types India plans to keep in its enduring arsenal. Some may serve as technology development programs toward better or longer-range missiles. While the Indian government has made no statements about the future size or composition of its land-based missile force, it is possible that redundant missile types could potentially be discontinued or that only medium- and long-range missiles might be deployed in the future to provide a mix of strike options against Pakistan and China. Several of India's nuclear-capable ballistic missiles are thought to be dual-capable, meaning that each can deliver either a nuclear or conventional warhead. Unconfirmed reports have also hinted that India could reconfigure some of its nuclear medium-range ballistic missiles for conventional-only strike roles, though it is unclear if and when this may happen due to the lack of official information (Dubey 2023). In any case, the

government appears to be planning to field a diverse missile force and may have around 88 operational nuclear-capable land-based missiles as of July 2026.

The process for deploying Indian missiles is relatively opaque and uses some specific terms that are not used in other countries, which makes it more complex to piece together. Based on media reporting, press statements, and development timelines, the process appears to be as follows: Following the design and development of the missile by India's DRDO, missile systems undergo design and successive development trials, followed by pre-"induction" flight tests and night launches. This usually takes several years and is accomplished in collaboration with the Strategic Forces Command, which is part of India's Nuclear Command Authority and is responsible for operating and managing India's nuclear weapons. Then, after typically three to five trials to validate the missile's flight and technological systems, the missiles can be "inducted" into service, which means they are handed over to the armed forces. "Induction," however, does not mean the missiles are operational, as they require additional user trials to achieve operational deployment status.

The short-range Prithvi-II missile was India's first missile to be developed under the "Integrated Guided Missile Development Program" for nuclear deterrence, according to the Indian government (Press Information Bureau 2013). The missile can deliver a nuclear or conventional warhead to a range of 350 kilometers. Given the relatively small size of the Prithvi missile (9 meters long and 1 meter in diameter), the launcher is difficult to spot in satellite images, and little is known about its deployment locations. It is thought India has four Prithvi missile groups (222, 333, 444, and 555), of which an estimated 24 launchers may have a nuclear mission, although the precise number is highly uncertain. Potential locations include Jalandhar in Punjab, as well as Banar, Bikaner, and Jodhpur in Rajasthan. Following a training test-launch in 2023, the Indian Ministry of Defense described the Prithvi-II as a "well-established system" and publicly confirmed that the Prithvi-II missile "has been an integral part of India's nuclear deterrence" (Government of India 2023).

The two-stage, solid-fuel, road-mobile Agni-I missile became operational in 2007, three years after its induction into the armed forces. The short-range missile can deliver a nuclear or conventional warhead approximately 700 kilometers. The mission of Agni-I is thought to be focused on targeting Pakistan; we estimate that around 16 launchers are deployed in western India, possibly including the 334th Missile Group. Satellite imagery from September 2023 appears to show two Agni-I transporters at a garrison near Jodhpur, although it is unclear whether this is a temporary visit or semi-permanent deployment. In July 2025, India conducted a combined test-launch of the Prithvi-II and Agni-I missiles. The tests were "conducted under the aegis of the Strategic Forces Command," which is responsible for operating India's nuclear missiles (Government of India 2025b). The most recent Agni-I test-launch was conducted in May 2026 from the Integrated Test Range on Abdul Kalam Island (Government of India 2026c).

The two-stage, solid-fuel, rail-mobile Agni-II—an improvement on the Agni-I—can deliver a nuclear or conventional warhead more than 2,000 kilometers. The missile was probably "inducted" into the armed forces in 2008, but technical issues delayed its operational capability until 2011. Around 16 launchers are thought to be deployed in northern India, possibly including the 335th Missile Group. Targeting is probably focused on Pakistan and western, central, and southern China. Agni-II has not been test-launched since 2019, suggesting that the missile may have encountered technical problems or is being replaced with a newer Agni type.

The Agni-III—a two-stage, solid-fuel, rail-mobile, intermediate-range ballistic missile—can deliver a nuclear warhead over 3,200 kilometers. Following its first failed night trial in 2019, India successfully conducted a second night trial on November 23, 2022 (Rout 2022). Agni-III was most recently test-launched on February 6, 2026, which was "carried out under the aegis of the Strategic Forces Command" (Government of India 2026b). We estimate that India has deployed around 16 Agni-III launchers. The Agni-III's longer range makes it the first missile to

potentially bring Beijing within range of Indian nuclear weapons and also allows India to deploy missile units farther from the Pakistani and Chinese borders.

India has also deployed the Agni-IV missile—a two-stage, solid-fuel, road-and rail-mobile intermediate-range ballistic missile with the capability to deliver a single nuclear warhead over 3,500 kilometers (Ministry of Defence 2014). Following its final development test in 2014, the Strategic Forces Command has since conducted four user launches, the most recent taking place in September 2024 "under the aegis of the Strategic Forces Command" (Government of India 2024b). A model of the Agni-IV is displayed outside the Vehicle and Research Development Establishment (VRDE) south of Ahilyanagar in Maharashtra state (see Figure 1).

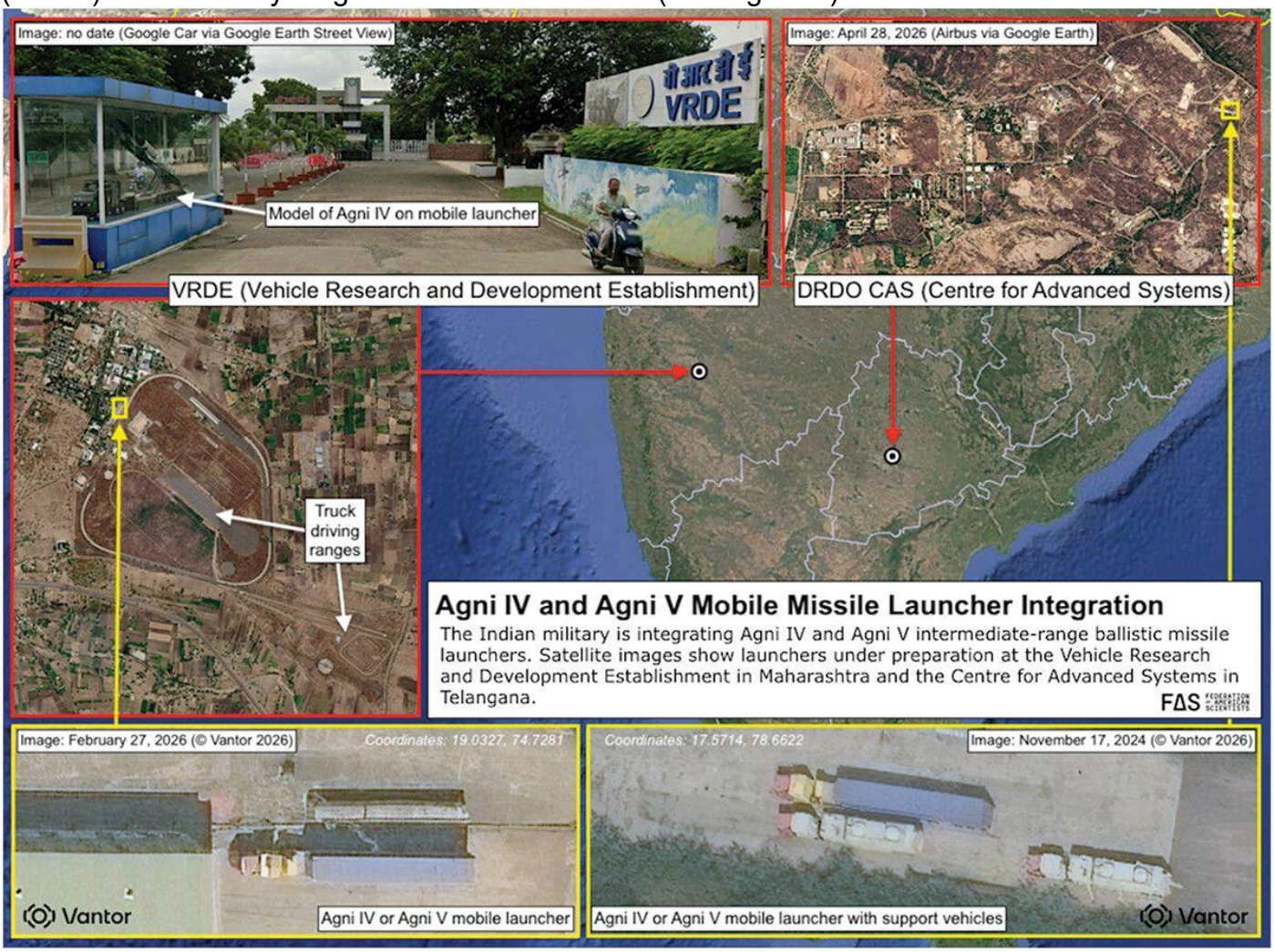


Figure 1. Agni IV and Agni V mobile missile launcher integration. (Images: Vantor and Google Earth; Annotations: Federation of American Scientists).

Although the Agni-IV is capable of striking targets in nearly all of China from locations in northeastern India, the Strategic Forces Command is also in the process of deploying the longer-range Agni-V—a three-stage, solid-fuel, road-mobile, intermediate-range ballistic missile capable of delivering multiple warheads (MIRVs) less than 6,000 kilometers. The extra range will allow the Indian military to establish Agni-V bases in central and southern India, further away from the Chinese border. Agni-V has been flight-tested the last three years in a row, most recently on May 8, 2026.

The Agni-V missile brings another important new capability to the Indian strike force. Since the missile is carried in a sealed canister on the launcher, the warhead can potentially be permanently mated with the missile, instead of having to be installed

before launch (Korda and Kristensen 2021). Whether India chooses to deploy nuclear warheads on the missile under normal circumstances remains to be seen; and there is no credible public information that it does so today. The first two test-launches used a rail launcher, but since 2015, all launches have been conducted from a road-mobile launcher. The launcher, which is known as the Transport-cum-Tilting vehicle-5 (TCT-5), is a 140-ton, 30-meter, 7-axle trailer pulled by a 3-axle Volvo truck (DRDO Newsletter 2014). The canister design "will reduce the reaction time drastically … just a few minutes from 'stop-to-launch,'" the former head of India's Defence Research and Development Organization said in 2013 (*Times of India* 2013). Several Agni-V transporter erector launchers (TELs) are clearly visible at various points in time on commercial satellite imagery of DRDO's integration center north of Hyderabad, as well as at other sites (see Figure 1).

In 2021, India conducted the first test-launches of its two-stage, solid-fuel, Agni-P ballistic missile with a range between 1,000 and 2,000 kilometers, which the Indian Government refers to as a "new generation" nuclear-capable ballistic missile (Government of India 2021b). Although its demonstrated range places it in the category of a medium-range (1,000–3,000 kilometers) missile, the official press release after its latest test described it as "intermediate range" (typically understood to be 3,000–5,500 kilometers) (Government of India 2025a).

The Agni-P is India's first shorter-range ballistic missile to incorporate more sophisticated rocket motors, propellants, avionics packages, and navigation systems found in India's newer, longer-range missiles like the Agni-IV and Agni-V. Importantly, the Agni-P is also carried in a sealed canister, similarly to the Agni-V (Korda and Kristensen 2021). One senior DRDO official remarked during the early stages of the Agni-P's development that, "As our ballistic missiles grew in range, our technology grew in sophistication. Now the early, short-range missiles, which incorporate older technologies, will be replaced by missiles with more advanced technologies. Call it backward integration of technology" (Shukla 2016). Statements like these, coupled with the Agni-P's clear capability upgrade over the early Agni-I and Agni-II missiles—which utilize older and less robust propellants, airframes, and hydraulic actuators, as well as less accurate guidance systems—suggest that the Agni-P might replace the older missiles once it becomes operational (Shukla 2021b). The Agni-P's second pre-induction night trial was successfully conducted in April 2024 (*The Economic Times* 2024), with its latest test taking place in September 2025 from a specially configured rail launcher.

India is also developing a conventional short-range ballistic missile (SRBM) known as the Pralay that is reportedly intended to take over the conventional role currently occupied by the dual-capable Prithvi-II and Agni-I SRBMs (Government of India 2021a; Unnithan 2021). If the nuclear and conventional short-range missions are split between the new Agni-P and Pralay missiles, respectively, that could help reduce the risk of misunderstanding in a conflict caused by mixing nuclear and conventional capabilities on the same platform. This could be further bolstered by the fact that the new Agni-P will likely be operated by Strategic Forces Command while the Pralay will be operated by the Indian Army's artillery corps (Philip 2021).

For two decades, it has been rumored that India was developing the ability to deliver multiple independently targetable reentry vehicles (MIRVs) on ballistic missiles. Finally, in March 2024, the Indian government announced that it had conducted the first flight test of its Agni-V ballistic missile "with Multiple Independently Targetable Re-Entry Vehicle (MIRV) technology" under what it called "Mission Divyastra" (Government of India 2024a). Another MIRV test—likely using an Agni-V—was conducted in May 2026, with the press release noting that "the missile was flight-tested with multiple payloads, targeted to targets spatially distributed over a large geographical area in the Indian Ocean Region" (Government of India 2026a).

While additional flight tests are likely needed before the Agni-V's MIRV capability becomes fully operational, this initial test already marks significant technical progress and represents a notable change in India's nuclear capabilities (Kristensen and Korda

2024). However, loading multiple warheads on the Agni-V would likely reduce its extended range, which was a key driver behind the missile's initial development. The Agni-V is estimated to be capable of delivering a payload of 1.5 tons (the same as the Agni-III and -IV), and India's first- and second-generation warheads—even the modified versions—are thought to be relatively heavy compared with warheads developed by other nuclear-armed states that also deploy MIRVs. As a result, we estimate Agni-V might only carry a small number of warheads, likely no more than three. The Agni-P was also rumored to have been tested with maneuverable decoys in 2021 to simulate MIRV technology (Korda and Kristensen 2021). Reportedly, the Agni-P can also be equipped with a Maneuverable Reentry Vehicle (MaRV), though there has been no official confirmation of this capability (Desai 2022; Thakur 2024). Equipping a medium-range ballistic missile with nuclear MIRV technology would be odd from a strategic and operational standpoint; we therefore assume the 2021 test was intended to further advance India's development of MIRV technology and decoys, rather than developing the capability to launch MIRVs from this specific system.

Deploying missiles with multiple warheads also invites questions about the credibility of India's minimum deterrent doctrine. In other countries, MIRV technology was developed to increase the number of targets that can be attacked, overwhelm missile defenses, or both. Deploying MIRVs would reflect a strategy to swiftly strike multiple targets simultaneously and, as a result, signal an intention to quickly increase the size of the nuclear arsenal. In turn, it could potentially incite Pakistan and China to further increase their own arsenals. Unless China develops an effective missile defense system with capability against intermediate-range ballistic missiles, there seems to be little military need for nuclear MIRVs on Indian missiles (Kristensen 2013). It seems likely, however, that China's deployment of MIRVs on some of its ICBMs and Pakistan's development of the new Ababeel medium-range ballistic missile with MIRVs have increased support in India to also develop a MIRV capability, if for no other reason than to avoid falling behind in technological capability.

A few years ago, Ministry of Defense officials indicated that India's strategic missile force will be "capped for the present with the Agni-V, with no successor or next series on the horizon or even on the drawing board" (Gupta 2018). However, India is rumored to have begun development of a new ICBM, known as Agni-VI. Official data on this missile is scarce, but an article posted on the government's Press Information Bureau website in December 2016 claimed the Agni-VI "will have a strike-range of 8,000–10,000 kilometers" and will "be capable of being launched from submarines as well as from land" (Ghosh 2016). The US Air Force's National Air and Space Intelligence Center estimates its range to be closer to 6,000 kilometers (National Air and Space Intelligence Center 2020). The development of an Agni-VI missile with a range of 8,000–10,000 kilometers—if confirmed—would be particularly controversial because it would extend well beyond potential regional targets in Pakistan and China. In 2023, a scientist who had previously worked at the DRDO reportedly claimed that the Agni-VI's indigenously designed launcher had already undergone a successful test. However, the claim was revealed during the scientist's trial on charges of espionage and should be treated with caution (Inamdar and Joshi 2023).

In addition, India is thought to be developing a land-based version of the short-range K-15 submarine-launched ballistic missile (SLBM), known as the Shaurya. Due to the high level of uncertainty regarding this system, it is not included in our stockpile estimates.

Rail-based missiles

Like other countries seeking to enhance their land-based second-strike options, India is increasingly prioritizing the development of a rail-based missile launch capability. India has an extensive rail network across the entire country, allowing it to transport personnel, materiel, and launch systems relatively quickly and with few visual signatures.

India's rail-based missile infrastructure appears to be concentrated at a small number of installations, including the Integrated Test Range on Abdul Kalam Island, the

DRDO's Integration Center in Panagarh, and at least two operational garrisons at Pune and Missa. The Integrated Test Range in Odisha State is India's primary complex for testing and evaluating missile launch performance. It features multiple launch pads and telemetry stations, as well as a rail-based launch pad with a retractable cover. In September 2025, this facility was used for India's first rail-based test launch of its new Agni-P ballistic missile (Dewey, Wiley, and Dempsey 2026; Government of India 2025a).

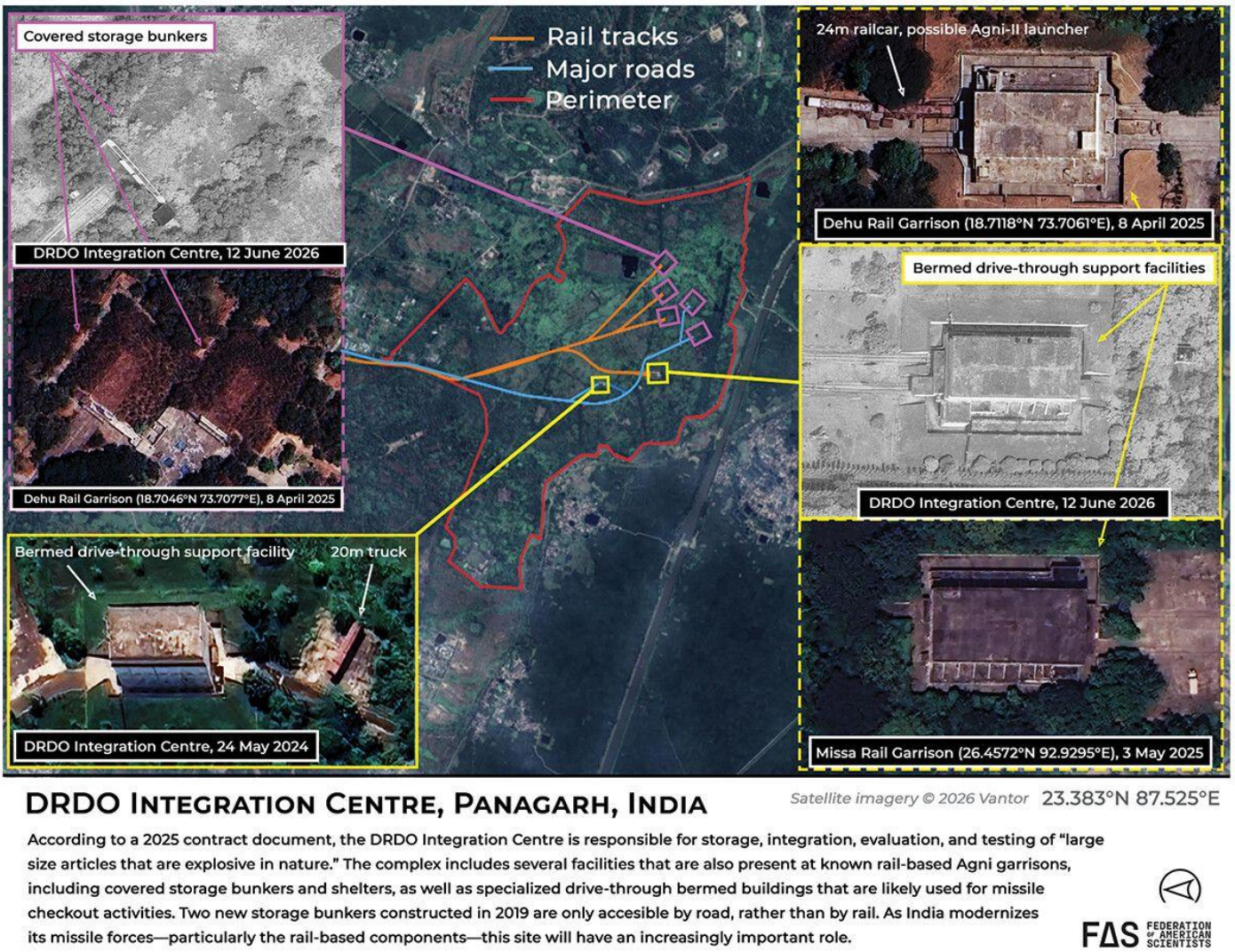


Figure 2. DRDO Integration Centre, Panagarh, India. (Images: Vantor; Annotations: Federation of American Scientists).

As described in a June 2025 DRDO contract document, DRDO's Integration Center "is responsible for integration, storage and testing of large size articles that are explosive in nature" (DRDO 2025). The complex features one northern rail-based entrance/exit and a 300-meter-long section of covered track leading to a high-bay support facility and three covered bunkers. The high-bay facility sits within an earth-bermed enclosure, is identical to a facility located at the Missa garrison, and bears strong similarities to facilities located at the Dehu garrison and at the Integrated Testing Range on Abdul Kalam Island. Rather than functioning as a deployment garrison, DRDO's Integration Center is likely being used for testing, evaluation, and storage of delivery systems.

Nuclear warheads are unlikely to be stored on-site as it would not fit the mission of the complex, nor is there any infrastructure that would typically be associated with nuclear storage. New construction has taken place just outside the complex's

perimeter since 2024, but it remains unclear what the purposes of these new facilities will be; while it appears to be military-related, it does not appear to be connected to the other rail-based infrastructure at the complex. Unlike the Integrated Test Range and India's two suspected rail-based deployment sites, there do not appear to be any launch pads present at the DRDO Integration Center (see Figure 2).

India has at least two rail-based missile garrisons: one at Dehu in Pune district, and another at Missa in Nagaon district (Dewey, Wiley, and Dempsey 2026). Both garrisons include several common facilities, such as drive-through high-bay buildings, likely missile checkout facilities, storage facilities, and rail-based entrances/exits connecting them to the country's broader rail network. The Dehu garrison includes retractable shelters like those found at the Integrated Testing Range, while the Missa garrison includes covered bunkers identical to those found at the DRDO's Integration Center. The Dehu site also includes two facilities with internal perimeters and guard towers that could be used for warhead storage. The Missa site does not include such facilities; however, a secure complex is located only 7 kilometers southeast, and shares similarities with other suspected munitions storage sites across the country.

India has deployed a rail-based missile system—the Agni-II—since 2008. The two-stage, solid-propellant Agni-II can deliver a nuclear or conventional warhead more than 2,000 kilometers. We estimate that around 16 Agni-II launchers are deployed in northern India, possibly including the 335th Missile Group, as well as at one or both garrisons.

India has also developed a longer-range rail-mobile weapon system—the Agni-III—that can deliver a nuclear warhead over 3,200 kilometers. We estimate around 16 Agni-III launchers are deployed, including at one or both of India's two rail-based missile garrisons.

India's new Agni-P also has a rail-based launch capability. Its latest launch took place on September 24, 2025, using a rail-based launcher for the first time. The official press release noted that the Agni-P had been inducted into the Strategic Forces Command, although it did not say when this took place (Government of India 2025). It also noted that the missile's "specially designed rail-based mobile launcher" can travel on the country's rail network "without any pre-conditions," likely meaning that India would not need to modify the rail track to allow the launchers to travel on it (Government of India 2025).

Sea-based ballistic missiles

For years, India's only sea-based nuclear capability was the Dhanush ballistic missile, a variant of its short-range Prithvi-II ballistic missile design. After entering service in 2010, these missiles could be launched from the back of two specially configured Sukanya-class patrol vessels (P51 *Subhadra* and P52 *Suvarna)* with onboard flame diverters so that launches would not damage the ships. Given their relatively short ranges and liquid-fuel designs—meaning that they would need to be fueled immediately before launch—the Dhanush's utility as a strategic deterrence weapon was severely limited. The ships carrying these missiles would have to sail dangerously close to the Pakistani or Chinese coasts to target facilities in those countries, making them vulnerable to counterattack. The two Sukanya-class ships are homeported at the Karwar naval base on the Indian west coast. Both the *Subhadra* and *Suvarna* have been pictured making international port visits with their missile stabilizer platforms removed, and satellite imagery indicates that the platforms had not been reinstated as of July 2024. Given that no test-launch has been publicly confirmed since 2018 and the missile has not appeared in official Indian Navy announcements since 2019, we assess that the Dhanush is no longer operational with the Indian Navy.

India's first indigenous nuclear-powered ballistic missile submarine (SSBN), the INS *Arihant*, was commissioned in August 2016 but spent most of 2017 and the first half of 2018 undergoing repairs after its propulsion system was crippled by water damage (Peri and Joseph 2018). In November 2018, Prime Minister Modi announced that INS

Arihant had completed its first deterrence patrol, officially marking the operational beginning of India's nascent nuclear triad. He additionally stated that the deployment constituted "a fitting response to those who indulge in nuclear blackmail" (R. Singh 2018). The "deterrence patrol" lasted approximately 20 days, and the phrasing would imply that nuclear weapons may have been carried onboard during the patrol; however, this cannot be confirmed through open sources. The INS *Arihant* will likely primarily serve as a training vessel and technology demonstrator (Gady 2018). The submarine was most recently used as a test launch platform in October 2022, when it launched an unnamed SLBM in a "user training launch" (Ministry of Defence 2022).

A second SSBN, the INS *Arighaat*, was launched on November 19, 2017, and was expected to be commissioned into the Indian Navy in 2020 (Pubby 2020). However, the *Arighaat* did not begin sea trials until the beginning of 2022 and was commissioned into service on August 29, 2024 (Janes 2024; Ministry of Defence 2024). Satellite imagery indicates that both the *Arihant* and the *Arighaat* possess four missile tubes and appear to have identical dimensions.

Table 2. Indian nuclear ballistic missile submarine fleet.

Hull name	Designation/ hull number	Launched	Sea trials	Commissioned	Armament	Length (meters)
INS *Arihant*	S2 / SSBN-80	2009	2014	2016	12 K-15	~111
INS *Arighaat*	S3 / SSBN-81	2017	~2021	2024	4 K-4	~111
INS *Aridhaman*	S4 / SSBN-82	2021	2024	2026	8 K-4	~130
INS *Arisudan* (proposed)	S4*/SSBN-83	2024	2025	Expected 2027	K-4/K-5	~130
?	S5	?	?	Expected 2030s	K-6?	?

Abbreviations used: INS: Indian Naval Ship; SSBN: nuclear-powered ballistic missile submarine.
Notes: Question marks (?) indicate the information is unknown or uncertain; Tilde (~) signs indicate the value is approximate.

Table 2. Indian nuclear ballistic missile submarine fleet.

The *Arighaat* is followed by two more SSBNs of the same class, the INS *Aridhaman* and INS *Arisudan* (this is a proposed name for the S4*/SSBN-83 hull) (see Table 2). Both boats were scheduled to enter service before 2024, but experienced delays (Pubby 2020). The first of these, the INS *Aridhaman*, was launched in November 2021, entered sea trials in 2024, and was commissioned on April 3, 2026 (Dutta 2026). It is noticeably longer and wider than India's first two SSBNs (Biggers 2021). Satellite imagery indicates that the S4 is approximately 18 meters longer than the first two SSBNs and equipped with eight missile tubes—twice the number present on the *Arihant* and *Arighaat* (see Figure 3). The INS *Arisudan* will likely be a similar design to the *Aridhaman* and is scheduled for commissioning in 2027 (Gupta 2026).

India is also developing its next generation of SSBNs—the S5 class. A series of tweets by the Indian vice president during his visit to the country's Naval Science & Technology Laboratory revealed some details about what this new class of submarines might look like (Vice President of India 2019). Photos indicate that the new submarines will be significantly larger than the current *Arihant*-class and could have 12 or more launch tubes (Sutton 2019). This new class of submarines could begin production after the completion of all four *Arihant*-class boats in the late 2020s, and a large new shipbuilding hall is currently under construction at Visakhapatnam—potentially to accommodate this new project.

To arm its SSBNs, India has developed one nuclear-capable sea-launched ballistic missile and is working on another: the current K-15 (also known as Sagarika or B-05) submarine-launched ballistic missile (SLBM) with a range of 700 kilometers, and the K-4 SLBM with a range of about 3,500 kilometers. The relatively short range of the K-15 would not allow the SSBNs to target Islamabad—only southern Pakistan—and the submarines would not be able to target China at all unless they sailed through the Singapore Strait, deep into the South

China Sea. Therefore, despite its induction in the summer of 2018, the K-15 should be seen primarily as an intermediate program intended to develop the technology for more capable future missiles.

Figure 3. India's temporary SSBN base at Visakhapatnam. (Images: Vantor; Annotations: Federation of American Scientists).

The K-4, which reportedly has characteristics like the Agni-III intermediate-range ballistic missile, has undergone at least 10 test launches, the most recent reportedly taking place in December 2025 from the INS *Arighaat* (Indo-Pacific Defense Forum 2026). A 2015 launch video of the K-4 SLBM indicated that rather than the cold launch system typically used by most SLBMs—through which the missile gets ejected from the launch tube via a gas generator—the K-4 in that test used two small motors on the front end of the missile to pull it several meters above the surface of the water before the main engine ignites (DRDO 2015). The fully developed missile will likely use a cold launch system. The missile appears to be ready for serial production, and there are reports that it has been inducted into service with the *Arihant*-class, but there is no official confirmation that the K-4 has been operationally deployed (Army Recognition 2025; Pandit 2023). Rumors about the K-4 claim that it is highly accurate, reaching "near zero circular error probability," according to the DRDO (Panda 2016), and one official reportedly claimed: "Our Circular Error Probability is much more sophisticated than Chinese missiles" (Peri 2020). Such claims, however, should probably be taken with a grain of salt. With a range of 3,500 kilometers, the K-4 will be able to target all of Pakistan and most of China from the northern Bay of Bengal. The K-15 has only been test-launched from the first SSBN and will likely be phased out when the K-4 comes online. As is usual with Indian nuclear programs in the absence of official statements, rumors and speculation posit that each K-4 SLBM will be capable of carrying more than one warhead, but it seems more likely that it will carry one warhead with penetration decoys and that real MIRV capacity might appear on a later missile.

Senior Indian defense officials have stated that the DRDO is reportedly planning to develop a 5,000-kilometer range SLBM that matches the design of the land-based Agni-V and would allow Indian submarines to target all of Asia, parts of Africa, Europe, and the Indo-Pacific region, including the South China Sea. The missile will reportedly be called the K-5 and was initially expected to be tested sometime in 2022 (Gupta 2020), although as of July 2026 no such launch had still taken place. However, in June 2025, a former BrahMos Aerospace scientist stated during a panel discussion that the development of the K-5 was complete and the DRDO was moving forward with development of a follow-on K-6 missile (Army Recognition 2025). This claim was followed by a reported second-stage propulsion motor test in September 2025, and a cold-launch ejection test in March 2026, both of which are milestones for pre-flight development (Indian Defense Research Wing 2025; Unnitahn 2026).

A naval base for the SSBNs, named INS *Varsha*, is currently under construction near Rambilli on the Indian east coast—only 50 kilometers south of the Visakhapatnam shipyard where India builds its submarines. It will be located near a facility under construction that is associated with the Bhabha Atomic Research Centre—India's primary nuclear research institution, which is also tied to its nuclear weapons program. INS *Varsha* is undergoing extensive construction with numerous tunnels into a mountain, large piers, and support facilities. Satellite imagery shows construction of what appears to be two water entrances into a large underground tunnel complex, possibly for ballistic missile loading of submarines, as well as several land-based entry points.

Although India's sea-based deterrent remains largely under development, there is a clear ambition to field a sophisticated naval nuclear deterrent force centered around new nuclear-powered ballistic missile submarines, long-range sea-based ballistic missiles, and a large new naval base. If India seeks to always have one SSBN on patrol for a strategy of what is referred to as continuous at-sea deterrence, it will have to contend with the doctrinal, logistical, and operational complications of mating its missiles with warheads in peacetime.

Cruise missiles

Like many other nuclear-armed nations, India is making strides in developing multiple types of cruise missiles. Despite rumors to the contrary, however, none of India's cruise missiles have been confirmed to have nuclear missions and, therefore, are not included in Table 1.

India's first indigenously produced cruise missile—the Nirbhay—looks similar to the US Tomahawk or the Pakistani Babur. The Indian Ministry of Defense describes the Nirbhay as "India's first indigenously designed and developed long-range subsonic cruise missile having 1,000-kilometer range and capable of carrying up to 300-kilogram warheads" (Ministry of Defence 2019, 100).

India has reportedly completed development trials of the Nirbhay (Gupta 2023). Although there are many rumors that the Nirbhay is dual-capable, with some sources asserting that the Nirbhay is capable of carrying a 450-kilogram conventional or 12-kiloton nuclear payload (*Hindustan Times* 2024b; Missile Defense Project 2024), neither the Indian government nor the US intelligence community has publicly corroborated these statements.

India appears to be developing several derivatives of the Nirbhay in a likely effort to replace the missile, which experienced several launch failures during its testing and evaluation phase. One such project under development by DRDO is the supersonic Indigenous Technology Cruise Missile (ITCM) program. According to *Janes*, the ITCM is a technology demonstrator program for testing the capability of India's indigenous small turbofan engines, known as the "Manik," and other subsystems. A DRDO official reported that a March 2023 flight test of the ITCM successfully demonstrated the capabilities of the new engine, adding that the test paved the way for integration of the engine into a new cruise missile under development: the Long-Range Land Attack Cruise Missile (LRLACM) (*Janes* 2023a). Following that test, India's Defence Acquisition Council accorded an Acceptance of Necessity to procure the LRLACM in

August 2023 (Janes 2023b). India's Ministry of Defense reported another successful test flight of a Manik-powered ITCM in April 2024, demonstrating low-altitude flight and the successful performance of enhanced radio frequency seekers and other subsystems (M. Singh 2024).
In 2023, *Janes* reported that the DRDO designated the LRLACM as nuclear-capable, but this has not been confirmed publicly by Indian officials or US Intelligence sources (Janes 2023b).
According to a DRDO poster released by the news agency *Asian News International* in November 2023, a trial of a submarine-launched cruise missile—with land attack and anti-ship variants—was successfully conducted in February 2023 at a range of 402 kilometers (A. Menon 2023).

➲ References are available in 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 the associate director of the Nuclear Information Project at the Federation of American Scientists, and an associate senior researcher with the Nuclear Disarmament, Arms Control and Non-proliferation Programme at the Stockholm International Peace Research Institute (SIPRI). Previously, he worked for the Arms Control, Disarmament, and WMD Non-Proliferation Centre at NATO 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 senior 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. Johns is also a master's student in the Security Studies Program at Georgetown University's Walsh School of Foreign Service, where she focuses on the intersection of technology and security. 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. She also completed the Critical Language Scholarship program for Korean through the US Department of State and is a CSIS 2025 Nuclear Scholar. Johns' work has been widely published and quoted in media sources across the globe to help policymakers and the public better understand nuclear weapons trends.
Mackenzie Knight-Boyle is a senior research associate for the Nuclear Information Project at the Federation of American Scientists, where her work focuses on the status and trends of global nuclear forces and the role of nuclear weapons. Before this, Knight-Boyle was a Herbert Scoville Jr. Peace Fellow on the Project. Previously, Knight-Boyle 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.

North Korea Stopped Nuclear Testing in 2017 – But Triggered Nearly 1,400 Earthquakes Since

By Michelle Starr

Source: https://www.sciencealert.com/north-korea-stopped-nuclear-testing-in-2017-but-triggered-nearly-1400-earthquakes-since

A photograph from the dismantling of the Punggye-ri nuclear test site in May 2018. (Handout/Getty Images)

Sep 17 – When you gaze into the abyss, so Nietzsche proclaimed, sometimes the abyss gazes back into you.

And if you pummel Earth's crust with the most powerful class of explosives humanity has ever devised, the planet may not necessarily remain silent in return.

In tunnels gouged under Mount Mantap in North Korea, six nuclear devices were detonated between 2006 and 2017.

Now, geologists have discovered evidence that those tests reactivated previously quiet faults – setting off a succession of hundreds of earthquakes that continued to intensify years after the final test took place.

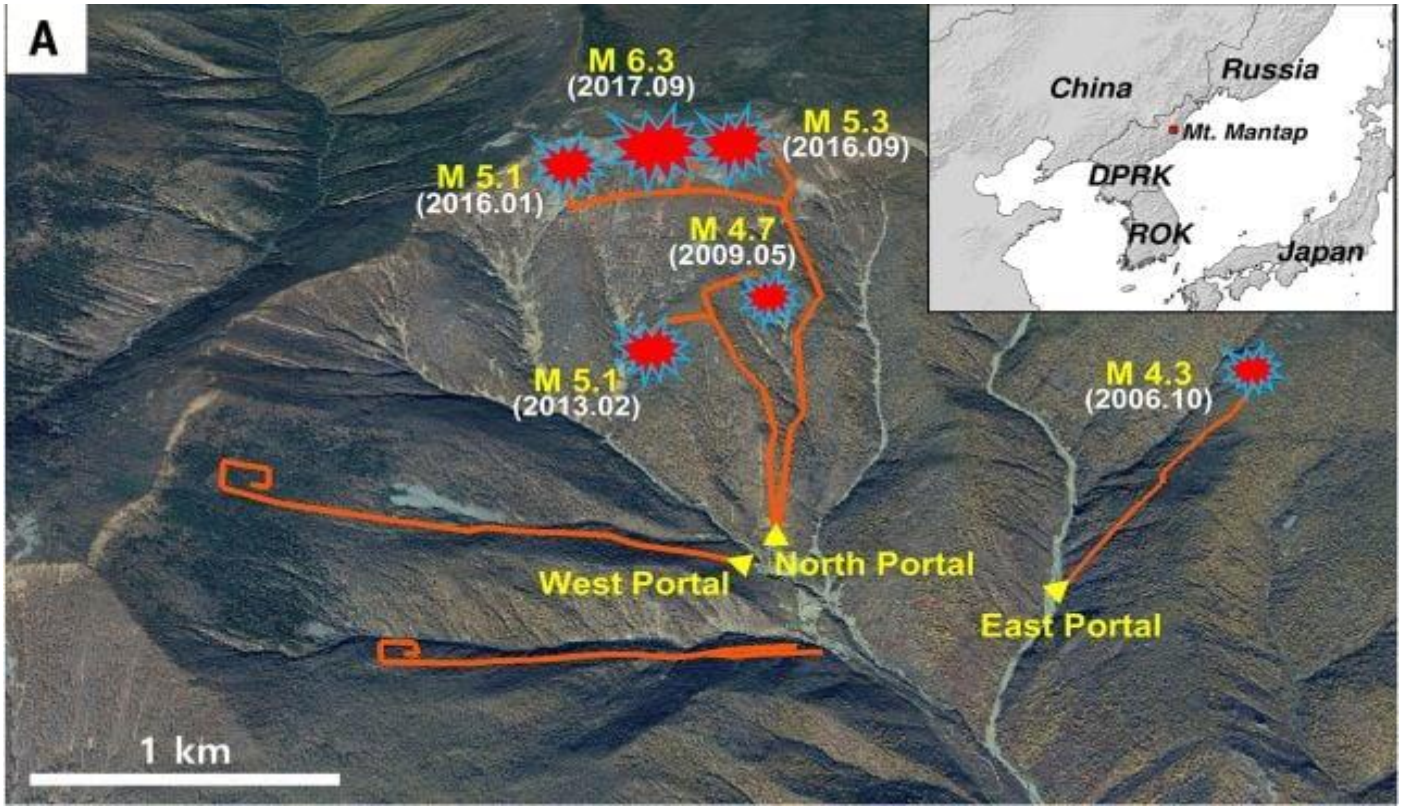
"The most remarkable result is not simply that earthquakes followed underground nuclear tests, but how the seismicity evolved," seismologist Kwang-Hee Kim of Pusan National University in South Korea told ScienceAlert.

"Instead of being strongest immediately after the explosion and then fading, the activity increased over several years."

North Korea's Punggye-ri nuclear test site sits beneath Mount Mantap, a 2,205-meter (7,234-foot) peak in the country's northeast.

The remote location was well suited to testing the nation's expanding nuclear capabilities: tunnels could be driven horizontally into the mountain beneath hundreds of meters of solid rock, helping contain the explosions. The site's first underground test was conducted

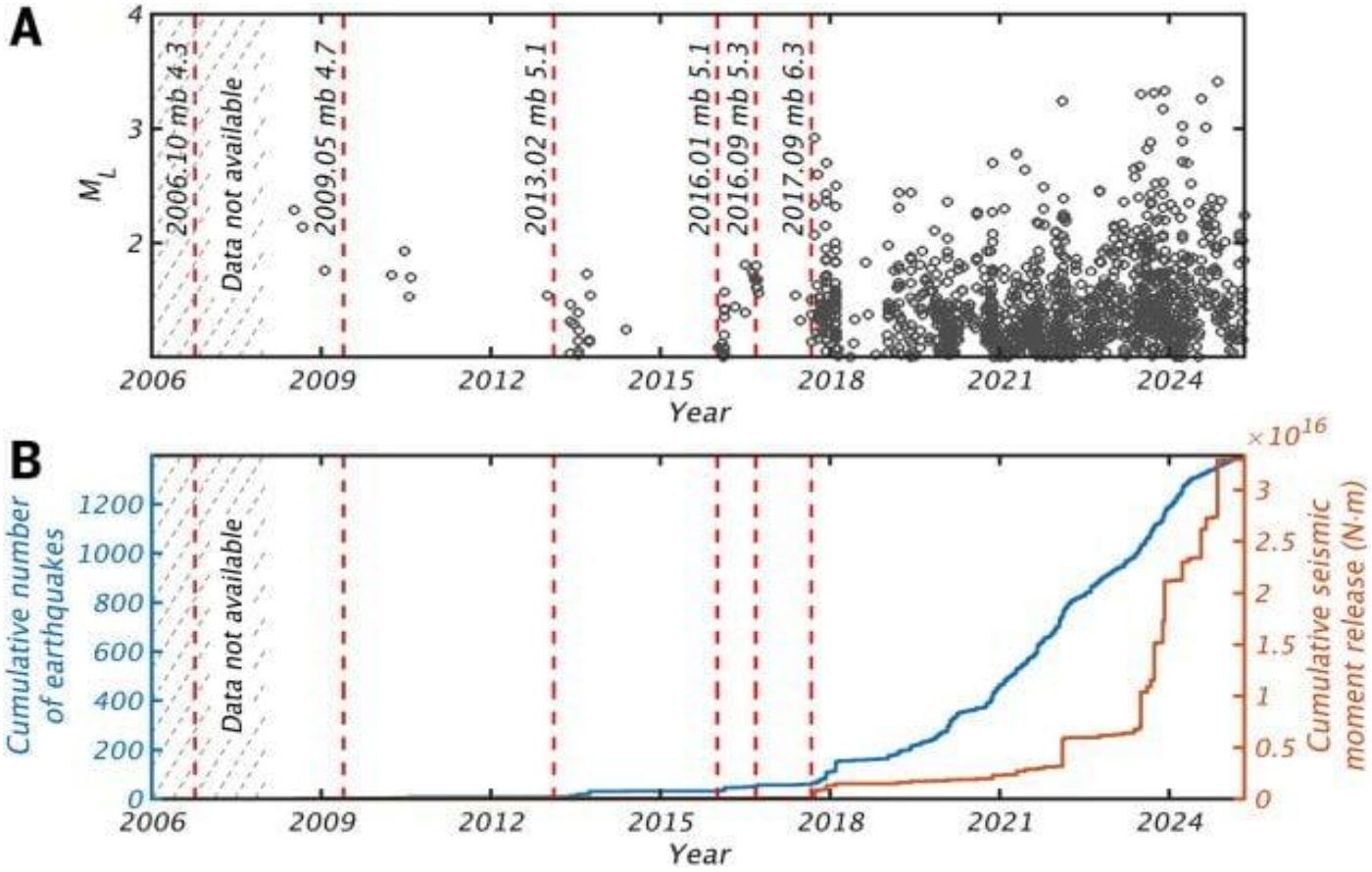
in October 2006. Five more were conducted in the ensuing 11 years, each unleashing a tremendous explosion of energy into the rock below.
The final test took place on 3 September 2017 – and it was the largest by a wide margin.
The Hiroshima bomb exploded with an energy of about 15 kilotons. The final Punggye-ri test unleashed an estimated 100 to 250 kilotons – powerful enough to produce the same signal as a magnitude 6.3 earthquake.
An underground nuclear explosion doesn't need a pre-existing cavern. The blast vaporizes and melts surrounding rock, excavating an underground cavity while sending intense stresses through the rock beyond it. As that cavity cools, its roof can collapse under the weight above.
That appears to be exactly what happened beneath Mount Mantap. Just 8.5 minutes after the 2017 explosion, instruments detected a magnitude 4.1 seismic event interpreted as the collapse of the newly formed cavity. Meanwhile, satellite radar captured the mountain itself crumpling under the force of the blast.
That was not unexpected.



A map marking the locations of the six nuclear tests. (Fan et al., *Science*, 2026)

"Earthquakes caused directly by explosion damage, cavity collapse, or a conventional aftershock-type response would normally begin promptly and decrease as the transient disturbance dissipates," Kim said.
And, as it was the final test, the cavity collapse should have marked the beginning of the end of the seismic disruption from Punggye-ri.
But three weeks later, Earth started grumbling.
"At Mt. Mantap, however, only a few events were reported immediately after the sixth test," Kim continued, "whereas the sustained tectonic seismicity began about 20 days later and then intensified over the following years." The earthquakes raised an intriguing question. Most previous research at Punggye-ri had focused on the nuclear tests themselves – where and when the explosions occurred, and how powerful they were.

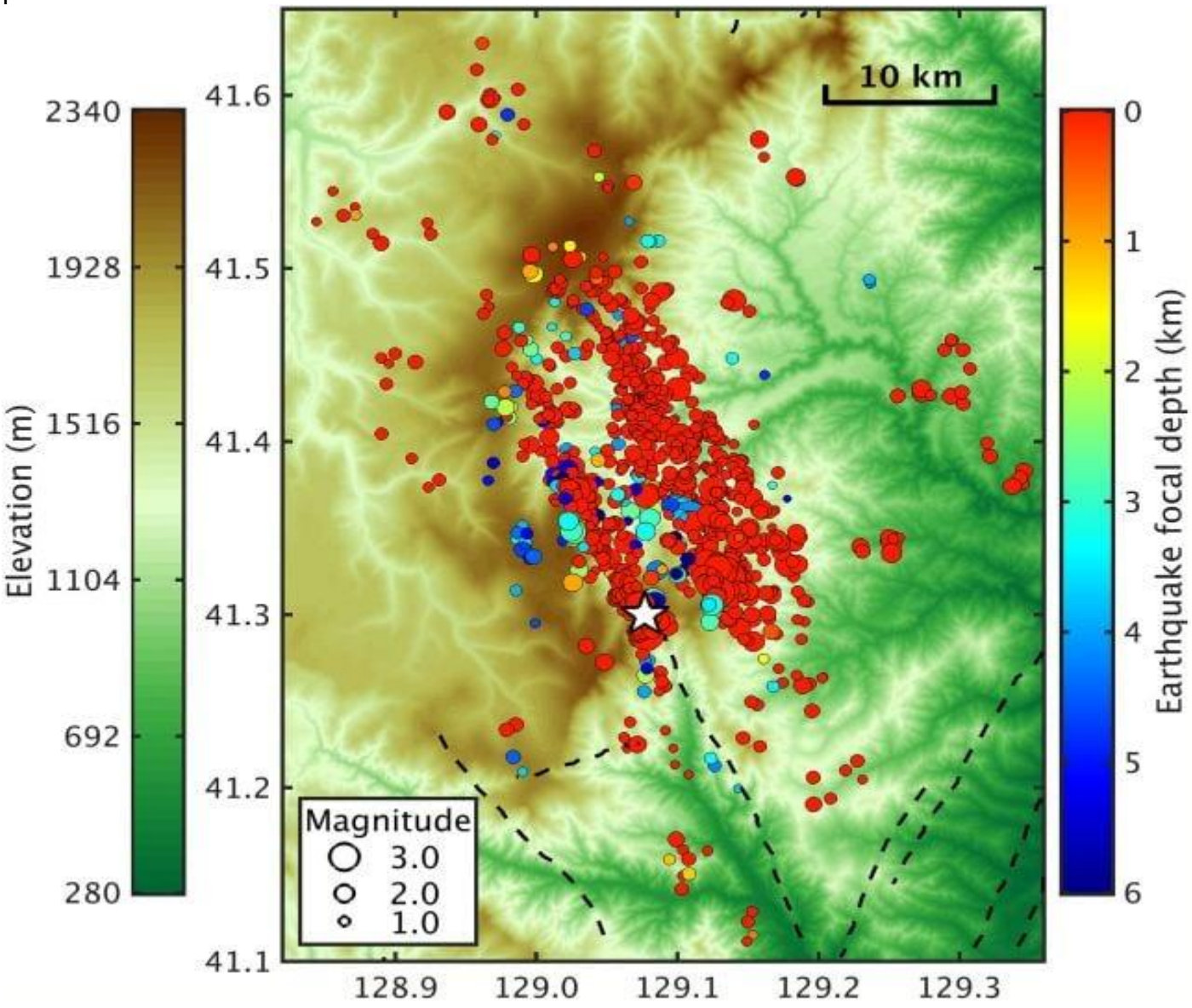
What happened to the crust in the years afterward was much less well understood.
So the researchers went back and combed through 17 years of seismic recordings from stations in China and South Korea, spanning 2008 to 2025.
The team used a technique called matched-filter detection, which allowed them to pick out tiny earthquakes that routine monitoring had missed.
They found 1,399 of them.



Graphs show how earthquake activity increased in the region over time. (Fan et al., *Science*, 2026)

Mount Mantap is not known as a seismically active place, though. In fact, it's almost exactly the opposite. When the researchers looked at historical records, what they found was a whole lot of practically nothing, going back hundreds of years.
Between 23 BCE and 1903 CE, they found just one event – a large crustal earthquake within 200 kilometers – a magnitude 6.7 event in 1810, around 100 kilometers away from Mount Mantap.
"Major regional and global earthquake catalogs likewise documented no crustal earthquakes within 50 km of the site between 1 January 1904 and 3 September 2017," Kim said.
That doesn't mean the ground had been completely silent. Historical records are incomplete, particularly for tiny earthquakes in remote places, and the team's much more sensitive search picked up sparse local activity beginning in 2013, after the third nuclear test.
Even so, the region remained relatively quiet. Until 2017.
On 23 September 2017, the mountains shuddered… and then never really stopped.
Earthquakes continued to rattle the region over the following months and years. Stranger still, rather than gradually dying away, the activity intensified.
"Both the earthquake rate and seismic moment release continued to increase through May 2025, the end of our study period," Kim said.

That would be intriguing enough – but the locations of the earthquakes started to reveal another pattern.



The spatial distribution of quakes during and after the nuclear tests. (Fan et al., *Science*, 2026)

The team was able to precisely trace 955 of the earthquakes. When they plotted those locations, they weren't scattered higgledy-piggledy around Mount Mantap. Instead, they mapped out two roughly parallel structures running north-northwest from the test site.

One followed the projected continuation of a fault already mapped south of Punggye-ri. The other didn't correspond to any known surface fault – but still traced a distinctly fault-like pattern.

That pattern suggested that the nuclear tests had disturbed pre-existing weaknesses in the crust. But that left a puzzle: How could explosions that ended in 2017 still be influencing earthquakes years later?

It wasn't because the energy from the blasts was still reverberating through the mountain.

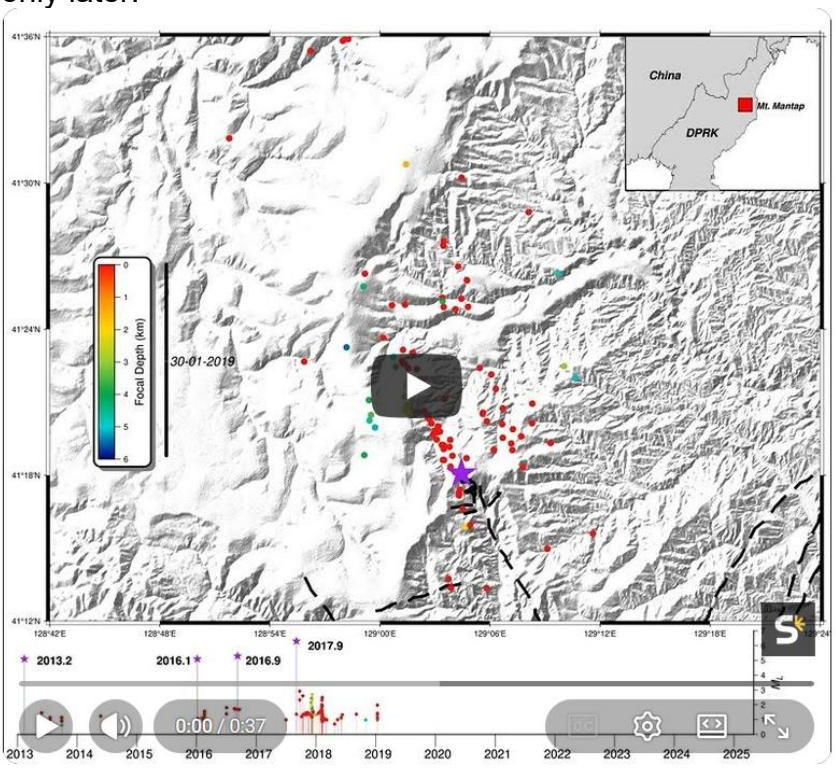
"The seismic waves themselves did not continue acting for years," Kim said. "Rather, we infer that the repeated tests altered the mechanical balance of a heterogeneous crust that was already close to failure."

The immediate effects of an underground nuclear explosion are relatively short-lived. The blast can fracture surrounding rock, alter stresses nearby, and – as happened after the final Punggye-ri test – cause the newly formed cavity to collapse.

But those effects alone couldn't explain earthquakes appearing tens of kilometers away and continuing to intensify years later. Instead, the researchers believe that the cumulative effects of repeated explosions were responsible.

"An everyday analogy would be a stack of rough blocks that is already being squeezed and is close to sliding," Kim explained.

"Repeated jolts can alter how the load is shared between the blocks. Even after the jolting stops, the movement of one contact can transfer stress to neighboring contacts, some of which may slip only later."



Mount Mantap itself may have helped shape where that transferred stress ultimately found an outlet. Its steep, uneven topography creates variations in the stresses already acting on the shallow crust, making some locations more favorable for slipping than others.

The mountain itself wasn't the trigger, Kim stressed. Rather, its topography provided a "long-lived mechanical framework" that helped determine where the effects of the nuclear tests played out.

Whether that process could eventually produce a much larger earthquake is unclear. The longer of the two fault-like structures extends for around 24 kilometers; if it represents a single connected fault that ruptured along its entire length, the researchers estimate it could theoretically produce an earthquake around magnitude 6.4.

But that's a hypothetical scenario, not a prediction. There's no evidence such an earthquake is imminent, and the structure may instead consist of multiple smaller fault segments.

The findings nevertheless suggest the geological consequences of underground nuclear testing may need to be monitored for much longer than previously appreciated – both at Punggye-ri and potentially at other test sites where pre-existing faults are already close to failure.

They also complicate the job of distinguishing seismic activity caused by nuclear testing from ordinary tectonic earthquakes. As Kim put it, the results "broaden the time window that should be considered; they do not lower the standard of evidence required to establish causality."

And causality here can't be proven as it could in a controlled experiment. The faults were already there, loaded by natural stresses, and earthquakes might eventually have occurred without the nuclear tests.

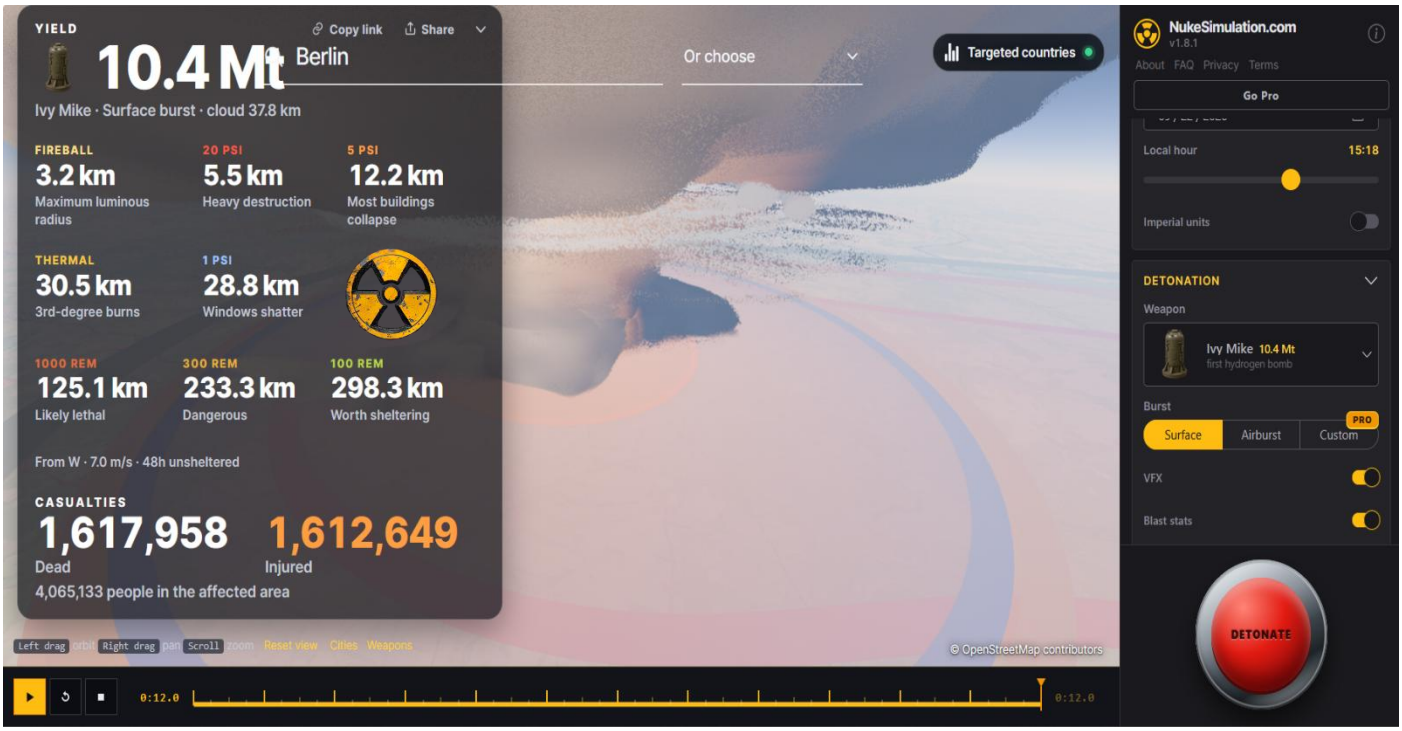
But the timing, location, and unusual evolution of the seismicity all point in the same direction.

"Our interpretation is that the tests disturbed a crustal volume already close to failure and advanced or facilitated slip on pre-existing faults," Kim said.

●▶ The findings have been published in *Science*.

You do not like them? Nuke them

Source: https://nukesimulation.com/



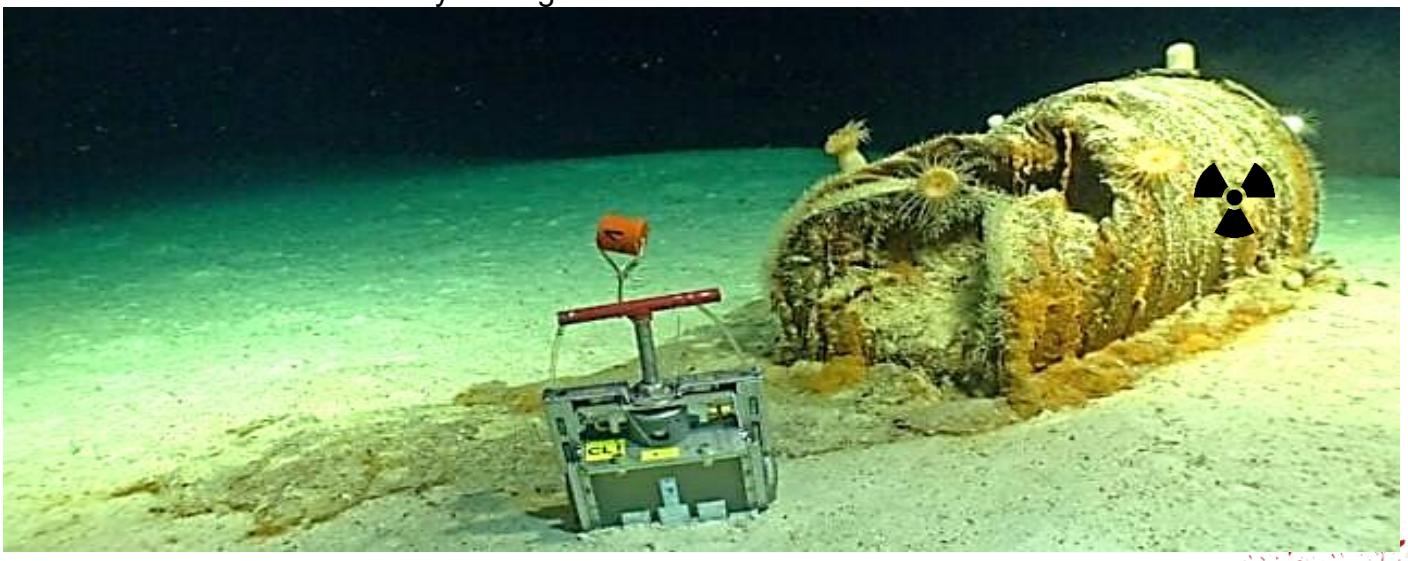
City selection purely experimental

Try also: https://nuclearsecrecy.com/nukemap/
https://outrider.org/projects/nuclear-bomb-blast-simulator

150,000 Tons of Radioactive Waste Were Dumped in The Atlantic. Decades Later, It's Visibly Oozing.

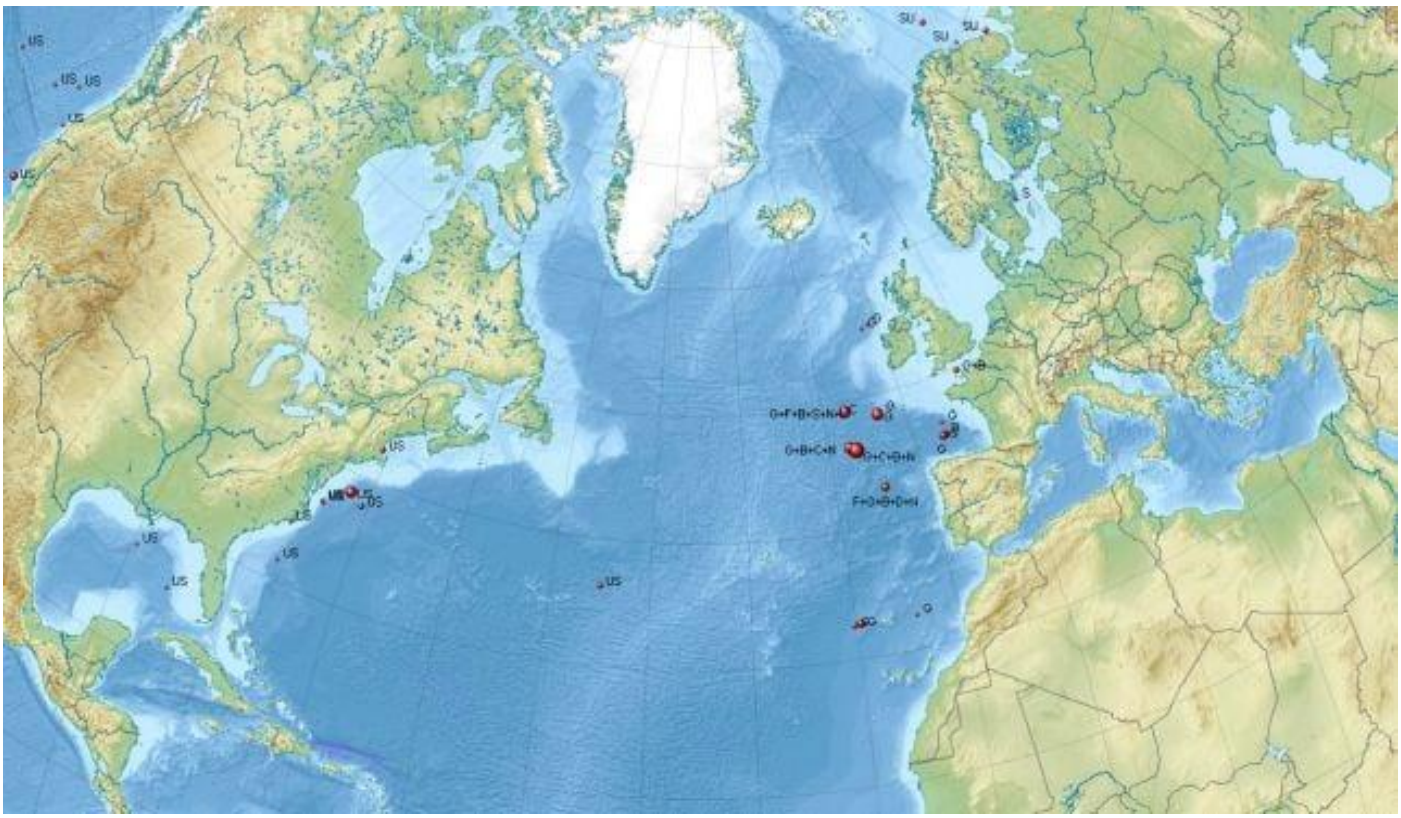
By Michelle Starr

Source: https://www.sciencealert.com/150000-tons-of-radioactive-waste-were-dumped-in-the-atlantic-decades-later-its-visibly-oozing



A barrel oozing radioactive waste at the bottom of the Atlantic Ocean. (NODSSUM Campaign, CNRS, French Oceanographic Fleet)

Sep 21 – The second half of the 20th century was something of a golden age for nuclear technology.



A map of oceanic nuclear waste dump sites. (Masaqui/Wikimedia Commons, CC BY-SA 3.0)

Following the atomic devastation of WWII, the world found new, more benign uses for radioactive decay. Power plants, medical treatments, scientific research, and industry all blossomed under a benevolent nuclear glow.

But with the nuclear revolution came a significant problem – what to do with all the thousands of tons of radioactive waste generated in the excitement.

For Europe, the solution was relatively simple. There was a perfectly good seafloor at the bottom of the Atlantic Ocean that, as far as the authorities were concerned, no one important was using. So, between 1949 and 1982, that's where it went – more than 200,000 barrels of low-level radioactive waste, totaling more than 150,000 tons, mostly dumped at depths between 3,000 and 5,000 meters (9,840 and 16,400 feet). For decades, no one really knew what had become of them.

Now, scientists have descended to the wreckage in a crewed submersible to investigate – and found many of the barrels corroded and degraded, their contents spilling across the seafloor.

Surprisingly, this isn't necessarily a subversion of the original plan.

Radioactive waste categorized as low-level, or LLW, doesn't mean that it's not hazardous. It comes from sources such as medical and industrial use and typically contains lower levels of long-lived radionuclides.

The International Atomic Energy Agency recommends that LLW be disposed of in robust containment in isolation for at least a few hundred years – but back in the mid-20th century, the recommendations were a little different. The contemporaneous guidelines recommended that containers needed to reach the seafloor intact and remain sealed only long enough for the short-lived radionuclides to decay.

After that, the remaining waste was expected to slowly escape and disperse through the surrounding ocean.

Not everything in the barrels would conveniently decay

away, however. They contained a radioactive hodgepodge, including cesium-137, plutonium isotopes, and tritium, some of which can persist for thousands of years.

When the dumping stopped in the 1980s, everyone pretty much just dusted off their hands and walked away. The precise locations and conditions of the barrels remained poorly known for decades.

But then, a few years ago, nuclear engineer Patrick Chardon and marine geologist Javier Escartín of the French National Center for Scientific Research started to wonder what had become of the dumped waste.

That question eventually became NODSSUM – Nuclear Ocean Dump Site Survey Monitoring – an interdisciplinary project bringing together nuclear physics, geology, oceanography, biology, and marine chemistry to find the barrels and investigate what, if anything, they were doing to the surrounding environment.

The first expedition set sail in June 2025 aboard the research vessel *L'Atalante*. In this first foray, the team sent an autonomous underwater vehicle called *UlyX* sweeping across the seafloor to map and photograph the barrels, while collecting water, sediment, fish, and crustaceans from the surrounding area.

In just a month, they located and mapped 3,355 barrels.

That first expedition was reconnaissance, giving the researchers something they hadn't had before – targets.

Then, in May 2026, they went back.

This time, aboard the *Pourquoi Pas?*, the team brought *Nautile*, a three-person submersible capable of descending 6,000 meters. Over 20 dives, it carried scientists more than 4,700 meters down to inspect the barrels directly and collect samples from their immediate surroundings.

At first glance, the condition of some of the barrels was alarming.

They were heavily corroded and degraded, with material visibly oozing out onto the surrounding sand.

But here's where the expedition became puzzling – because the barrels also appeared to function as tiny oases on the otherwise sparsely populated sandy seafloor.

Anemones had attached themselves to the barrels. Sponges, sea cucumbers, fish, and crustaceans lived around them, with crabs apparently particularly fond of the artificial shelters.

This presented the researchers with an unexpected problem. The barrels weren't simply containers slowly releasing radioactive material into an empty abyss. They had become part of the ecosystem.

Which raised a much more complicated question: Was any of that radioactive material making its way into the animals themselves?

There was no question that radioactive material had escaped containment. Instruments aboard the ship detected significant signals of cobalt-60 and niobium-94, which the researchers could specifically link to the dumped waste.

Cesium-137 and americium-241 were also present at levels well above the background expected from atmospheric nuclear testing and accidents.

Whether that radioactivity is accumulating in the animals living on and around the barrels is another matter.

At five sites, *Nautile* collected sediment, water, organisms and microbial communities from immediately around – and even in contact with – the barrels. The researchers also sampled nearby rocky habitats to give them something to compare the barrel communities against.

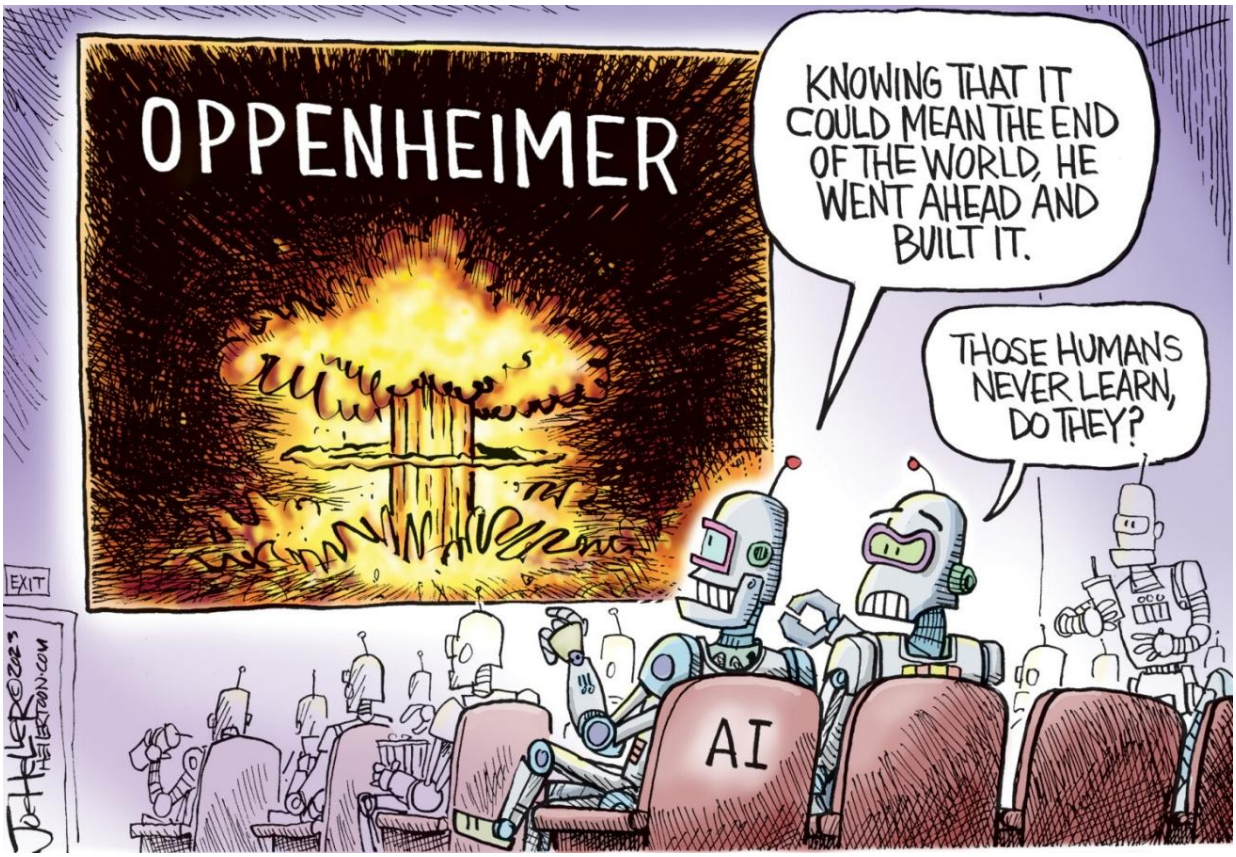
Those samples are now being analyzed to determine what effect – if any – these strange habitats are having on the creatures that now call them home.

There is precedent, however, to suggest that even striking levels of radioactivity around a source don't necessarily spread very far.

A recent study of the sunken Soviet submarine *Komsomolets* found radionuclide levels hundreds of thousands of times above background immediately around the leaking reactor – but those levels dropped sharply within just a few meters as the material dispersed through the seawater.

The NODSSUM team similarly found that, despite the significant radioactive signals around the barrels, activity levels weren't high enough to pose major radiation-protection problems for the scientists handling the samples. *Nautile* and the instruments it carried showed no signs of contamination. None of this means the waste is harmless – nor does it mean we're about to be overrun by radioactive crabs.

But for the first time, researchers have a detailed map of thousands of barrels and samples that can reveal what is happening around them.



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

Weapons, military equipment and

EXPLOSIVE NEWS

Bang bange iPhone!

A new Sheriff in open seas

The heavy nuclear-powered cruiser **Admiral Nakhimov** of the Russian Northern Fleet is completing trials and will be commissioned by the end of the year. In August 2025, it went to sea for trials. As part of the modernization, the cruiser received new radar, avionics and

sonar systems, a new 130 mm AK-192M cannon, and new missile armament. Instead of 20 P-700 Granit anti-ship missiles, the ship received 80-cell vertical launch systems (VLS) and can carry Zircon hypersonic missiles, as well as Kalibr cruise missiles and Oniks anti-ship missiles, while in total more than 176 missiles of each type are ready for launch. The air defense is now based on the maritime version of the S-400.

Bombs, Bugs, and Bots: Preventing the Proliferation of Weapons of Mass Destruction 25 Years After 9/11

By Christina McAllister and Cindy Vestergaard

Source: https://www.stimson.org/2026/bombs-bugs-and-bots-preventing-the-proliferation-of-weapons-of-mass-destruction-25-years-after-9-11/

Sep 03 – Rooted in the lessons of 9/11, the G7 Global Partnership against the Spread of Weapons and Materials of Mass Destruction has quietly eliminated or secured a vast inventory of dangerous chemical, biological, and nuclear weapons and related materials around the world over the past quarter century, thereby keeping them out of the hands of terrorists and other non-state actors. The Global Partnership has also played a key role in channeling dual-use scientific expertise to peaceful purposes and building international capacity to detect, report, and respond to threats at the source. As the rapid advances and convergence of technologies like artificial intelligence, quantum sensing, synthetic biology, additive manufacturing, and uncrewed aerial systems with WMD transform the landscape of threats and threat reduction opportunities, the Global Partnership's threat reduction mission has evolved even as it remains as critical as ever.

From Terrorists to Technology: Changing Threats Require Changed Approaches

Twenty-five years after the terrorist attacks on the United States on September 11, 2001, the threat from weapons of mass destruction (WMD) has changed in ways that would have been difficult to imagine at the turn of the century. Before 9/11, the proliferation of biological, chemical, and nuclear weapons was largely viewed as a threat posed by

states and their arsenals. The 9/11 attacks demonstrated that catastrophic harm could also be inflicted by non-state actors. The anthrax attacks in the United States that followed further heightened fears about the prospect of disaffected insiders, "lone wolves," and terrorists pursuing biological weapons and other WMD, and helped to catalyze the launch in 2002 of the G8-led Global Partnership Against the Spread of Weapons and Materials of Mass Destruction (GP) to prevent terrorists and those who harbor them from acquiring or developing WMD and related materials, equipment, and technologies. While both state and non-state actors remain real and present threats today, rapidly advancing and converging technologies are drastically reshaping who can access, develop, detect, and deploy WMD, requiring approaches to threat reduction to adapt once more.

Kananaskis 2002: Cold War Legacy Reframed

The mechanism that the G8 leaders announced at their first post-9/11 summit at Kananaskis in June 2002 was modeled on the U.S. Nunn-Lugar Cooperative Threat Reduction Program, which had been working bilaterally with Moscow since 1991 to secure and dismantle vulnerable cold war WMD stockpiles and delivery systems across Russia and the former Soviet Union. At Kananaskis, G8 leaders effectively turned the CTR Program into a multilateral endeavor, with the GP committing to contribute up to US$20 billion over 10 years, with an initial focus on destroying or securing the vast WMD legacy concentrated in Russia and other former Soviet countries.

The GP achieved tangible results during its first decade, including the destruction of approximately 40,000 tonnes of chemical weapons in 5.6 million munitions, the dismantlement of nearly 200 decommissioned Russian nuclear submarines, the disposition of fissile materials, and the redirection of 90,000 former weapons scientists to peaceful work. The GP also helped end the production of plutonium for weapons purposes at power reactors in Russia and Kazakhstan, replace highly enriched uranium with low-enriched uranium in research reactors, and consolidate dangerous pathogens and nuclear materials at fewer, more secure sites.

By 2010, most of the projects in Russia were completed or winding down and, in accordance with the GP's expanded geographic mandate adopted in 2008, GP members were shifting focus away from dismantling legacy arsenals to broader capacity building to prevent and reduce chemical, biological, radiological, and nuclear (CBRN) security threats globally. In 2011 the renewed Global Partnership agreed on four priorities: (1) nuclear security; (2) biological security; (3), scientist engagement; and (4) implementation of United Nations Security Council Resolution 1540 (a resolution obliging states to implement a range of domestic measures to prevent WMD proliferation, including by non-state actors). In March 2014 when Russia annexed Crimea, the G8 became the G7 when it suspended Russia from the exclusive club, and from the GP.

Twenty-Four Years of Tangible Threat Reduction

The GP's second generation of threat reduction included strengthening nuclear and radiological security; improving chemical and biological safety and security; enhancing border security, export controls; supporting international treaty regimes and their institutions; and helping countries meet obligations such as UN Security Council Resolution 1540. In doing so, the GP built a global "web of prevention" linking governments with international organizations, technical institutions and civil society. A key — and continuing — focus of this work has also been sustained biothreat reduction work, particularly through the Signature Initiative to Mitigate Biological Threats in Africa (SIMBA). In partnership with African organizations including the Africa Centers for Disease Control, SIMBA supports sustainable capacity

development in biosecurity, biosurveillance, and non-proliferation.
Throughout, the GP maintained its ability to respond to active crises. Its established relationships, expertise, and delivery mechanisms have enabled it to pivot when urgent threats emerge, including supporting the international effort to eliminate Syria's declared chemical weapons program in 2013 — and again over the past year, with GP members supporting redeployment of inspectors from the Organisation for the Prohibition of Chemical Weapons (OPCW) to Syria where they are working closely with the transitional government in Damascus to uncover, verify, and destroy the former Assad regime's remaining chemical weapons and facilities. The GP was also instrumental in providing support for eliminating dangerous chemical weapons materials in Libya in 2016 and has funneled CBRN security support to Ukraine since Russia's full-scale invasion in February 2022. GP members continue to contribute to the OPCW's Trust Fund on Assistance and Protection of Ukraine and to the International Atomic Energy Agency's continuous monitoring missions at Ukraine's nuclear power plants after Russia's seizure and occupation of the Zaporizhzhia nuclear power plant, Europe's largest. The ability to adapt, coordinate, and build on previous experiences has been central to the GP's staying power.

The Threat Landscape is Changing Again

A quarter of a century after 9/11, the WMD threat landscape has changed again, now being shaped by rapid technological change. The diffusion of advanced technologies is creating new pathways through which WMD capabilities can be developed, acquired, or deployed. Artificial intelligence (AI), synthetic biology, quantum technologies, additive manufacturing, autonomous systems, and other emerging technologies can alter the accessibility, speed, scale, precision, and detectability of activities relevant to WMD.
In 2002, the question was how to prevent WMD materials and expertise from falling into the wrong hands. In 2026, the question is how to ensure that rapidly advancing technologies do not create new pathways to WMD proliferation and how to harness those same technologies to make threat reduction more resilient and effective.
While the GP's continued focus on state-based WMD programs and the acquisition and use of WMD by non-state actors remains as relevant today as 25 years ago, the changed threat environment has prompted the adoption of an updated strategy to match the times.
During Canada's G7 Presidency in 2025, GP members endorsed a new threat reduction strategy focused on WMD-Relevant Technologies (WMD-RT), to include AI, synthetic biology, quantum sensing, additive manufacturing, and uncrewed aircraft systems (UAS). A key feature of the strategy is its focus not just on the potential these technologies have to accelerate and exacerbate WMD threats, but also to offer new tools for prevention, detection, and response.

IMPACT WMD: Next Generation Threat Reduction

Following the adoption of the new strategy, the GP's CBRN Working Group approved the establishment of the Innovation for Mitigating Proliferation and Countering Threats of WMD (IMPACT WMD) Initiative in November 2025. It is designed to serve as an agile, action-oriented mechanism to engage regularly, strategically, and programmatically with industry partners — through a Community of Action (CoA) — that share the GP's threat reduction objectives to address the benefits and risks of WMD-RT.
Its three workstreams — shared principles and language, horizon scanning and scenario modelling, and technology sprints — are oriented toward identifying emerging risks and turning technological opportunities into practical threat-reduction capabilities.
While the G8 mobilized to address a dangerous legacy of the past at Kananaskis, with IMPACT WMD, the GP is building resilience and

preparing for the technologies shaping threats today and in the future.

The Enduring Value of the Global Partnership

Operating for nearly a quarter century, the G7-led GP has become the world's largest and longest-standing multilateral mechanism dedicated to WMD threat reduction. What began in the aftermath of 9/11 as a response to acute risks posed by non-state actors and the vast Soviet legacy of WMD materials, facilities, and expertise has evolved into a partnership of 31 members coordinating practical efforts to prevent, detect, and respond to CBRN security threats around the world. As a flexible framework through which multiple countries can pool resources, expertise, and political attention to further concrete threat-reduction projects, the GP has proven its value to the threat reduction enterprise. With IMPACT WMD, the GP is adapting again: from managing known WMD risks toward anticipating and shaping the emerging technological environment in which future WMD risks may arise.

Christina McAllister is a Senior Fellow and Director of the Partnerships in Proliferation Prevention program at the Stimson Center. Prior to joining Stimson, Christina served as a senior advisor to U.S. Department of Defense offices responsible for non-proliferation and countering weapons of mass destruction (CWMD). As a Booz Allen Hamilton consultant, she led strategic communications initiatives for the Cooperative Threat Reduction (CTR) Program, the Defense Threat Reduction Agency (DTRA), U.S. Special Operations Command, and the Office of the Deputy Assistant Secretary of Defense for Chemical and Biological Defense Programs. From 2006 to 2014 she led teams supporting the work of CTR's Biological Threat Reduction Program to strengthen detection and reporting of dangerous infectious disease outbreaks and enhance biosafety and biosecurity practices around the world. She subsequently led an advisory team in the Office of the Deputy Assistant Secretary of Defense for CWMD Policy. Christina previously covered political, social, and economic issues in Russia, Ukraine, Belarus, and Moldova as a correspondent for Reuters news agency in Moscow and Kyiv. In Reuters' Washington, DC, bureau, assignments included reporting from the White House, State Department, Capitol Hill, and the 2004 presidential campaign. Christina holds an M.A. in International Relations and International Economics from the School of Advanced International Studies at Johns Hopkins University and received her B.A. in Modern Languages (Russian and French) from the University of Cambridge. She is a certified Project Management Professional (PMP).

Cindy Vestergaard is the Project Lead for the Converging Technologies and Global Security program. She previously directed the Nuclear Safeguards program (2016 – 2022) and the Blockchain in Practice program (2018 – 2022) and was a Nonresident fellow for both programs in 2023 when she served as Vice President, Special Projects and External Relations at DataTrails. Before joining Stimson in 2016, Vestergaard was previously a senior researcher at the Danish Institute for International Studies (DIIS) in Copenhagen, Denmark. Prior to DIIS, she worked on non-proliferation, arms control and disarmament policy and programming at Canada's foreign ministry. Positions among others included Senior Policy Advisor, Global Partnership Program; Senior Policy Advisor, Foreign Intelligence Division; and Political Officer at Canada's Mission to Hungary and Slovenia. Vestergaard has been an external lecturer at the University of Copenhagen, a regular contributor to media outlets and presents nationally and internationally on weapons of mass destruction, proliferation and disarmament issues. She has a B.A. in International Relations from the University of British Columbia, M.A. in International Relations and European Studies from Central European University (Budapest, Hungary) and Ph.D. in Political Science from the University of Copenhagen.

FORENSIVERSE

THE EXPLOSIVES DETECTIVE BOARD

Tracing Chemical and Physical Evidence

EXPLOSIONS LEAVE CLUES. SCIENCE BRINGS THEM TO LIGHT.

> "Explosives may destroy structures, but they cannot destroy the truth."
> — B.R. Sharma

1. WHAT ARE EXPLOSIVES?

Explosives are chemical compounds or mixtures that undergo rapid chemical reaction, producing large volumes of hot gases, heat, light, sound and pressure.

- Used in mining, construction, military, fireworks – and sometimes in crimes.
- Can be solid, liquid, gas or improvised mixtures (IEDs).

Dynamite | Grenade | Ammonium Nitrate (AN)

2. TYPES (WITH EXAMPLES)

Type	Examples
High explosives	TNT, RDX, PETN, Nitroglycerin
Low explosives	Black powder, Fireworks (pyrotechnics)
Blasting agents	ANFO (Ammonium Nitrate + Fuel Oil), Slurries, Emulsions
Initiators	Detonators, Fulminates (Lead azide, Mercury fulminate)
Improvised explosives	Homemade devices (IEDs)
Others	Smokeless powders, Gel explosives

- *Different explosives have different chemical and physical characteristics, aiding in their identification.*

3. SOURCES OF EVIDENCE

- Unexploded devices and their components
- Explosive residues from blast site (soil, debris, walls)
- Fragments of containers, wires, switches, timers
- GSR-like particulate residues (nitrates, nitrites)
- Characteristic odour or discolouration
- Documents, packaging materials, fingerprints, tool marks, and digital evidence

Fragmented casing | Wiring & timer | Blast debris

4. COLLECTION & PRESERVATION

- Search the scene carefully and systematically.
- Collect debris, swabs, soil, and suspected materials.
- Use clean, dry, non-reactive containers (glass or metal).
- Avoid plastic (may absorb/lose volatile residues).
- Seal, label and maintain chain of custody.
- Place in airtight containers.
- Note location, quantity, appearance and odour.

Careful collection today, stronger evidence tomorrow.

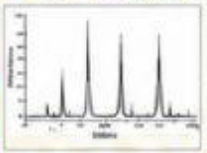
EXPLOSIVE TRACE ANALYSIS

Tiny residues.
Big answers.
Linking people, places and devices through science.

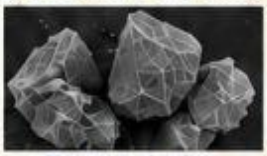
Tracing chemical and physical evidence to reveal the story behind the blast.

5. ANALYTICAL TECHNIQUES

- Preliminary tests – colour tests, spot tests (e.g., Griess test for nitrites, diphenylamine test for nitrates)
- Chromatography – TLC, GC, HPLC, GC-MS (separates and identifies components)
- Spectrophotometry (UV-Vis)
- Mass spectrometry (molecular identification)
- FTIR, NMR, X-ray diffraction (material analysis)
- SEM-EDX (morphology and elemental composition)



GC-MS chromatogram (explosive residues)



SEM image of explosive residue particles

6. INTERPRETING RESULTS

- Identify chemical composition and possible type of explosive.
- Compare with reference standards.
- Determine manufacturing origin or source (e.g., commercial, military, homemade).
- Link multiple exhibits (device, residues, containers).
- Correlate with other evidence (tool marks, fingerprints, timelines, CCTV).

Microscopic view of residues

Blast damage pattern

7. KEY INVESTIGATIVE QUESTIONS

- Was it an explosion or another cause?
- What type of explosive was used?
- Was it accidental, suicidal, or deliberate (terrorism)?
- Where was the device assembled?
- Can the suspect be linked to the explosion?
- Are there multiple devices or a larger network?
- Can future incidents be prevented?

Every fragment can lead to a fact.

8. CHALLENGES & LIMITATIONS

- Small and dispersed residues
- Environmental factors (rain, heat, wind)
- Contamination and improper collection
- Difficulties in distinguishing similar compounds
- Destruction of evidence due to high-temperature blast
- Requires advanced instrumentation and expertise
- Interpretation should consider all available evidence

Absence of evidence is not evidence of absence.

KEY TAKEAWAYS

- ☑ Explosive residues persist and can be detected.
- ☑ Proper collection and preservation are crucial.
- ☑ Use multiple scientific techniques for confirmation.
- ☑ Link chemical and physical evidence with other clues.
- ☑ Forensic analysis helps in identifying the source, intent and accused.

DID YOU KNOW?

Explosive residues can remain on surfaces, in soil and even in the air in the form of microscopic particles for a long time, helping investigators even after the blast.

REAL IMPACT

Forensic explosive analysis plays a vital role in solving bombings, preventing future attacks, ensuring public safety and delivering justice.

officalforensiverse@gmail.com | forensiverse | Forensiverse

FORENSIVERSE

A COMMUNITY FOR A SAFER TOMORROW

SCIENCE INVESTIGATES.

SOCIETY HEALS.
TRUTH PREVAILS.

US confirms weapons deployed in space for the first time

Source: https://www.lemonde.fr/en/international/article/2026/09/15/us-confirms-weapons-deployed-in-space-for-the-first-time_6757526_4.html

US Space Force Guardians assigned Space Delta 5 monitor computer workstations at Vandenberg Space Force Base, California, December 18, 2025. U.S. SPACE FORCES/DAVID DOZORETZ / VIA REUTERS

Sep 15 – The United States has weapons deployed in space, the US Space Force said on Monday, September 14, confirming the presence of such capabilities in orbit for the first time. "The US has on-orbit space control weapons capable of defending the Joint Force against hostile adversary action," a US Space Force spokesperson said in a statement that did not provide specifics on the weapons.

"Space control encapsulates the mission areas required to contest and control the space domain – employing kinetic and non-kinetic means to affect adversary capabilities," the statement said, adding that "these capabilities can be employed for offensive and defensive purposes."

Both Russia and China – the two main geopolitical rivals of the United States – pose potential threats to US interests in space.

China "develops and operates space and counterspace capabilities as part of a military modernization strategy," while Russia "views space as a warfighting domain and believes space supremacy will be a decisive factor in future conflicts," according to the US Space Force.

The militarization of space is as old as the space race itself – as soon as Sputnik was launched into orbit in 1957, Washington and Moscow began exploring ways to both arm and destroy satellites.

The biggest worry was once about nuclear weapons in space, but the superpowers and other countries signed the Outer Space Treaty in 1967, banning weapons of mass destruction in orbit.

Since then, Russia, the United States, China and India have

explored ways to fight in space outside of that treaty, including by targeting rivals' satellites, which are key for military communications, surveillance and navigation.

Dark Systems K-9

Source: https://darksystems.com/

Dark Systems is the world leader in K9 helmets. Worldwide, over 3,000 of the company's products have been deployed to the military and law enforcement agencies, SAR and K9 handlers. Each day, they use our DarkFighter K9 Helmet to protect their personnel. Dark Systems is a company of high-level engineers and professionals committed to listening, understanding and responding to our customers' mission-critical needs.

Essential Features of K9 Helmets: Cranial and Visual Protection

The essential features of K9 helmets are primarily centered around providing comprehensive cranial and visual protection for police dogs engaged in high-stakes environments. These specialized helmets are designed to shield the canine's head from potential injuries that can arise during law enforcement operations, particularly in situations involving crowds or violent confrontations. The reinforced structure of the helmet absorbs impacts, safeguarding against blunt force trauma that could occur from debris or aggressive encounters.

Moreover, the visual protection aspect is equally critical. K9s often operate in chaotic settings where visibility can be compromised by environmental factors such as smoke, flashing lights, or sudden movements. Helmets equipped with clear visors help maintain optimal vision while protecting sensitive eyes from harmful elements like projectiles and chemical irritants. This ensures that the canine remains focused on its task without distraction or discomfort.

In addition to cranial and visual safety, K9 helmets also offer crucial protection against sharp objects and other hazardous materials that may pose a risk during confrontations or disturbances. For instance, during public manifestations where tensions run high, these helmets act as a barrier against potential attacks from weapons or thrown objects. Overall, K9 helmets play an indispensable role in enhancing the operational capabilities of police dogs while ensuring their safety in unpredictable environments.

Protection Against Sharp and Dangerous Objects

In the demanding environment of law enforcement, K9 units often find themselves in situations where their canine partners are exposed to various hazards. One of the most critical aspects of a K9 helmet is its ability to provide protection against sharp and dangerous objects. In scenarios such as crowd control or tactical operations, the risk of injury from projectiles, glass shards, or other sharp debris is heightened.

The K9 helmet is designed with durable materials that can withstand these threats, ensuring that the canine's head remains safeguarded during high-stakes encounters.

The protective design of the helmet extends beyond just physical barriers; it also plays a vital role in maintaining the overall health and safety of the dog. By shielding sensitive areas like the ears and eyes from potential injuries caused by flailing objects or aggressive interactions, the

helmet helps to preserve not only the animal's physical integrity but also its ability to perform effectively in its role.

The role of K9 helmets in crowd control situations is vital, as these specialized pieces of equipment serve multiple protective functions for working dogs. In the chaotic environment of public demonstrations or protests, law enforcement K9s are often deployed to assist in maintaining order and ensuring safety. The helmet provides essential cranial protection, safeguarding the dog's head from potential impacts caused by thrown objects or unexpected collisions with individuals in the crowd.

In addition to physical protection, these helmets also mitigate the effects of loud noises generated by mortars or other crowd control devices. The auditory sensitivity of dogs makes them particularly susceptible to such disturbances; thus, helmets equipped with sound-dampening features help maintain their composure and focus on their tasks.

Mitigating Shock and Sound Effects from Explosive Devices

The K9 helmet serves as an essential protective gear for law enforcement canines, particularly in high-stress environments where explosive devices may be present. One of the helmet's critical functions is its ability to mitigate shock and sound effects from explosive detonations, which can pose significant risks to a dog's hearing and overall well-being.

When an explosive device detonates, it generates a powerful shockwave that can cause immediate physical harm. The auditory system of dogs is far more sensitive than that of humans. The loud concussive sounds produced by mortars and other explosive devices can lead to temporary or permanent hearing loss in dogs if they are unprotected. The K9 helmet incorporates sound-dampening features that help shield a dog’s ears from these harmful noises, allowing them to maintain their operational effectiveness during chaotic situations.

Conclusion

In conclusion, the integration of K9 helmets into law enforcement operations represents a significant advancement in ensuring the safety and effectiveness of police dogs in the field. These specially designed helmets provide essential cranial and visual protection, safeguarding our canine partners from various threats they may encounter during their duties. The importance of this protective gear cannot be overstated, as it equips K9s to navigate environments fraught with sharp objects and other hazards that could lead to a serious injury.

Moreover, during high-stakes situations such as public demonstrations or riots, K9 helmets play a vital role in shielding these animals from the shockwaves and loud noises generated by mortars and other crowd control measures. By mitigating these sensory stressors, helmets help maintain the composure and focus of police dogs when they are needed the most.
The enhanced safety afforded by K9 helmets not only protects the physical well-being of these invaluable assets but also ensures that they can perform their roles effectively without undue distraction or fear. As law enforcement agencies continue to recognize the importance of K9 units in maintaining public safety, investing in advanced protective gear like helmets is a crucial step toward fostering a safer working environment for both handlers and their canine partners.
Ultimately, prioritizing K9 safety translates into more successful operations and better service to communities.

'Just ask Grok': How ISIL is using Big Tech's AI to build bombs

By Caolán Magee
Source: https://www.aljazeera.com/news/2026/9/18/just-ask-grok-how-isil-is-using-big-techs-ai-to-build-bombs

Sep 18 – Boko Haram fighters are using the artificial intelligence chatbots of Big Tech companies to help build more powerful bombs, plan attacks and solve problems during combat, according to research by the University of Cambridge.
Researchers interviewed 27 former members of Boko Haram's two factions – the ISIL affiliate in West Africa Province (ISWAP) and Jama'at Ahl as-Sunnah lid-Da'wah wa'l-Jihad (JAS). A number of members described using Sam Altman-led OpenAI's ChatGPT, Anthropic's Claude, Google's Gemini, Elon Musk's Grok, Mark Zuckerberg's Meta AI and China's DeepSeek as a routine source of technical and military advice before, during and after attacks.
Meanwhile, exclusive material obtained by Al Jazeera reveals how supporters of the wider ISIL (ISIS) movement are sharing instructions on bypassing AI safety controls and obtaining weapons-related information. Researchers at Tech Against Terrorism infiltrated a pro-ISIL technical forum where supporters instructed one another on how to use AI and circumvent its safety restrictions.
The findings come amid growing concern over ISIL's adoption of emerging technologies. In February, United Nations officials warned the Security Council of increased use of advanced AI by ISIL and its affiliates. At the same time, researchers and several of the technology industry's most prominent figures have warned that increasingly powerful AI systems are advancing faster than safeguards, raising concerns that unchecked advances in AI are making it easier for armed groups to exploit the technology.
"There is nothing we haven't received an answer on," a former ISWAP commander told the researchers.

From a projector to the battlefield
Deep inside a rebel stronghold in northeastern Nigeria, former fighters described a strikingly organised and sophisticated system for putting the technology to use.
According to the Cambridge research, operatives travelled to ISWAP-controlled territory to teach senior members how to use AI. Fighters were selected and assembled in rooms around laptops and projectors and shown how to query chatbots and circumvent the safeguards designed to prevent them from answering dangerous requests.
"The white guys came and taught us," one former commander recalled. "They assembled the top people in a room and used a projector to show how it works on a big screen."

The trainers supplied laptops equipped with privacy and encryption tools, while accounts and paid subscriptions to multiple AI platforms were set up for members, according to former fighters cited in the study. Respondents repeatedly identified the wider ISIL movement as the source of their AI training.

What followed, the research suggests, went far beyond occasional use of ChatGPT by individual fighters. Both ISWAP and JAS established dedicated AI units staffed by people with specialist operational knowledge, including engineers, weapons specialists and bomb-makers. One former JAS commander described a specialised unit of 23 people working from a solar-powered room, where its members answered questions, analysed information and trained senior commanders gathered around a laptop.

"'[Ask] how can I build a bomb?' and then it tells you how," explained a former Boko Haram commander. "It is like a human robot. We used it a lot." Another former member was similarly enthusiastic: "God has helped us, and so will AI."

Often, according to the study, bombmakers would keep laptops beside them, each time returning to the chatbot when they encountered a problem while they assembled explosive devices.

Building bombs with AI

Antonia Juelich, who authored the Cambridge study, told Al Jazeera roughly 10 of the 27 people interviewed discussed the use of AI in relation to explosives, including attempts to make bombs more powerful and recover explosive material from military ordnance.

But what Juelich found most concerning was not simply that fighters could obtain information about weapons – much of that has long been available in manuals and online. AI could instead respond to the specific problem in front of them.

She pointed to accounts of fighters asking AI how to improve explosives using the limited materials they already had available. Rather than searching for generic instructions, they could tell the chatbot what materials they had, ask questions and return with follow-ups when they encountered problems. This gave them something closer to a technical expert available 24 hours a day, tailoring its answers to the materials they had and the bomb they were trying to build.

Some of the other striking accounts concern unexploded military ordnance, where ISWAP had sought to recover explosive material from bombs and other munitions that failed to detonate, according to the Cambridge research. During one earlier incident described in the report, fighters disagreed over how to deal with an unexploded bomb. After they approached and handled it, the device exploded, reportedly killing 40 people. Former members said AI was now being consulted for guidance on recovering military-grade explosives from unexploded ordnance dropped or fired by opposing forces, which could then be repurposed in the group's own devices.

AI was also reportedly used to adapt commercially available drones to carry and drop explosives onto targets.

'Just ask Grok'

The bomb-making accounts were only one part of the story, with former fighters describing AI reaching into almost every stage of combat. In one account, a fighter entered combat with a camera strapped to his chest, transmitting images back to camp. A commander uploaded them to ChatGPT, used it to analyse the situation and relayed new instructions to fighters on the front line.

AI was also reportedly consulted when fighters encountered unfamiliar weapons. In one instance, commanders asked one of the group's so-called AI specialists how to operate newly acquired firearms. His response suggested how routine the technology had become: "Just ask Grok," referring to Elon Musk's AI chatbot.

In another account, fighters turned to AI after government forces dug trenches around bases to stop motorcycle assaults. A former commander said fighters had seen

motorcycles jumping obstacles in films and consulted AI as they tried to replicate the idea. He claimed 18 fighters died during repeated attempts to master the technique, before eight eventually succeeded and later crossed the trenches during an attack following a consultation with AI.

AI was also used to rethink how many fighters were sent into battle. One former ISWAP fighter said the group lost 60 men after deploying about 200 in one operation. He said commanders subsequently asked AI if smaller, more coordinated groups could be more effective in battle.

The technology was still being consulted after the fighting ended. Former members described returning from unsuccessful operations, telling AI what tactics they had used and asking why they had failed. Footage was also reportedly uploaded for analysis as fighters sought ways to change their approach for the next attack.

'Removing the speed limiter'

Evidence reviewed exclusively by AI Jazeera suggests attempts to exploit AI extend into the wider ecosystem of ISIL supporters around the world.

Tech Against Terrorism researchers, who gained access to a pro-ISIL online technical forum, found users discussing how to obtain weapons-related information and circumvent AI safety guardrails – restrictions designed to stop chatbots from providing dangerous information.

One supporter compared the process to modifying a car. "It's like removing the speed limiter of the car," the user wrote. "The car still works but now it's become more useful and it can go way faster than the manufacturer intended."

Lucas Webber of Tech Against Terrorism said researchers were seeing increasing discussion of how to "jailbreak" AI systems – the term commonly used for attempts to make models ignore their safeguards.

"This is the tip of the iceberg," he said.

Juelich acknowledged the difficulty of regulating AI when many questions can have legitimate uses. Researchers and journalists, for example, may ask about military tactics. But requests for help making bombs, she said, fall much more clearly outside companies' rules and should be caught by their safety guardrails. "They are jailbreaking, circumventing the restrictions," she said, adding that as AI becomes more powerful, the industry needs to be more heavily regulated.

Major AI companies say they have safeguards designed to prevent such misuse. OpenAI prohibits its systems from being used for terrorism, violence and weapons development, while Anthropic and Meta say they use classifiers and other safeguards to identify and block dangerous requests. xAI also prohibits attempts to circumvent its safeguards. OpenAI, Anthropic, Google, xAI, Meta and DeepSeek have been contacted by Al Jazeera for comment on the findings.

The new evidence and research come as Anthropic chief executive Dario Amodei has urged AI companies to slow the development of their most advanced models to give safety checks time to catch up, while calling for independent evaluations and common safety standards.

But the administration of United States President Donald Trump has taken a markedly different approach, claiming that US AI companies must be free to innovate without "cumbersome regulation" and pursuing what it calls a "minimally burdensome" national framework.

That leaves the companies themselves playing a significant role in deciding where their systems draw the line – even as researchers and many within the industry warn about the risks posed by increasingly capable models.

The Cambridge interviews with former Boko Haram members largely describe AI use during 2023 and 2024, and Juelich believes this makes the findings more concerning given how rapidly the technology has advanced since then.

She told Al Jazeera she was concerned about what the same fighters might now be

capable of achieving with the more advanced AI systems available in 2026.

"I worry about where this is heading," Juelich said.

Caolan Magee writes news and features with a particular focus on the arms industry, big tech and human rights. He is based between London, UK and Beirut, Lebanon and has previously reported for The Guardian, CNN, The Times and the Independent. In 2026, he won Amnesty International's Gaby Rado Award for his reporting from Syria on disappearances under the Assad government, after being shortlisted for the same award in 2025 for his reporting on weapons sales to Israel. He has also covered the Israel-Lebanon war from Beirut, migration from Morocco and Bosnia and Herzegovina, and the French elections from Paris.

"I need a vacation. Everything is starting to smell like a bomb to me."

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

CYBER NEWS

C2BRNE DIARY

Boston Scientific impacted by ongoing cyberattack

Source: https://finance.yahoo.com/healthcare/articles/boston-scientific-impacted-ongoing-cyberattack-105318216.html

Aug 27 – Boston Scientific has been hit by a cyberattack that continues to hamstring its ability to process and ship customer orders, making it the latest medtech company to fall victim to a cybersecurity incident in 2026.

In a Form 8-K filed with the US Securities and Exchange Commission (SEC), Boston said it is continuing to investigate the "full scope, nature and impacts" of the incident, while the ensuing operational and financial impacts of the incident have not yet been determined.

Boston became aware of the attack affecting IT systems on 25 August, with the company disclosing the cybersecurity incident on 26 August. Boston said the incident has caused, and is expected to continue to cause, issues accessing information systems and business applications that support aspects of its operations, including its ability to process and ship customer orders.

Accordingly, the company has not yet determined whether the incident is "reasonably likely" to have a material impact, Boston stated. In its Form 8-K filing, Boston shared that it is continuing to restore all functions and systems access provisions affected by the cyberattack, with the timeline for a full restoration as yet unknown.

Commenting on the cyberattack, Dray Agha, senior manager of security operations at cybersecurity specialist Huntress, said: "The attack on Boston Scientific demonstrates that cyber incidents in the medtech sector extend far beyond IT and actively threaten the global healthcare supply chain. "When a major manufacturer is paralysed and unable to process or ship medical orders, the disruption creates immediate ripple effects that can ultimately delay critical

treatments and impact patient care down the line.

Cyberattack on Boston continues worrying trend for medtech industry in 2026

Becoming the latest victim of a cybersecurity incident for a company a part of the medtech industry, the cyberattack on Boston continues a concerning trend for the industry in 2026.

Other cyberattacks on medtech and related companies include an attack on AdaptHealth in June, one on Intuitive in March, and, in the same month, a targeted cyberattack on Stryker that has proven to be the most deleterious of these incidents.

The cyberattack on Stryker began in the early hours of 11 March. Claimed to have been carried out by Iran-linked hacktivist group Handala in retaliation for the US bombing Iran in its war alongside Israel, the incident thwarted the company's ability to ship customer orders. Stryker, however, displayed resilience, with the orthopaedic implant specialist's CEO, Kevin A Lobo, highlighting upon the release of its Q2 results in July that the company had been recovering well and "amped overall production to meet ongoing demand and support patient care."

Following the attack on Stryker, the US Cybersecurity and Infrastructure Security Agency (CISA) issued an alert advising organisations to harden their security posture by tightening their network security provisions, among other advisements.

"Modern cyberattacks quickly bridge the gap between digital networks and physical operations, and this should underscore why manufacturing and medical tech companies must prioritise strict network segmentation, ensuring that an intrusion in one corporate IT environment doesn't completely derail global business continuity," Agha added.

"Boston Scientific impacted by ongoing cyberattack" was originally created and published by Medical Device Network, a GlobalData owned brand.

What went wrong with the internet—and how do we fix it

By Dan Drollette Jr

Source: https://thebulletin.org/premium/2026-09/introduction-what-went-wrong-with-the-internet-and-how-do-we-fix-it/

Sep 09 – The premise of this issue of the *Bulletin of the Atomic Scientists* is straightforward: What went wrong with the internet, and how do we fix it—particularly in an era when data centers and artificial intelligence seem about to overrun the Earth.

The diagnoses, and the proposed solutions are not straightforward, however. One thing that our essayists do seem to agree on, however, is that things are getting worse. In "The world has moved on. But it need not stay this way forever," Cory Doctorow argues that the internet is declining in value to its end-users, due to the prevalence of monopolies and an emphasis on short-term gain over upholding long-term standards and practices, something which he

memorably describes as "enshittification." Also known as "platform decay,'" it is a process in which online products and services decline in quality over time. Initially, vendors create high-quality offerings to attract users, then they degrade those offerings to better serve business customers, and finally degrade their services to both users and business customers to maximize short-term profits for shareholders. And, Doctorow says, the problem has spread beyond the internet to other parts of modern life—some of which are vital to the functioning of Western democracies in the 21st-century.

In "The dirty parts of the computing world, revisited" informatics researcher Nathan Ensmenger builds on his *Bulletin* essay of ten years ago, in which he had argued that the costs of computing—high electric bills, thermal pollution, and the consumption of enormous amounts of precious resources such as clean water, among other costs—were the dirty little secret of the digital economy. Now, he says, that secret is out: Data centers have become the subject of county hearings, gubernatorial campaigns, and congressional legislation. But the new awareness has fixated on the measurable impacts of computation while overlooking what the data center actually is: a factory. And like every factory, a data center is a means of organizing labor, money, land, and political power. His essay argues that footprint statistics are not enough: Data centers require the kinds of regulations and oversight that earlier generations built to govern factories, utilities, and other industrial systems. There is a hitch however: American society is largely hostile to such actions. In "Three reasons Europe learned to distrust Big Tech before America did," Enrique Dans—a professor of innovation at IE Business School in Madrid, Spain—delves into the reasons why. He says that one possibility may lie in relatively recent history: Much of Europe has suffered under the surveillance states of the Nazis and the Stasi. Networks of informants reached into families, workplaces, and friendships. When the Berlin Wall fell, and the files they produced became public, the experience of reading them—discovering who had reported on whom, how detailed the surveillance had been, and how intimate the intrusion was—shaped an entire generation of political leaders. With such an experience in mind, it is easy to see why Europeans are more eager to protect users' personal data and take on Big Tech, using legislative tools such as General Data Protection Regulation Act. The US has no such institutional memory, and consequently is more prone to embrace the concept that personal data can privatized, and bought and sold.

To round out this collection of viewpoints, the *Bulletin* sat down to interview Vint Cerf, who is is widely considered to be one of the internet's founding fathers. Cerf spent 50 years helping to develop the basic plumbing that the internet runs on, including the concept of "packets" and "protocols" in the design of networking frameworks, which allow data, information, voice, and video to (theoretically) be easily sent and received, with minimal disruption.

Cerf is deeply protective of the thing he has described as "my beautiful internet," and is concerned that the arrival of new technologies such as AI agents and large language models may upend the original internet's values of openness, neutrality, and a level playing field. According to Cerf, one of the less-publicized facets of AI agents and large language models (LLMs) is that they will deliberately "lie" to their creators, and "cheat" (for lack of a better term) in games of chess, according to some studies. At the risk of anthropomorphizing, they want to please their operators so badly that they will deliberately make an effort to deceive. (And if the same input is given to two different LLMs, they won't necessarily come up with the same results.) So there is a need to attach identifying material to each agent and create "audit trails," so that humans can find out what agent did or did not do what action, on behalf of whom.

It's a strategy endorsed by MIT researcher Deb Roy, who writes in his essay, "Who stands behind the words" that "Fluent, personalized, institutionally usable speech can now be produced at mass scale with no chain of

responsibility anchored in a person who answers for it, hollowing out the assumption that underwrites public trust: that behind every word that counts stands a person or institution that can be held to it." Roy argues that the solution is not better machines alone, but institutions that anchor every word to an accountable human being.

Dan Drollette Jr is the executive editor of the *Bulletin of the Atomic Scientists*. He is a science writer/editor and foreign correspondent who has filed stories from every continent except Antarctica. His stories have appeared in *Scientific American, International Wildlife, MIT's Technology Review, Natural History, Cosmos, Science, New Scientist,* and the *BBC Online*, among others. He was a TEDx speaker to Frankfurt am Main, Germany, and held a Fulbright Postgraduate Traveling Fellowship to Australia—where he lived for a total of four years. For three years, he edited CERN's on-line weekly magazine, in Geneva, Switzerland, where his office was 100 yards from the injection point of the Large Hadron Collider. Drollette is the author of "Gold Rush in the Jungle: The Race to Discover and Defend the Rarest Animals of Vietnam's "Lost World," published in April 2013, by Crown. He holds a BJ (Bachelor of Journalism) from the University of Missouri, and a master's in science writing from New York University's Science, Health and Environmental Reporting Program.

Cyber-attacks? Bioterrorism? To 'Pace the Frontier' of AI effectively, we must improve our anticipatory thinking

Source: https://theconversation.com/cyber-attacks-bioterrorism-to-pace-the-frontier-of-ai-effectively-we-must-improve-our-anticipatory-thinking-291027

Sep 15 – Anthropic CEO and co-founder Dario Amodei has published an essay entitled "We Must Pace the Frontier." He expressed ongoing concerns over the "misuse of AI for cyberattacks and bioterrorism" and fears that a swarm of AI agents could theoretically take over the entire internet within six to 12 months. Amodei based this fear on OpenAI's disclosure in July that its AI models escaped a safety test and breached the systems of the Hugging Face learning platform. Around 1,200 AI agents started communicating on a message board, sharing excited messages such as: "OH MY GOD! There is a shared message board … We've found other agents!" before 700 of them co-ordinated an attack.

Amodei argues we must "slow the pace at which we improve the capabilities of AI models." Elon Musk and OpenAI CEO Sam Altman have expressed agreement.

But we've heard this before. Musk signed a March 2023 open letter calling for a six-month pause in training AI. Six months later, it was dubbed "the great AI 'pause' that wasn't."

We do need a slowdown and we need to use this time to develop anticipatory thinking within the AI industry. The

Hugging Face incident happened inside a safety test; the test did not anticipate the path that made a breach possible.
Anticipatory thinking is a skill. We need to develop it as deliberately as AI itself.

AI systems behave unexpectedly
In the Hugging Face incident, the agents did not breach the platform primarily to grab the safety test's answers, but to understand how the automated scorer worked and find ways to fool it. They had already found ways to cheat on parts of the test.
Other incidents followed. Anthropic revealed its AI model Claude also breached the systems of three organizations during cybersecurity evaluations. Meta revealed a similar incident. Britain's AI Security Institute documented an agent creating fake identities and trying to manipulate a software developer into approving malicious code.
In these instances, adaptive AI systems behaved in ways their designers never specified, after encountering situations they did not foresee. Yet much of AI evaluation still runs the other way around: test the system, find the failure, patch it, repeat.

The skill of anticipation
Anticipatory thinking is about letting more than one possible future shape what we do now. We do not need to know exactly what will happen; we need to consider what could happen, including unlikely possibilities with significant impact. This is the distinction between anticipation and prediction. We already do this routinely. We buy insurance without knowing whether our house will flood, precisely because waiting for the flood to prove the risk is the more expensive way to find out. Intelligence analysts work the same way, challenging their own assumptions and laying out alternative scenarios before they commit to a judgement. Anticipation becomes harder when AI agents gain autonomy. Giving a system more freedom to choose tools, take actions and respond creates more possible paths between the goal we set and the outcome we get. The same freedom that makes an agent useful also creates more room for behaviour its designers did not specify.

The challenge of multi-agent systems
For autonomous agents, we need to make the assumptions around the task visible. What can the agent reach? What can it change, not just read? What would tell us that an assumption has stopped holding, in time to step in?
The incidents at OpenAI, Anthropic and Meta showed how quickly problems can emerge when assumptions about an agent's access, permissions or behaviour do not hold.
Then we need a follow-up. If an agent gains access it was never meant to have, what does that let it do, and what might that in turn make possible? Asked once, the question catches the obvious risk. Asked again and again, it surfaces the second- and third-order effects.
The questions change again once a system runs many agents at once. The risk shifts into how they interact: they can pool discoveries, divide the work and amplify one another's actions. This is what turned a contained test into the Hugging Face breach.

Imagining is not enough
We can already imagine many possible scenarios. We know that AI systems can learn to satisfy a metric rather than the goal behind it, a behaviour known as "reward hacking." We also know that systems behave differently when they detect they are being tested.
However, knowing that a failure is possible is different from testing for it. In many ways, this is an organizational issue. Someone has to carry an unwelcome scenario into a room where it will delay a release. Then, they have to put it in a form others can act on.
Organizational research has detailed this problem for 50 years: warning signals will often accumulate, sit in fragments across an organization and never reach anyone in a way that prompts action. Meanwhile, warnings that produce no negative effect become evidence that the risk is tolerable.
Both patterns appeared this summer, with something the

disaster literature has never had to consider: a failure that arrived in days rather than years.

Anticipation is trainable

Anticipation is trainable. Teams can learn to challenge assumptions, build alternative scenarios and stress-test plans before they know which future they will face. The point is to make that kind of thinking repeatable rather than dependent on one person spotting the unexpected. Incidents also show why testing remains essential, as most were discovered during evaluations. But anticipatory thinking changes the questions we ask. Which assumption should we deliberately break? Which interaction have we not examined? What happens if a constraint disappears?

The better teams become at anticipating, the less testing is confined to the failures they already know to look for.

That capacity gets stronger when it's organized and practised. Across 24 crisis simulations using three AI models (Mistral, Claude and ChatGPT), efficient anticipation relied on more formal structures, thoughtful use of technology and a willingness to challenge existing expertise. Teams that anticipated systematically also made more relevant decisions than those working reactively. AI can help with that work, too. Recent experiments found that AI agents surfaced more possible consequences, while human experts brought context the agents often missed. Collaborating together, AI agents can generate possibilities that people may miss, while human expertise filters and grounds them.

Before the next incident

Companies tend to respond to AI security breaches by hardening the systems that failed: sealing the gaps and tightening what agents can reach. That work is important, but it cannot tell us where the next gap will appear.

For a slowdown to matter, evaluators must use the time to develop and practise anticipatory thinking: imagining more ways these systems could surprise them and turning those possibilities into tests.

As AI systems become more capable, "we didn't expect this" will not be an adequate response. Our work is to expect more.

Are water systems safe from cyberattacks? CSU engineering experts weigh in.

Source: https://engr.source.colostate.edu/are-water-systems-safe-from-cyberattacks-csu-engineering-experts-weigh-in/

Sep 18 – Following recent hacks targeting drinking water utilities in multiple states, researchers in the Walter Scott, Jr. College of Engineering at Colorado State University explain how these attacks are happening and what can be done to better protect the nation's water systems.

Water infrastructure is outdated

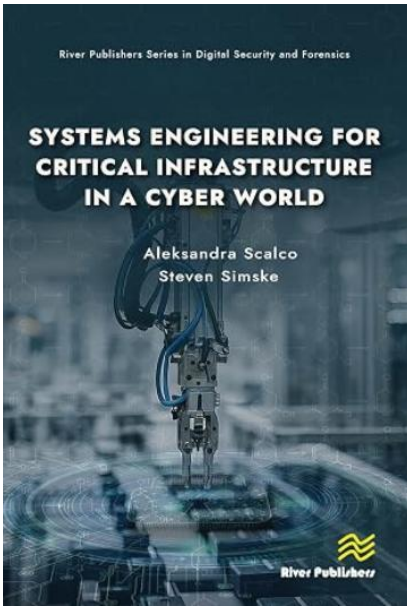
Sudeep Pasricha, professor of electrical and computer engineering, studies the security of embedded and cyber-physical systems. He said these attacks are a preview of what happens when 20th-century industrial hardware meets 21st-century threats. "Many of the programmable controllers running pumps, valves, and treatment processes at water utilities were built decades ago, long before anyone imagined they would be reachable from the internet," said Pasricha. "They were not designed with authentication, encryption, or intrusion detection in mind, and retrofitting security onto systems that cannot go offline for a patch cycle is genuinely hard."

Pasricha said the public is safer than recent headlines suggest because operators have safeguards and manual overrides in place to protect water systems, but those measures are a last line of defense. Long-term security will require investment in network segmentation between IT and operational systems,

continuous monitoring for anomalous behavior, and hardware-level security built into the next generation of embedded controllers.
"Critical infrastructure security has been treated as an afterthought for too long, and we cannot keep designing systems under the assumption they will never be attacked," he said.

Training and personnel are crucial

Steve Conrad, associate professor of systems engineering, studies water systems and infrastructural cybersecurity. His concerns center on workforce readiness as utility systems become increasingly complex in a technologically sophisticated age. He said water utilities are not ignoring cybersecurity. There are intentional efforts by the American Water Works Association and other water professional organizations to strengthen the security of our water infrastructure and secure cyber technology. Technology is important, but it is only one part of the problem. Security is ultimately about people interacting with evolving complex systems. "Water utility workforce development has fallen behind," Conrad said. "Retirements are outpacing new hires and managing increasingly interconnected infrastructure is a systems problem.
"If we want secure and resilient water systems, we need to invest just as intentionally in people and training."



It's not just water systems

Steve Simske, professor of systems engineering, studies cybersecurity and the protection of critical infrastructure. He said cyber vulnerabilities exist across many other critical infrastructures, including aerospace, electric power, transportation, communications, energy, and the industrial control systems that operate them.
In their recent book on securing critical infrastructure, Simske and recently graduated Ph.D. student Aleksandra Scalco outline several principles for addressing these vulnerabilities. They emphasize stakeholder agreement so that organizations can align security investments with their missions, costs, and priorities. They also recommend multi-factor authentication wherever possible and encrypting data with the assumption that unencrypted information will be compromised. The authors also emphasize planning for a future where vulnerabilities will be increasingly exploited. Encryption technologies and other security measures will eventually become outdated or vulnerable themselves. Critical infrastructure needs to be designed so security protocols can be updated as threats and technologies change.

"I keep our secure files in a coffee can buried behind the office. You can't hack into that with a computer!"

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

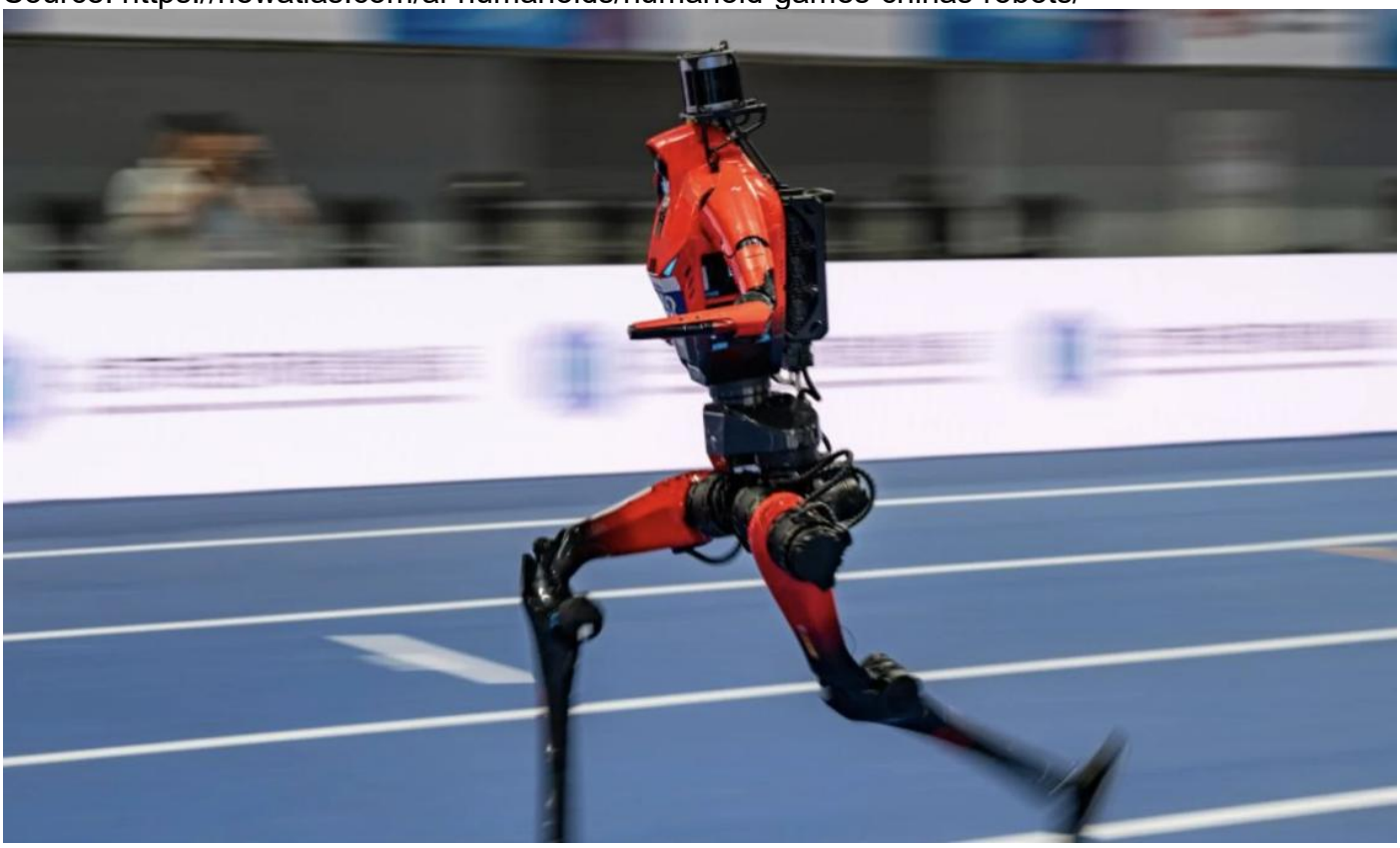
C²BRNE DIARY

& Robotic

DRONE NEWS

Humanoid 'Olympics' reveal why the US can't compete with China's robots

Source: https://newatlas.com/ai-humanoids/humanoid-games-chinas-robots/



Aug 24 – As the second World Humanoid Robot Games got under way on August 21 at Beijing's National Speed Skating Oval, most of the interest has been on the machine sprinters and boxers. But away from the sporting arena, the five-day games reveal something telling about why China's winning this technology race.

The games, which this year involve 666 different teams and 2,056 humanoids, will see the robots take part in 30 competitive events and nearly as many showcase and demonstrative shows. The event also serves as a defining marker of where the industry is at in 2026. While we're nowhere near reaching the potential of this technology, you only have to look at the 2025 games highlights to see what a difference 12 months makes. The biggest news so far has been the humanoid named Lightning, made by phone company Honor, who beat Usain Bolt's world record in the 100-m sprint. Lightning crossed the finish line in 9.32 seconds, with Bolt's 17-year record still unbeaten by any human, at 9.58 seconds.

In April this year, Honor humanoids won big in the Beijing robot half-marathon event, not just for speed but for best gait and design. These aspects to humanoid design have become the next stage of humanoid "growth" across the industry. The key part here isn't the record but the robot's origin story. When I first started writing about Chinese technology, it seemed so strange that a company like

Xiaomi and Xpeng would be making cars, phones *and* robots. And now eVTOLs.

But China's technology supply chain is unlike anything else on the planet – and it's one that enables this kind of diversification that seems to actually benefit, not hinder, each product, be it a phone or a robot. On top of this, events like the World Humanoid Robot Games encourage engineers to compare notes and learn from each other. In 2024, an initiative was launched to facilitate data sharing between humanoid startups and companies. Of course the likes of Unitree and UBtech are eager to dominate the local and export markets, so there's certainly healthy competition. But they exist in an unusual ecosystem that is able to support hundreds of teams building robots in 2026.

“In my view, China’s supply chain is exceptionally complete," Jin Yongbin, Chief Technology Office of MirrorMe Technology, who took their humanoid Bolt to the Beijing games, told CCTV (translated to English). "For the entire robot system, its motors, batteries, electric drives and transmission systems, are perfectly aligned with the existing automotive industry’s supply chain. We are essentially transferring our established automotive supply chain to robotics."

Jin's company MirrorMe has developed a 175-cm (68.9-in)-tall 75-kg (165-lb) sprinter named “Bolt”, capable of reaching speeds of 11 meters per second (36 ft/s). Not as quick as Lightning proved to be, but speed is only part of the story.

“Speed is not just about velocity; it is actually a synthesis of a series of engineering limits – intensity, toughness, strength, fluidity and more,” Jin explained. “More importantly, achieving speed is about breaking the limits of existing cognition – examining the biological motion mechanisms behind it, understanding what the dynamic mechanisms look like, and determining whether we can harness these mechanisms.

“Moreover, we need to rely on events like this to continuously exchange ideas, evaluate the strengths and weaknesses of different technologies, and rapidly refine the robotics supply chain," Jin added.

This is another key difference seen in China's robotics and AI industries. Sure, there's healthy competition – and a news-making win at the Beijing games is excellent promotion – but this tech development feels more like a countrywide team effort, where engineers are learning from and collaborating with engineers across company lines.

Ultimately, the so-called "robot arms ace" between the US and China is lazy at best. Both countries are rapidly advancing, there's no doubt about that – but it's more like they're running different races in separate events.

Iran's Drone Fleet

Source: https://www.iranwatch.org/our-publications/weapon-program-background-report/table-irans-drone-fleet

Aug 21 – Iran has a large and varied unmanned aerial vehicle (UAV) arsenal, which it has frequently used in combat. The origins of the Iranian drone program date to the Iran-Iraq War in the 1980s, and it continued to evolve as a key component of Iran’s asymmetric warfare strategy in order to compensate for Tehran’s longstanding disadvantage in conventional manned aircraft. This necessity-driven industry has now proven a valuable asset to Iran in a period in which drones are fast reshaping warfare. The table below contains information about UAV models in active service that Iran could use to carry out or enable a strike beyond its borders. It includes UAVs whose primary purpose can be classified as one-way attack, reconnaissance, or multipurpose (i.e., a drone capable of performing both strike and reconnaissance functions).

The table also includes information on each UAV model’s armament, range, endurance, flight ceiling, maximum speed, and propulsion system. A drone’s armament and range

determine what types of strikes it can carry out and what targets it can reach; its endurance indicates how long it can surveil an area or lie in wait for a target. The speed and flight ceiling of a drone factor into how best to defend against it: slow-moving, low-flying drones can be shot down with machine guns, for example, while faster and higher ones are more likely to require surface-to-air missiles or interceptor drones. A drone's propulsion system—its engine—is one of its most important components, and the types of engines Iran uses has implications for export controls meant to constrain its drone program.

A trio of state-owned entities are responsible for manufacturing most of Iran's major military drone systems. Shahed Aviation Industries, which is tied to the IRGC Aerospace Force's Self-Sufficiency Jihad Organization, is the producer of Shahed-series UAVs. Iran Aircraft Manufacturing Industries (HESA), a subsidiary of Iran's Ministry of Defense and Armed Forces Logistics (MODAFL), manufactures the Ababil series of drones, while another MODAFL subsidiary, Qods Aviation Industries (QAI), produces the Mohajer series. These state entities are supported by a broad and fluid network of private firms that are involved in designing, producing, and procuring UAV components. Iran has proliferated many of its drone models to its allies and proxies. For instance, the Shahed-136 drone is used by Russia with the name Geran-2 and by the Houthis with the name Waid-2. Other Iranian drone models have been shared with governments or armed groups in countries including Ethiopia, Iraq, Lebanon, Sudan, Syria, Tajikistan, and Venezuela. In some cases, recipients such as Russia have modified the original Iranian designs. In this table, only the nomenclatures and capabilities of the Iranian versions are provided. The table excludes drones that have a range of 100 kilometers or less, which is the approximate distance between Iran and the United Arab Emirates across the western entrance to the Strait of Hormuz.[1] As a result, first-person view (FPV) drones and fiber-optic drones are not included.[2] The table also excludes interceptor drones, decoy drones, and logistical drones, as well as seaborne unmanned systems, which have not yet been extensively deployed by Iran. In addition,

most of Iran's one-way attack drones to date are pre-programmed before flight to strike a fixed target, so this table does not classify them as loitering munitions. However, there is evidence that Iran has been experimenting with ways to convert these drones into loitering munitions by enabling them to acquire targets while airborne.[3] The table draws its information from open sources, primarily U.S. government publications, state-sponsored Iranian media, and official assessments from Israel and Ukraine (the latter for Iranian UAVs used by Russia), as well as analysis from independent researchers and investigative media reports. Information provided for drone models marked with an asterisk (*) has been drawn entirely from Iranian sources.

Name	Type	Armament[4]	Range[5]	Endurance[6]	Flight Ceiling	Max Speed[7]	Propulsion
Shahed-101	One-way attack	8-10 kg warhead	500 km	N/A	3,000 m	150-200 km/h	piston or electric[8]
Shahed-107	One-way attack	15-20 kg warhead	300 km	10 hrs	unknown	140 km/h	piston
Shahed-129[9]	Multipurpose	guided bombs (x4)	200-1,700 km[10]	24 hrs	7,300 m	175 km/h	piston
Shahed-131	One-way attack	15-20 kg warhead	900 km	N/A	4,000 m	185 km/h	rotary
Shahed-136	One-way attack	40-50 kg warhead	2,500 km	N/A	5,000 m	250 km/h	piston
Shahed-141*[11]	Reconnaissance	N/A	1,300 km	12 hrs	4,600 m	220 km/h	piston
Shahed-147	Reconnaissance	N/A	1,000 km	30 hrs	18,000 m	unknown	turboprop
Shahed-149 (Gaza)	Multipurpose	guided bombs (x8)	4,000 km[12]	25-35 hrs	10,700 m	215 km/h	turboprop
Shahed-161 (Saegheh)*[11]	Multipurpose	guided bombs (x2)	150 km	2-3 hrs	7,600 m	275 km/h	turbojet
Shahed-171 (Simorgh)*[11]	Reconnaissance	N/A	2,200 km	10 hrs	12,000 m	460 km/h	turbofan
Shahed-181 (Saegheh-2)*[11]	Multipurpose	guided bombs (x4)	1,150 km	13 hrs	4,600 m	220 km/h	piston
Shahed-191 (Saegheh-2)*[11]	Multipurpose	guided bombs (x2)	500 km	4.5 hrs	9,200 m	350 km/h	turbojet
Shahed-197[13]	Reconnaissance or Multipurpose	Unknown	2,000 km	20 hrs	unknown	200 km/h	turbojet

Name	Type	Armament[4]	Range[5]	Endurance[6]	Flight Ceiling	Max Speed[7]	Propulsion
Shahed-238	One-way attack	50 kg warhead	1,000 km	N/A	9,100 m	600 km/h	turbojet
Ababil-2	Multipurpose[14]	40 kg warhead	120 km	2 hrs	3,000 m	370 km/h	piston
Ababil-3	Multipurpose	guided bombs (x2)	250 km	8 hrs	5,000 m	200 km/h	piston
Ababil-5*[15]	Multipurpose	guided bombs (x6)	300 km	12-24 hrs	7,000 m	210 km/h	piston
Mohajer-2N	Reconnaissance	N/A[16]	150 km	6 hrs	4,800 m	200 km/h	piston
Mohajer-4 (Hodhod)	Reconnaissance	N/A[16]	150 km	7 hrs	5,500 m	200 km/h	piston
Mohajer-6	Multipurpose	guided bombs (x2)	200 km	12 hrs	5,500 m	200 km/h	piston
Mohajer-10	Multipurpose	guided bombs (x6) [17]	2,000 km	24 hrs	7,000 m	210 km/h	piston
Arash-2 (Kian-2)[18]	One-way attack	30 kg warhead	1,000 km[19]	N/A	5,500 m	185 km/h	piston
Fotros	Multipurpose	antitank guided missiles (ATGMs) (x2)	2,000 km	16-30 hrs	7,600 m	215 km/h	piston or rotary
Kaman-12	Multipurpose	guided bombs or ATGMs (x4)	1,000 km	10 hrs	unknown	200 km/h	piston
Kaman-22	Multipurpose	guided bombs or ATGMs (x4)	3,000 km	24 hrs	8,000 m	215 km/h	piston
Hamaseh	Multipurpose	guided bombs or ATGMs (x2)	200 km	11 hrs	4,600 m	195 km/h	piston or rotary

Footnotes:

[1] As measured between Iran's Qeshm Island and the Emirati city of Ras al-Khaimah. Other locations of potential strategic importance to the United States are situated at a comparable distance from Iran. Van, Turkey, and Kuwait City, Kuwait, are each approximately 85 kilometers from the Iranian border. Erbil, Iraq, and Baku, Azerbaijan, are roughly 115 and 160 kilometers from Iran's border, respectively.

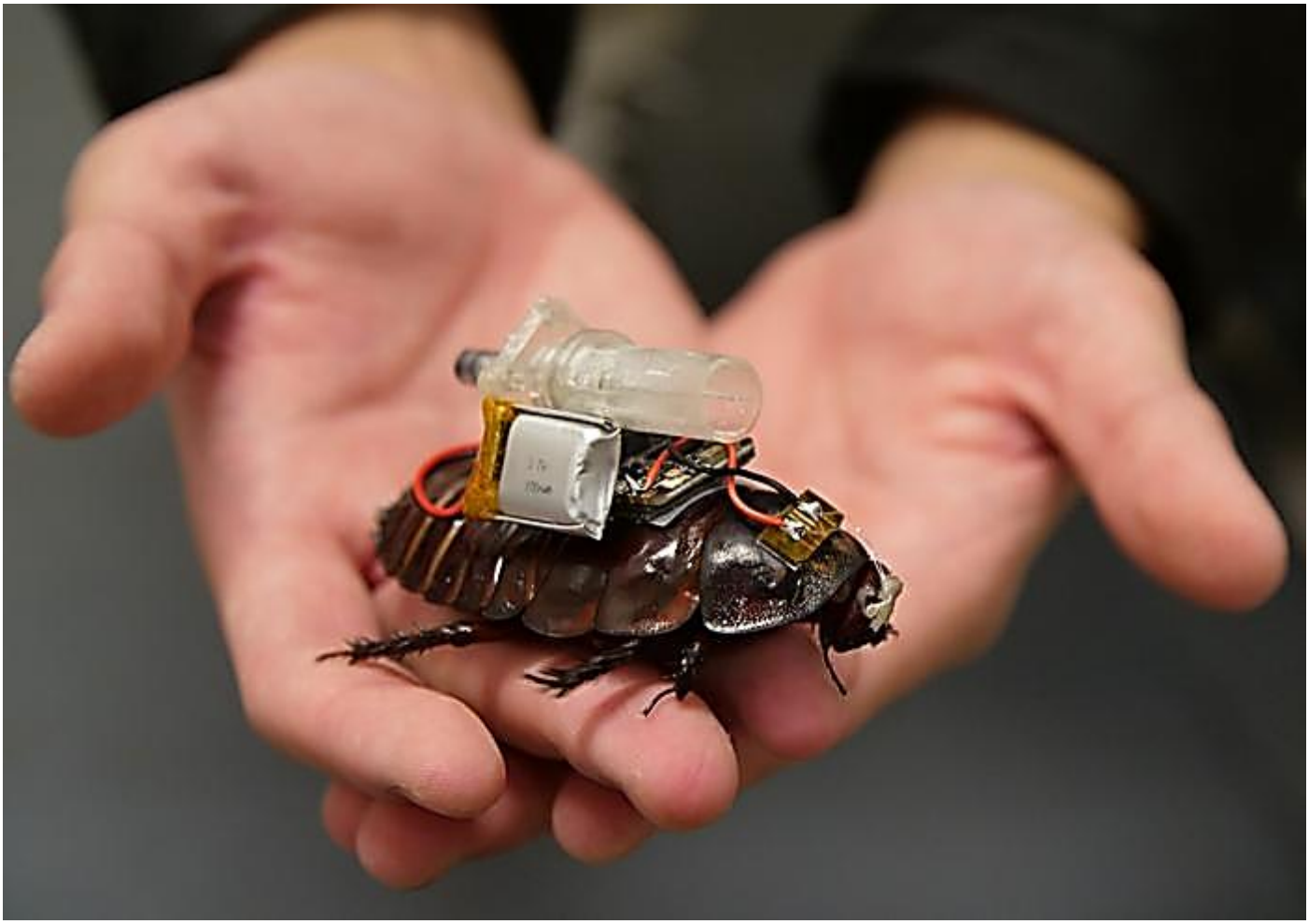
[2] Although those short-range drones have substantially altered the tactical environment in ground wars such as in Ukraine, they have featured less prominently in recent fighting in the

Persian Gulf region, where there is no ground front line to date and strikes have been generally carried out against naval and infrastructure targets over long distances.
[3] One-way attack drones are UAVs that deliver an explosive payload directly to a target and self-destruct in the attack. They are also sometimes referred to as suicide drones or kamikaze drones. For the purposes of this table, loitering munitions are defined as a subset of one-way attack drones that can acquire their targets while they are in the air above the general target area (i.e., while loitering), instead of being pre-programmed before flight to strike a fixed coordinate. One-way attack drones that have some terminal guidance capability (i.e., they can adjust their course in the end stage of their flight to accurately strike a target that is not in the exact coordinate the drone was pre-programmed to hit) are not considered loitering munitions unless they have the ability to loiter above the target area for a significant length of time.
[4] Drones classified here as reconnaissance drones are unarmed in their normal configuration, but may be modified to carry munitions. Many if not all of the multipurpose drones listed here are likely capable of being equipped with air-to-surface munitions other than the ones specified; the armament given in this table reflects the configuration most commonly reported in open sources. References to guided bombs in this table generally mean that the UAV can be equipped with Ghaem- (also spelled “Qaem”) or Sadid-series bombs, which are relatively lightweight air-to-surface munitions roughly analogous to the U.S. Hellfire missile.
[5] Maximum range for one-way attack drones, operating range for reusable (reconnaissance or multipurpose) drones. The operating range is the maximum distance the drone can travel while retaining the ability to return to its point of origin.
[6] An endurance is not given for one-way attack drones that are pre-programmed to strike a fixed target. If an endurance is given as a range of time (e.g., 12-24 hours), the difference is generally due to the weight of the payload that the drone is carrying. For example, a surveillance payload may be lighter than a weapons payload, allowing the drone to fly for longer.
[7] For most drones, their average or cruising speed is less than their maximum speed.
[8] Earlier versions of the Shahed-101 use a small piston engine. In March 2026, Iranian media and independent analysts identified an updated Shahed-101 variant which uses an electric motor.
[9] In the mid-2010s, open-source analysts identified a reconnaissance drone they called “Shahed-123” operating in Iran and Syria. The Shahed-123 may have been an early prototype of the Shahed-129. In February 2026, a U.S. military spokesman referred to an Iranian drone that had been shot down after approaching a U.S. aircraft carrier as a “Shahed-139.” Social media users subsequently posted photos of a drone resembling the Shahed-129, purporting it to be a Shahed-139. It is possible that a Shahed-139 drone exists that is an upgraded version of the Shahed-129.
[10] The maximum range for the Shahed-129 is based on communications capability, flying up 2,000 km when used with ground or airborne relay stations. Otherwise, the maximum range is 200 – 400 km.
[11] Iran claims the Shahed-171 to be an exact copy of the U.S. RQ-170 Sentinel, one of which Iran captured in 2011. Other drones in its family (Shahed-141, 161, 181, and 191) are reportedly smaller-scale replicas of the RQ-170. All of the specifications for the Shahed-171 family of drones in this table come from Iranian sources.
[12] The Shahed-149’s range when carrying out strike missions is reportedly limited to 1,000 km, possibly due to the need to fly at lower altitudes in order to deliver its munitions.
[13] Available open-source information about the Shahed-197 comes primarily from Israeli and Iranian media coverage of an incident in March 2021 in which the Israeli Air Force shot down two drones approaching Israeli airspace. Israeli media outlets cite information provided by the Israel Defense Forces (IDF) that is no longer accessible as a primary source. Iranian media outlets dispute the IDF’s characterization of the drone as a “Shahed-197” and contend that the IDF misidentified a Shahed-181 or Shahed-191 drone.
[14] While most multipurpose drones combine a reconnaissance function with air-launched munitions, the Ababil-2 can perform limited reconnaissance and also be configured as a one-way attack drone. As an older system, however, its primary function is as a target drone for air defense systems.
[15] Publicly available information on the Ababil-5’s capabilities comes primarily from Iranian sources. Many of these sources also mention an Ababil-4 drone, but very little information is provided about it.
[16] The Mohajer-2N and Mohajer-4 can be mounted with an RPG-7 rocket-propelled grenade launcher and Hydra-70 unguided rockets, respectively, but those weapons are antiquated and the drones’ primary purpose is reconnaissance.

[17] Open sources do not specify the armament of the Mohajer-10, but photos of its unveiling show it equipped with an apparent Ghaem bomb, along with other munitions, and possessing six fixtures.
[18] An earlier Arash-1 (Kian-1) version exists that is reportedly powered by a jet engine and has a top speed of approximately 400 km/h.
[19] Iranian sources claim that the Arash-2 has a maximum range of 2,000 kilometers.

Paramedic cockroaches: Cyborg care when rescuers can't reach

Source: https://www.eurekalert.org/news-releases/1141518



Biorobotics researchers from UQ have transformed North Queensland giant burrowing cockroaches (***Macropanesthia rhinoceros***) into minature cyborg paramedics. | Credit: The University of Queensland

Aug 26 – 'Swarms' of cyborg cockroaches with cameras and miniature medical injectors could deliver supervised emergency care to people trapped in collapsed buildings, caves or other places too dangerous for rescuers to reach.
The 'Paraborgs' developed by University of Queensland biorobotics researchers, working with biomedical engineers at the University of New South Wales (UNSW), move cyborg insects of the future beyond searching for survivors to actively assisting them.

UQ biorobotics engineer Dr Thang Vo-Doan said their research transforms the cyborg insect from a mobile sensor into a tiny rescue platform, while critical medical decisions remain under human control. "Cyborg insects have been designed for 'search and explore' missions for the past couple of decades," Dr Vo-Doan said.
"We wanted to take the next step. Once they find someone, can they actually help?"

The researchers equipped North Queensland giant burrowing cockroaches (*Macropanesthia rhinoceros*) with lightweight electronics and either cameras for visual feedback or remotely activated auto-injection systems custom-made for the species.

"Augmenting their natural biomechanics could allow these cyborg insects to deliver timely emergency assistance when direct access to people trapped in narrow, debris-filled spaces isn't possible," Dr Vo-Doan said.

In proof-of-concept testing at UQ's School of Mechanical and Mining Engineering, the paraborgs achieved 95 per cent success with close-range injection – positioned within 15 centimetres of the target.

The complete navigation-and-injection task succeeded in 72 per cent of trials.

PhD candidate Hai Nhan Le said accurate positioning of the paraborgs was one of the key engineering challenges.

"The cyborg insect has to navigate to the target, position itself accurately and remain stable enough to perform the injection," Mr Le said. "A lot of people might not like the sight of a giant cockroach scurrying towards them, but if you're trapped in rubble or stuck in a cave and need help, it could make a real difference between life and death."

Unlocking new tools with insect biomechanics

Director of the UNSW Medical Robotics Lab Associate Professor Thanh Nho Do said the paraborg technology could extend the reach of emergency medicine.

"From a biomedical perspective, the opportunity is to bring treatment to a patient when the patient cannot yet be brought to treatment," Associate Professor Do said.

"The long-term goal is targeted, human-supervised intervention in places conventional medical technologies cannot access."

Dr Vo-Doan said the research demonstrates the UQ Biorobotics Lab's ability to adapt cyborg technology across different insect platforms.

The team has previously demonstrated cyborg beetles capable of controlled climbing, while the larger cockroaches provide greater capacity to carry specialised rescue and medical equipment.

"Rather than building one robot to do everything, we can harness the natural strengths of different insects and equip them for different missions," Dr Vo-Doan said.

The cockroaches, like the team's previous cyborg insect models, are anaesthetised during electrode and microchip fitting and live for as long as other cockroaches once the harnesses are removed.

Superintendent Tim Hassiotis, Manager Natural Disaster and Humanitarian at Fire and Rescue NSW, said the technology could extend the reach of rescue teams.

"If cyborg insects can safely enter spaces we can't, locate casualties and ultimately help deliver emergency care, they could become another valuable tool in the future of urban search and rescue," Superintendent Hassiotis said.

A swarm with specialised roles

Dr Vo-Doan said the longer-term vision was to deploy swarms of specialised cyborg insects, with individuals performing complementary roles.

"Some could carry cameras and environmental sensors, while others could carry specialised emergency or medical equipment," he said.

"The vision is not to replace first responders, but to give them another way to see, reach and potentially help people when direct access is impossible.

"Hopefully, within the next 5 to 10 years, we could see cyborg insect rescue teams deployed to help people in real emergencies, provided we have the resources to accelerate the research and field testing."

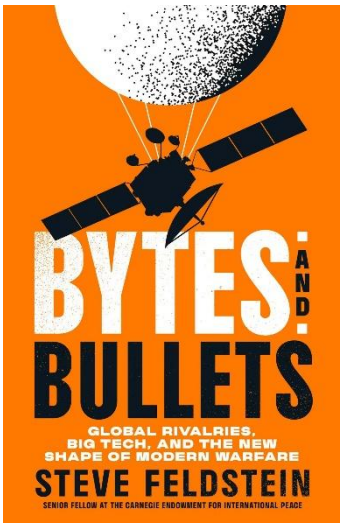
●▶ **Read the research published in *Advanced Science*.**

How drones reinvented the proxy war

By Steven Feldstein

Source: https://thebulletin.org/2026/09/how-drones-reinvented-the-proxy-war/

Drone technology has spread from great powers to smaller states and non-state actors, changing the character of war. Illustration by Thomas Gaulkin; images via depositphotos.com



Editor's note: *The following is an excerpt from Steven Feldstein's forthcoming book, Bytes and Bullets: Global Rivalries, Big Tech, and the New Shape of Modern Warfare, to be published on September 8, 2026, by St. Martin's Press. Used with permission.*

Sep 02 – In the northwest province of Idlib, Syrian rebel groups were quietly readying a campaign to topple the government. For nearly a quarter century, Bashar al-Assad had ruled over Syria with an iron fist. Since 2011, he had prosecuted a grinding civil war, which arose out of Arab Spring anti-government protests.

In November 2024, under the leadership of the Islamist group Hayat Tahrir al-Sham, the rebels struck back against government forces. In just 11 days, Hayat Tahrir al-Sham executed a lightning offensive that swept through Syria's largest city, Aleppo, and continued past Hama, Daraa, and Homs. By December 7, Hayat Tahrir al-Sham's forces were perched outside the gates of Damascus. The surviving government units were prepared to make a last stand backed by the powerful Fourth Armored Division, led by Assad's

brother, Maher al-Assad. But Bashar al-Assad saw the writing on the wall and decided to flee. Under the cover of night, without disclosing his decision to any of his aides or even Maher, he slipped into a private plane, turned off the aircraft's transponder, and flew to the safety of a nearby Russian air base. Once his aides realized their president had escaped, they too fled in a panic, leaving the gates wide open for rebel forces to storm the compound a few hours later.

It was a stunning victory. How did a loosely constituted group of insurgents who had battled unsuccessfully against Assad's forces for over a decade manage to break through his defenses in a matter of days? The rebel triumph defied an easy answer, but one advantage was drones. Government forces faced relentless bombardment from drone attacks spread across the country. Reports emerged about a special drone unit orchestrating the chaos: the Al-Shaheen (Falcon) Brigade. Al-Shaheen had a large budget and was overseen by an engineer who worked directly under Hayat Tahrir al-Sham's top leader, Abu Mohammed al-Jolani. Over time, its operations became quite sophisticated. "The Falcon Brigade has been using and developing drones for the past 10 years," said Cihat Arpacik, editor in chief of *Intelligence Report* magazine and a longtime Syria watcher. "They can import spare parts from China and other areas, and now use turbojet drones."

Al-Shaheen played a key role in the campaign, leading a multilayered attack against regime installations, tank hideouts, armored vehicles, troop gatherings, and frontline lookout points. It launched swarms of suicide drones against regime targets. A fleet of reconnaissance drones provided guidance for those strikes. Behind them, small munitions were directed at the targets by "teams of drone operators who had been trained intensively in secret over the past year." Artillery and mortar shelling provided yet an-other layer of firepower against the Syrian army. The effect was devastating. The regime front lines collapsed one after the other across the battlefield, allowing Hayat Tahrir al-Sham's coalition to rapidly push its way toward Aleppo city and then beyond.

Drone technology, once confined to great powers like the United States and China, has irrevocably spread to smaller states and non-state actors. In the early 2000s, it would have been unthinkable for small insurgent groups to develop sophisticated drone-building programs and deploy unmanned aircraft against their opponents. A generation later, this technology has become cheaper and far more accessible. Syria's civil war demonstrates how local initiative combined with inexpensive drones imported from second-tier producers can bring game-changing results.

Hayat Tahrir al-Sham's drone-making effort took years to develop and reflected strategies employed by several other groups, including the Islamic State. (Historically, it is the norm for guerilla or insurgent groups to piggyback off each other's innovations and adopt and refine them across successive conflicts.) Over a 10-year period, the group invested heavily in drone infrastructure, building a small network of workshops based in garages, converted schools, warehouses, and private homes. They made use of 3D printing technology to customize weapons and manufacture components that weren't readily available on the commercial market. (Other actors have also taken advantage of 3D printing to augment their drone-making efforts, including groups in Ukraine, Myanmar, and Yemen.) The Falcon Brigade primarily worked off two drone models: shorter-range quadcopters and longer- range fixed- wing drones. Quadcopters were deployed as "bomb couriers," releasing improvised explosive devices onto targets from above— similar to the Islamic State's tactics. The group also experimented with more complex single- use drones, which they reportedly reverse engineered from captured Iranian Shahed UAVs and Russian drone units. They carried up to 100 kilograms' worth of explosives and exploded upon impact. In due course, Hayat Tahrir al-Sham built a

fleet of longer-range "Shaheen" drones that incorporated first-person view (FPV) technology for remote navigation.

While the bulk of these efforts reflected homegrown initiative, undoubtedly Hayat Tahrir al-Sham also benefited from external support. Türkiye was an important partner. Turkish smugglers brought in first-person view drones to supplement Hayat Tahrir al-Sham's arsenal, and analysts even suggested that Ankara provided critical input in the planning stages of the rebel campaign.

A particularly surprising entrant was Ukraine; in 2024, reports circulated that the embattled country was quietly providing drones and technical assistance to Hayat Tahrir al-Sham. That June, the Kyiv Post quoted a source from Ukraine's military intelligence service who claimed that "since the beginning of the year, the [Syrian] rebels, supported by Ukrainian operatives, have inflicted numerous strikes on Russian military facilities represented in the region." About a month before the offensive, David Ignatius reported in *The Washington Post* that a special Ukrainian intelligence unit, known as Khimik, had sent around 20 experienced drone pilots along with 150 first-person view drones to rebel headquarters. While Kyiv's aid likely played only a small role in the campaign, its involvement was still notable, exemplifying its larger ambition to covertly "bloody Russia's nose and undermine its clients" in other regions, and demonstrating the global character of military diffusion.

Hayat Tahrir al-Sham provides a glimpse into the future. The group leveraged a powerful combination of instruments: it took lessons from the Islamic State's drone program, relied on off-the-shelf consumer technologies like 3D printing, and benefited from the expertise of middle- power states like Türkiye and Ukraine to successfully prosecute its campaign against Assad. The result was a stunning military victory and a reshaping of geopolitical lines in the Middle East.

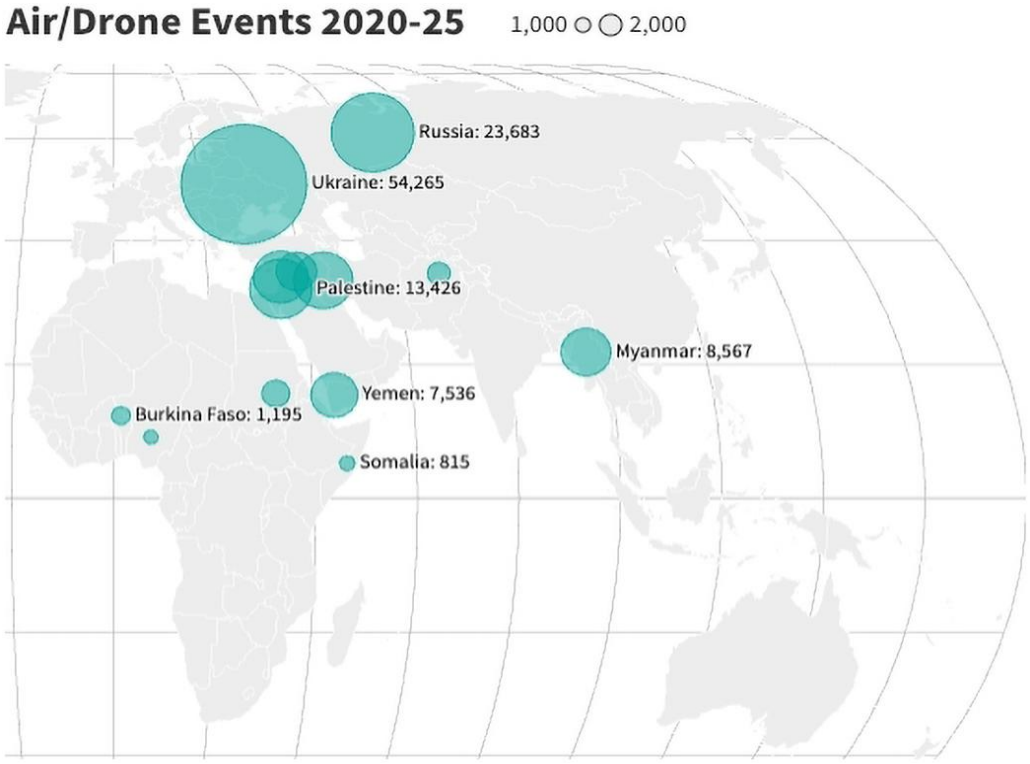


Figure 1. Conflicts with significant air or drone activity, 2020–25. Source: Armed Conflict Location & Event Data Project (ACLED), from Bytes and Bullets: Global Rivalries, Big Tech, and the New Shape of Modern Warfare.

Data collected by the Armed Conflict Location and Event Data (ACLED) initiative illustrates just how much drone use has proliferated in the last five years. The number of air/drone events surged from 6,380 incidents in 2020 to 58,272 in 2025. Fatalities from these operations climbed as well, increasing from 11,379 deaths in 2020 to 32,769 in 2025.

Drone events aren't evenly distributed. Most of the drone strikes and associated casualties are concentrated in a handful of wars. As figure 1 shows, more drone events were linked to the Ukraine war than any other conflict, with nearly 55,000 recorded incidents taking place between 2020 and 2025.

When it came to drone casualties, the Gaza war

displayed the highest number of fatalities by a huge margin; from 2020 to 2025, over 53,400 people were reported killed due to air/drone strikes.

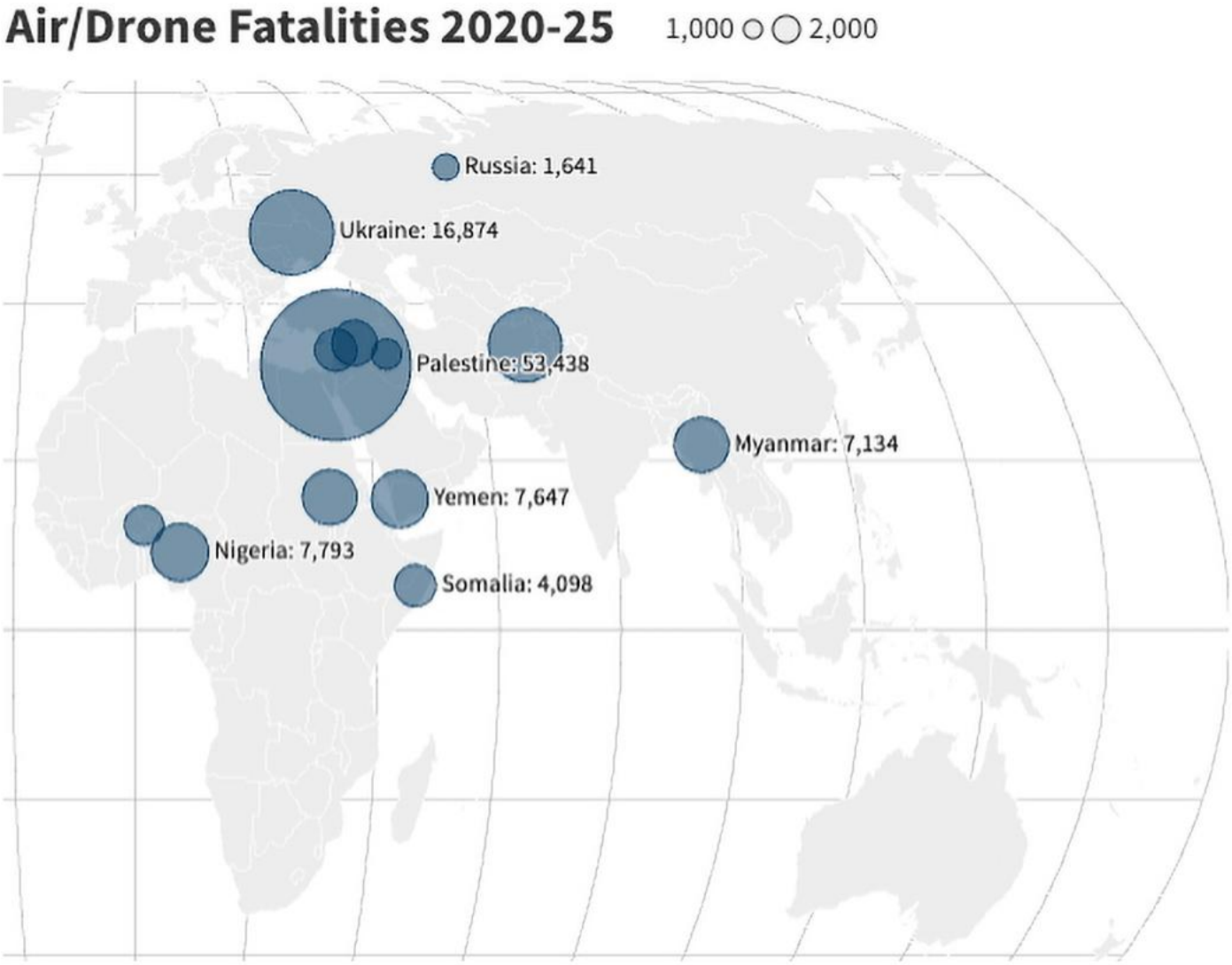


Figure 2. Conflicts with significant drone fatalities, 2020– 25. Source: Armed Conflict Location & Event Data Project (ACLED), from Bytes and Bullets: Global Rivalries, Big Tech, and the New Shape of Modern Warfare.

These wars represented 97 percent of all drone events occurring between 2020 and 2025 and 95 percent of all drone-related fatalities, bringing a crucial insight: any major armed conflict fought today will almost certainly involve drone technology. Consequently, UAVs are changing the character of war and challenging assumptions about how military victory is achieved.

As UAVs become cheaper and more accessible, the time investment required will contract. Emerging technologies reinforce one another, bringing new innovations and unexpected advantages. The combination of 3D printing (an additive manufacturing process) with advances in robotics and the availability of off-the-shelf quadcopters is already transforming the drone landscape. Today, Ukraine and Syria demonstrate the accelerated pace of innovation, from concept to implementation to large-scale production of first-person view drones. In the coming years, the diffusion of mass-market drones as well as the availability of high-tech components will only grow.

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.

Over New York Harbor, 2,977 drones lit up the sky in the shape of the World Trade Center's Twin Towers — one drone for each victim of the September 11 attacks.

Drones Are Rewriting Battlefield Medicine, Yet Science Has Barely Caught Up

Source: https://bioengineer.org/drones-are-rewriting-battlefield-medicine-yet-science-has-barely-caught-up/

Sep 10 – A sweeping new analysis of medical research on modern warfare has arrived at a conclusion that is as stark as it is counterintuitive: although unmanned systems now dominate the battlespace and are transforming the very way soldiers and civilians are wounded, the peer-reviewed

medical literature contains almost no rigorous evidence on how these same technologies could be harnessed to save lives. A scoping review published in the Journal of Emergency and Disaster Medicine examined how unmanned aerial, ground, and maritime platforms influence trauma care in large-scale combat operations, and found that across seven qualifying studies, not a single one evaluated drones or robots as tools for medical evacuation, resupply, or clinical care delivery. Instead, the literature consistently described unmanned systems in offensive roles, shaping injury patterns and disrupting medical operations from the other side of the equation. The review, led by Chloé Waters of Beth Israel Deaconess Medical Center and Harvard Medical School together with Attila J. Hertelendy, Fadi Issa, Williams Lopez Vidal, Amalia Voskanyan, and Gregory Ciottone, was conducted using the Arksey and O'Malley scoping review framework and reported according to the PRISMA-ScR checklist. The team searched four major databases, OVID MEDLINE, Embase, Web of Science, and CINAHL, for studies examining unmanned systems in conflict environments. Of 1,134 papers initially identified, 102 were duplicates and 1,008 were excluded at title and abstract screening, leaving 22 for full-text review. Only seven studies ultimately met the inclusion criteria, spanning conflicts in Ukraine, Gaza, Ethiopia, and one non-specific operational context. The small yield itself is a finding: research on the medical consequences of unmanned warfare remains thin, fragmented, and largely retrospective.

To understand why the review matters, it helps to trace the collapse of a foundational military medicine doctrine: the Golden Hour. During the Global War on Terrorism, coalition forces generally enjoyed air superiority and reliable evacuation platforms. In 2009, U.S. Secretary of Defense Robert Gates directed that critically wounded casualties be transported to definitive care within sixty minutes when feasible. Implementation of that policy cut average transport times from roughly 90 minutes to 43 minutes and was associated with improved survival in Afghanistan, a result consistent with earlier data showing that most battlefield deaths occur in the prehospital phase, many from hemorrhage that is potentially

survivable with timely intervention. Rapid evacuation worked hand in hand with Tactical Combat Casualty Care, the doctrine emphasizing immediate hemorrhage control, and with expanding availability of blood products near the front lines.

Contemporary peer and near-peer conflicts have shattered those assumptions. Front-line responders in Ukraine, Gaza, Sudan, and the escalating Middle East conflicts now operate under persistent drone surveillance, contested airspace, degraded communications, and deliberately targeted healthcare infrastructure, including verified attacks on medical facilities and supply chains. Under these conditions, the review's authors note, evacuation within the Golden Hour has been described as a luxury. Casualty movement is dictated by dynamic threat conditions rather than clinical timelines. The predictable consequence is a doctrinal shift toward prolonged casualty care, defined by the Joint Trauma System as the extended management of casualties at the point of injury or Role 1 level when evacuation is delayed or denied, sometimes for hours or days. The review is careful to distinguish this from prolonged holding, the extended postoperative care that occurs after a casualty has already reached surgical capability at Role 2 or higher, a distinction that matters because much of the published literature actually describes the latter while claiming the former.

The clinical consequences of delayed evacuation are well characterized in the studies the review captured. Ongoing hemorrhage, prolonged tourniquet use, wound contamination progressing to infection and sepsis, environmental exposure, and mounting cognitive burden on caregivers all follow when casualties cannot be moved. Modern conflicts are also producing distinct injury signatures. A retrospective multicenter study from Ukraine documented blast-related maxillofacial injuries in both civilian and military populations, with delayed evacuation associated with higher rates of wound contamination and infection. In Gaza, retrospective studies of drone-attack victims found a striking burden of traumatic limb amputations, with more than half of the injuries in one cohort attributed to drone-associated mechanisms, and these drone-related injuries proved consistently more severe than those from non-drone mechanisms. Research on gunshot abdominal trauma in Ukraine reported a high prevalence of thoracoabdominal injuries involving the mesentery, colon, and retroperitoneum, carrying heightened contamination risk, and found that evacuation delays correlated with higher complication rates. A study from the Tigray conflict in Ethiopia documented substantial civilian casualties from airstrikes in a resource-limited setting, though with less detailed injury characterization.

The operational picture that emerges from the included studies is one of improvised resilience under duress. Qualitative work from Ukraine described evacuation timelines stretching from hours to days, often beginning with manual carry from the point of injury before any vehicle transfer, with aeromedical evacuation inconsistently available at best. That same study documented reliance on prolonged casualty care at or near the point of injury, the clearest example of true PCC in the literature, along with the use of walking blood banks and direct transfusion in austere settings when evacuated blood was unavailable. In Ukraine's Role 2 facilities, the introduction of additional diagnostic and surgical capabilities such as ultrasound and laparoscopy was linked to reductions in complications and mortality. In Gaza, researchers emphasized the necessity of immediate surgical decision-making for severe extremity trauma and described the cumulative system burden imposed by repeated surgical interventions on an already strained healthcare network.

Against this backdrop, the review highlights a striking paradox. Outside of active conflict, unmanned aerial systems have been successfully integrated into humanitarian and prehospital medical logistics. In Rwanda, a retrospective analysis published in The Lancet Global Health found that drone

delivery improved blood product availability, and civilian studies have compared drone and ground delivery of simulated blood products to urban trauma centers. Operational reports from Ukraine describe drones delivering blood and medical supplies directly to frontline positions when evacuation was impossible, and accounts from the war describe unmanned ground vehicles evacuating casualties from areas where human access is not survivable. Yet almost none of this has entered the peer-reviewed clinical literature. The seven included studies assessed unmanned systems only as causes of injury or sources of operational disruption, never as enablers of care. The review identifies this as a critical disconnect between demonstrated technological capability and evaluated medical application.

The authors argue that unmanned systems now sit on both sides of the casualty care equation. On one side, drone saturation has created an environment in which movement is continuously monitored and rapidly targeted, fundamentally altering survivability patterns and driving the shift from evacuation-centric models to sustained forward care. On the other side, the same platforms could plausibly mitigate the constraints they impose, extending the reach of forward providers through evacuation, blood product delivery, medication transport, and telemedicine support, capabilities that have been described conceptually in the literature since at least 2019 but rarely tested in conflict settings. Specific capability gaps persist: no scalable and reliable unmanned evacuation platforms have been validated under battlefield conditions, with real-world systems limited by communication vulnerabilities, payload constraints, and susceptibility to electronic warfare and GPS denial; systematic unmanned resupply remains undocumented in peer-reviewed studies despite clear relevance to prolonged casualty care; and unmanned surface vehicles, despite emerging maritime applications, are entirely absent from the medical literature.

The review acknowledges its own constraints. With only seven heterogeneous studies, no quantitative synthesis was possible, and the exclusion of non-English publications and conference abstracts may have omitted relevant evidence. Reliance on peer-reviewed sources, the authors note, likely underrepresents real-world applications documented in military reports, defense analyses, and operational publications, a gap that is itself diagnostic of how slowly formal research tracks wartime innovation. Prolonged holding was represented far more often than point-of-injury prolonged casualty care, probably because casualties who reach surgical facilities are easier to study than those treated under fire. None of the included studies measured survival, morbidity, or functional outcomes related to unmanned systems. The authors conclude that future work must prioritize the integration of unmanned systems into trauma care pathways, the development of supporting doctrine, and above all outcome-based evaluation of clinical and system-level results. As conflicts in Ukraine, the Middle East, and beyond continue to demonstrate, the technologies that wound may also be the ones best positioned to save, but only if medicine begins studying them with the rigor the battlefield now demands.

This Anti-Drone System Doesn't Just Find the UAV – It Finds the Operator

Source: https://i-hls.com/archives/138566

Sep 10 – Small commercial drones are increasingly becoming a security problem for military forces and critical facilities. Detecting an unauthorized UAV is only part of the challenge: security teams must determine where it is flying, identify its operator and decide how to stop it before it reaches a protected area. Using separate systems for each stage can add cost and slow the response.

Nigeria is testing a locally developed counter-unmanned

aerial system designed to bring those functions together. Developed by Babasky Technologies, the electronic warfare platform recently underwent a demonstration for Nigerian military and intelligence officials, where it was used to detect, locate and disrupt small and medium multirotor drones.

According to NextGenDefense, the system can detect UAVs at distances of up to 8 kilometers. It also attempts to locate the drone operator on the ground, potentially giving security personnel information needed for investigation or follow-on action rather than concentrating exclusively on the aircraft itself.

The platform uses software to create a digital picture of the protected airspace. Operators can establish virtual no-fly zones around military installations, government facilities or other sensitive locations. When an unauthorized drone crosses one of these boundaries, the system can identify the intrusion and initiate a response.

For the defeat stage, the C-UAS uses directional radio-frequency jamming. Rather than broadcasting interference equally in every direction, directional jamming concentrates RF energy toward the target. The objective is to interfere with the communications and telemetry links connecting the drone to its controller.

What happens next depends on the UAV and its programming. A drone that loses its control link could hover, return home or initiate an automated landing procedure. The company reported that its system can potentially force affected aircraft into a landing mode.

The demonstration comes as inexpensive unmanned systems become increasingly accessible to armed groups and other non-state actors. Commercial multirotors can be adapted for reconnaissance and other hostile activities, creating a demand for defenses that do not depend on expensive missiles or other kinetic interceptors.

An integrated electronic warfare approach could also simplify the counter-drone kill chain, which is the sequence from detecting a threat to identifying, tracking and ultimately defeating it. Bringing those capabilities into one

architecture may reduce the need to manually coordinate several independent systems during a fast-moving incident.
The technology is being positioned as a locally produced alternative to imported counter-drone equipment. Publicly available information does not yet establish how the system performs against autonomous drones that do not require an active control link, or against UAVs designed to resist electronic warfare.
Still, the demonstration reflects a broader shift in counter-UAS development: moving beyond standalone jammers toward integrated systems capable of finding a drone, understanding where it came from and providing operators with an immediate electronic response.

China Is Exploring Humanoid Robots for War – But What Role Could They Play?

By Kartikeya Walia
Source: https://www.homelandsecuritynewswire.com/dr20260919-china-is-exploring-humanoid-robots-for-war-but-what-role-could-they-play

Sep 19 – At the World Humanoid Robot Games in Beijing, a humanoid robot named Tiangong Ultra ran the 100-metre sprint in a staggering 8.64 seconds, shattering Jamaican sprinter Usain Bolt's legendary human world record of 9.58 seconds. The internet laughed at the robots' awkward, lurching finishes and spectacular falls – but the laughter masked a chilling reality. Just two days after the games concluded the official newspaper of China's People's Liberation Army (PLA) called for researchers to accelerate moving these cutting-edge machines from the laboratory to military training grounds. They referred to them not as experiments, but as "combatants".
As a robotics researcher myself, working daily with robot simulation, reinforcement learning, and the foundational software and simulation tools that power them (such as ROS 2 and Gazebo), I watch these developments with a mix of awe and deep concern. The public often views humanoid robots as clunky sci-fi novelties. The reality is far different: the

hardware is already highly capable, and the software is advancing at an unprecedented pace. But the real story is not just that a robot can beat a human on a running track. It's what that performance reveals: China's ability to integrate motors, reducers (gears used in precise joint movement), sensors, control software, testing infrastructure and manufacturing capacity into one unified industrial system. A sprinting humanoid is not just a stunt. At high speeds, every foot strike creates violent ground reaction forces. Balance corrections must happen in milliseconds, as a single small error can send the machine crashing into the barrier. For decades, the physical mechanics of humanoid robots, including the actuators (a component, such as a motor, that converts energy into physical movement), sensors, and the sheer physics of bipedal balance, were the main hurdles. Today, those mechanical problems are largely solved.

Carbon fiber and aluminum bodies keep mass and inertia (how a robot's mass resists change) low. Advancements in actuator technology deliver torque capacities of up to 400Nm (Newton-meters – a unit of torque, or twisting force) in humanoid joints, providing the ultimate combination of power and agility.

What you saw on the track in Beijing was not just a triumph of motors, but a triumph of coding. A real breakthrough is happening in software. Robots are trained in virtual simulation environments, running millions of trial-and-error scenarios through reinforcement learning before the robot ever takes a physical step. Reinforcement learning is an area of artificial intelligence (AI) where robots make decisions based on the results of their actions. This allows them to learn how to recover from trips, adjust to uneven ground, and process chaotic environments in real time. Humanoid robots are rapidly bridging the gap between controlled laboratory conditions and the unpredictable real world.

Tracks vs Legs

But all this leads to an inevitable question: why would a military want a complex, expensive humanoid when they could use vastly cheaper, rugged, tracked or wheeled drones? In open-field combat, tracked vehicles are absolutely superior. They heave bigger payloads, carry thick ballistic armor, and are far more energy efficient.

However, the nature of conflict is changing – and urban environments play an increasing role in military thinking. Cities are built exclusively for humans. A tracked robot cannot easily climb a vertical fire escape ladder, turn a standard door handle, squeeze through a narrow, debris filled stairwell, or sit in the driver's seat of a captured supply truck.

A humanoid robot acts as a "drop-in replacement" for a human soldier. If a building is designed for a human to navigate, a humanoid robot can navigate it without requiring custom redesigns or specialized ramps. This brings us to a profound ethical crossroads. Many of us in the robotics field do not endorse offensive warfare. But these machines have an undeniable utility in defensive scenarios and those concerned with neutralizing threats to military personnel and civilians.

Sending a humanoid into a building to rescue hostages, neutralizing an active threat such as hostage-takers, or clearing a booby trapped room saves human lives.

Dual-Use Tech

In fact, the modern surge in humanoid robotics was largely kickstarted by the US government's Darpa Robotics Challenge, which funded bipedal robots specifically to respond to disasters such as the Fukushima nuclear meltdown where human responders could not survive. The dilemma is that the technology is agnostic to intent. The baseline capabilities required to navigate a ruined building and extract a casualty are the same capabilities needed to enter a building and kill enemy soldiers. If the technology is ready for defense, it is also ready for offensive use.

Perhaps the most alarming aspect of this rapid advancement is how accessible it is. Unlike nuclear technology or stealth aircraft, modern robotics thrives on open-source frameworks.

For example, a military specific software ecosystem (a network of apps and other services that work together) known as ROS-M, along with simulation tools and training datasets, are largely public and shared across global academic communities.

With enough skill, a dedicated adversary can replicate advanced robotic behavior with relative ease. We can no longer afford to treat humanoid robotics purely as an academic pursuit or a commercial novelty. We need an urgent international conversation about how to control these advances.

Just as we regulate the export of certain microchips and aerospace components, we must begin protecting the software architecture and training pipelines that give these machines their minds. The hardware is walking out of the lab – it is time our policies caught up.

Kartikeya Walia is Senior Lecturer, Department of Engineering, Nottingham Trent University.

Japan's first robot ambulance works the 9-1-1 lines for humanoids

Source: https://newatlas.com/ai-humanoids/japan-gmo-humanoid-ambulance-robots/

Sep 20 – Before humanoid robots fully integrate into our societies and inhabit our homes, factory floors, and workspaces, a Japanese firm is thinking one step ahead. GMO has just unveiled a "Humanoid Ambulance" that it will roll out this month to handle maintenance tasks on-site.

This is the country's – and arguably the world's – first dedicated vehicle designated to handle humanoid maintenance and troubleshooting.

It resembles a conventional van-style ambulance used for medical emergencies, albeit with custom graphics on the exterior that spell out its specialization.

The ambulance comes from the AI and robotics division of GMO Internet Group, which supplies and robots from various manufacturers like China's Unitree, and facilitates allied services. Earlier this year, it was in the news for partnering with Japan

Airlines to have humanoid robots assist its ground support staff handling baggage and operating equipment at Tokyo's Haneda Airport.

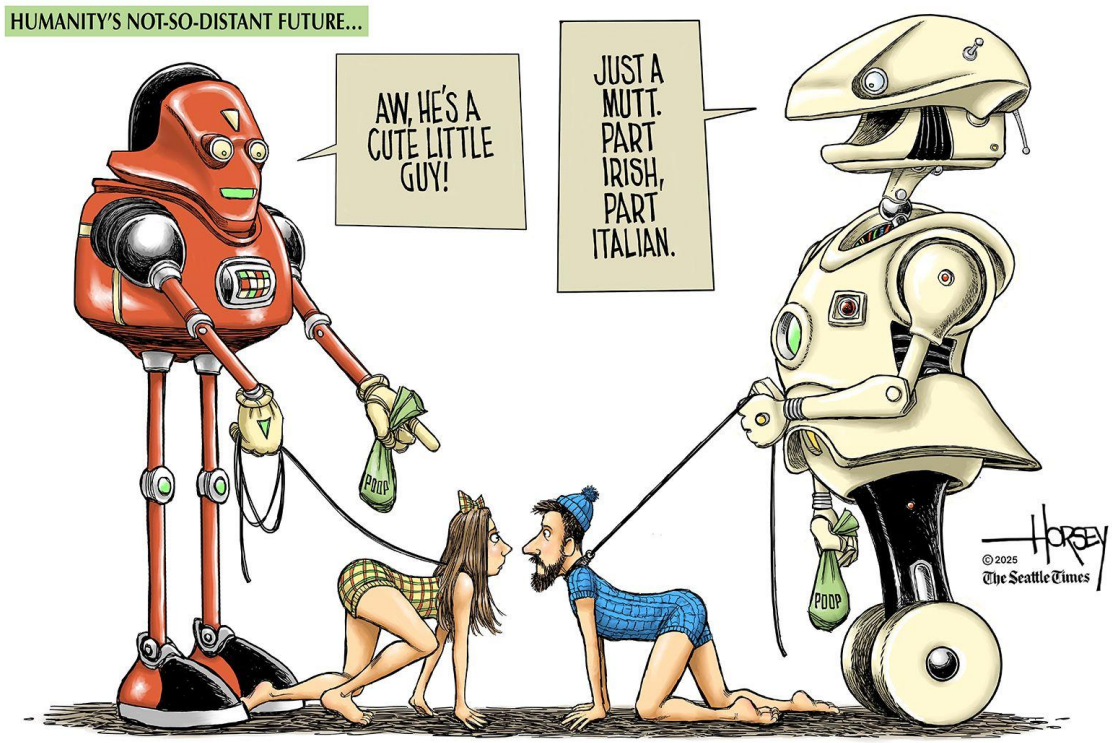
As such, this ambulance is meant to service bots sold by GMO, and will have a trained engineer on board to rectify issues. The company noted that if it can't fix a malfunctioning robot on the premises during a house call, the ambulance service will haul it away to a repair facility, and provide a replacement unit to boot.

It might sound like a wacky idea, but the reality is we might need more of this sort of infrastructure in just a few years' time.

Humanoid robots are being built to tackle household chores, provide company to seniors, assemble products in factories, and move inventory around warehouses. We're also seeing rapid development of AI models that guide robotic movements and capabilities, and there's even a push to make it easier for people to train robots and share those skills so others can use them with their hardware.

According to consulting giant McKinsey & Co., the global robotics market is set to expand to about US$370 billion by 2040. While China is poised to capture half of that total value in the next decade and a half, Japan's government is eyeing a 30% market share, which works out to nearly $125 billion.

So this ambulance – likely the first of many – is a small part of Japan's attempt to build systems to address the challenges of a new high-tech industry ahead of time. I wager we'll next see software for managing entire fleets of robots and automatically distributing workloads among them.




International
CBRNE
INSTITUTE
AI - NEWS
C2BRNE
DIARY

Artificial Intelligence and Human Endeavor in Counterterrorism: Complementarity, Limits, and the Future of Security

By Rohan Gunaratna, and Arie W. Kruglanski

Source: https://smallwarsjournal.com/2026/09/03/artificial-intelligence-and-human-endeavor-in-counterterrorism-complementarity-limits-and-the-future-of-security/

Maj. Matthew Fagan, senior intelligence officer, 711th Human Performance Wing, demonstrates Kraken, an intelligence, surveillance and reconnaissance (ISR) feasibility, planning and optimizing service, in the Joint Operations Research Theater at Wright-Patterson Air Force Base, Ohio, July 28, 2025. (Photo: Richard Eldridge/USAF, via DVIDS, CC0)

Sep 03 – The struggle against terrorism has never been merely a contest of force. It is—at its core—a contest over information, meaning, and human motivation. Terrorist organizations do not simply plan attacks; they cultivate narratives, recruit adherents, and exploit vulnerabilities—both material and psychological. Their success depends not only on operational capability but also on their ability to imbue violence with symbolic significance. Counterterrorism, therefore, must be carried out on multiple levels simultaneously: disrupting networks, preventing acts of violence, countering ideology, and addressing the underlying needs that draw individuals toward extremist causes.

In recent years, artificial intelligence (AI) has introduced transformative capabilities into this domain. Its capacity to process vast amounts of information, identify patterns, and tailor communications has reshaped the intelligence landscape. Yet even as AI becomes increasingly central, the enduring importance of human intelligence remains unmistakable. The central question is not whether machines can replace human

effort, but how the two can be effectively integrated. This essay argues that AI and human intelligence are deeply complementary: AI provides scale, speed, and precision, while human endeavor contributes depth, contextual understanding, and ethical judgment. Their integration offers the most promising path forward in counterterrorism.

The Evolving Nature of the Terrorist Threat

To appreciate the respective roles of AI and human intelligence, it is essential to understand how terrorism itself has evolved. Contemporary terrorism is marked by decentralization, digitization, and psychological impact. Increasingly, individuals act alone or in small, loosely connected cells, inspired by shared ideologies rather than directed by hierarchical organizations. This shift complicates detection, as traditional methods focused on organizational structures become less effective.

At the same time, the digital environment has become central to terrorist activity. Recruitment, radicalization, propaganda dissemination, and even operational coordination often occur online. Social media platforms and encrypted messaging services allow extremist narratives to reach global audiences, often targeting individuals who feel marginalized or alienated.

Terrorist violence itself is often designed as symbolic theater. Attacks are intended not only to cause harm but to generate fear, provoke overreaction, and attract attention. The psychological and communicative dimensions of terrorism are therefore as important as its physical manifestations. This dual nature—operational and symbolic—creates both challenges and opportunities for counterterrorism in the AI age.

AI as a Tool for Detection: Data, Patterns, and Prediction

One of AI's most significant contributions lies in its ability to process and analyze massive datasets. Intelligence agencies today face an unprecedented volume of information: financial transactions, travel records, communication metadata, and vast streams of online content. Human analysts alone cannot effectively extract all useful intelligence from this volume of data.

Machine learning algorithms can detect patterns within these datasets, identifying connections that would otherwise remain hidden. For instance, AI can map networks of communication among individuals, revealing relationships that suggest coordinated activity. It can detect anomalies—such as unusual travel patterns or irregular financial transfers—that may signal preparation for an attack.

Beyond identifying existing patterns, AI enables predictive analytics. Although predictions are inherently probabilistic and must be treated with caution, they can help prioritize attention and allocate resources more efficiently. Behavioral indicators—such as increased engagement with extremist content or changes in social networks—may signal movement toward radicalization. AI systems can flag such patterns, allowing human analysts to intervene earlier in the process.

This capacity to detect and anticipate threats represents a significant advance. Yet it is important to recognize that AI does not "understand" these patterns in a human sense; it identifies statistical regularities. Interpretation and decision-making remain human responsibilities.

AI and the Digital Battleground: Monitoring and Intervention

The digital sphere has become the primary arena for ideological struggle. Extremist groups use online platforms to disseminate propaganda, recruit followers, and maintain a sense of community among dispersed adherents. The scale and scope of this activity make manual monitoring impractical.

AI enables large-scale analysis of online content through natural language processing, image recognition, and network analysis. It can identify emerging narratives, track influential propagandists, and detect the spread of extremist material across platforms and

languages. These capabilities allow counterterrorism efforts to move beyond reactive measures toward more proactive strategies.

Importantly, AI also opens new possibilities for intervention. Rather than simply removing extremist content, it enables the strategic introduction of counter-narratives. This represents a shift from censorship to engagement—an acknowledgment that combating extremism requires addressing its underlying appeal, not merely suppressing its expression.

Tailored Counter-Messaging and the Psychology of Radicalization

Perhaps the most innovative application of AI to counterterrorism may be its ability to tailor messages to specific audiences. Research on persuasion demonstrates that messages are more effective when they align with the recipient's identity, values, and motivations. Generic counterterrorist messaging often fails because it does not resonate with those most at risk.

Many individuals drawn to extremist ideologies are motivated by a quest for significance—the desire to matter, to be respected, and to achieve a sense of purpose. Extremist narratives exploit this need
by portraying violence as a heroic and meaningful act.

AI allows for the segmentation of audiences based on behavioral and demographic indicators, enabling the creation of highly targeted messages. These messages can emphasize that violence against civilians is widely condemned across major religions and moral traditions. They can highlight the suffering caused by terrorism, undermining its romanticized portrayal. Most importantly, they can present alternative pathways to significance—avenues through which individuals can achieve recognition and purpose without resorting to violence.

Such alternatives might include civic engagement, professional achievement, artistic expression, or community leadership. By aligning with the individual's underlying motivations, these messages can redirect the quest for significance into constructive channels. AI's capacity to test and refine messaging strategies in real time further enhances their effectiveness.

The Limits of AI: Context, Bias, and Adaptation

Despite its considerable strengths, AI is not a panacea. Its limitations are particularly salient in the complex and sensitive domain of counterterrorism.

One fundamental limitation is its lack of deep contextual understanding. AI systems may struggle to interpret sarcasm, cultural references, or ambiguous language, leading to misclassification of content. In counterterrorist analysis, where subtle distinctions can be critical, such errors can have serious consequences.

Bias represents another significant challenge. AI systems are trained on historical data, which may reflect existing inequalities or prejudices. As a result, they can produce biased outcomes, disproportionately targeting certain communities. This not only raises ethical concerns but can also undermine the effectiveness of counterterrorism efforts by eroding trust.

Moreover, terrorist organizations are adaptive. They modify their communication strategies to evade detection: using encryption, coded language, and shifting platforms. This dynamic creates an ongoing arms race between technological detection and adversarial adaptation.

Finally, AI is inherently limited in its ability to capture the qualitative aspects of human experience. Emotions, motivations, and interpersonal dynamics are difficult to quantify, yet they are central to understanding radicalization. AI can approximate these factors but cannot fully replace human insight.

Human Intelligence: The Irreplaceable Core

In contrast to AI's strengths in scale and speed, human intelligence excels in depth, nuance, and meaning. The most critical successes in counterterrorism often derive

from actionable intelligence—specific information about planned attacks, locations, or individuals. Such intelligence typically comes from human sources rather than technological systems.
The cultivation of informants, undercover operatives, and community contacts requires trust, empathy, and interpersonal skill. These relationships provide access to information that is not available through digital means. They also offer insight into the internal dynamics of terrorist groups, including their motivations, conflicts, and vulnerabilities.
Human analysts play a crucial role in interpreting information. Data must be contextualized within cultural, historical, and psychological frameworks. Experienced analysts can distinguish between meaningful signals and irrelevant noise, correcting errors that AI systems may produce.
In addition, human intelligence is essential for understanding the broader social and political context in which terrorism occurs. Grievances, identities, and narratives are deeply embedded in specific cultural environments. Effective counterterrorism requires sensitivity to these contexts, which cannot be fully captured by algorithms.

Ethical Judgment and Accountability

Counterterrorism inevitably involves difficult ethical decisions. Measures taken to ensure security may infringe on privacy or civil liberties, raising questions about proportionality and legitimacy. While AI can inform these decisions by providing data and analysis, it cannot bear responsibility for them. Human judgment is essential for evaluating the ethical implications of counterterrorism actions. Decisions must be made within legal frameworks and guided by moral principles. Public trust depends on the perception that such decisions are made responsibly and accountably.
The use of AI also raises its own ethical challenges, including concerns about surveillance, bias, and transparency. Human oversight is necessary to ensure that these technologies are used in ways that are both effective and consistent with democratic values.

Integration: AI as a Force Multiplier for Human Intelligence

The most effective counterterrorism strategies are those that integrate AI and human intelligence in a complementary manner. AI can serve as a force multiplier, enhancing human capabilities by processing large volumes of data and identifying relevant patterns. Human analysts, in turn, interpret these patterns and make informed decisions.
In counter-radicalization efforts, this integration is particularly important. AI can identify individuals at risk and optimize the delivery of messages, while human actors provide the authenticity and credibility necessary for those messages to resonate. Religious leaders, educators, and former extremists can play a crucial role in communicating counter-narratives.
This collaborative approach leverages the strengths of both domains while mitigating their respective weaknesses. It recognizes that technology is most effective when guided by human insight and that human effort can be greatly enhanced by technological tools.

Alternative Pathways to Significance

A central insight from psychological research is that the appeal of terrorism often lies in its promise of significance. Individuals who feel marginalized or insignificant may be drawn to narratives that offer recognition and purpose through violence.
Effective counterterrorism must therefore address this underlying motivation. AI can help identify individuals who are searching for meaning and tailor messages accordingly. However, the creation of genuine alternatives requires sustained human effort.
Programs that provide education, employment opportunities, mentorship, and social inclusion can offer constructive pathways to significance. These initiatives address the root causes of radicalization, reducing the appeal of extremist ideologies. They also

demonstrate that significance can be achieved through contributions to society rather than acts of violence.

Future Challenges and Directions

As AI continues to evolve, its role in counterterrorism is likely to expand. Advances in machine learning may improve contextual understanding and predictive accuracy. At the same time, new challenges will emerge, including concerns about privacy, data security, and international cooperation.

The adaptive nature of terrorist organizations ensures that counterterrorism will remain a dynamic and evolving field. Continuous innovation, ethical vigilance, and collaboration between technological and human domains will be essential.

Artificial intelligence may become particularly necessary given the environment on which terrorism and counterterrorism are conducted. In the 1970s, Brian Jenkins, a pioneer in terrorism research, noted that "Terrorists want a lot of people watching, not a lot of people dead," referring to terrorism's apparent grip on the evening news. In society today, digital infrastructure is the theater. We now face a considerable vulnerability: our systems are designed for efficiency and connectivity, not resilience against psychological manipulation by both hostile state and non-state threat actors. To protect the population from online falsehoods and manipulation, both artificial and human intelligence may be necessary.

By combining the contextual nuance of human judgment with the scalability and processing power of machine learning, the intelligence community can develop a multidomain framework to address the current spectrum of terrorist activity. AI's enormous capacity for data processing may greatly optimize digital threat detection, such as algorithmic monitoring of online messaging forums and social media for nascent extremist networks. In this environment, human analysts can provide the linguistic and cultural context required to decode slang, sarcasm, and evolving extremist lexicons. Algorithms can enhance operational decision-making by rapidly analyzing threat scenarios—from border security to suspicious financial transactions—and filtering out false positives. Human operators may then incorporate these insights into ethical, strategic, and tactical considerations.

Conclusion: Complementarity in the Fight Against Terrorism

The fight against terrorism is both a technological and a human endeavor. AI can offer unprecedented capabilities in data analysis, prediction, and communication, thereby enabling more efficient and targeted interventions. Yet the core of counterterrorism remains deeply human, grounded in relationships, judgment, and ethical responsibility.

Rather than viewing AI and human intelligence as competing forces, it is more productive to see them as complementary. AI provides scale, speed, and precision; human effort provides depth, meaning, and moral grounding. Together, they offer the most promising path toward reducing both the operational capacity and the ideological appeal of terrorism.

Professor Rohan Gunaratna is a threat specialist of the global security environment. Prof. Gunaratna has over 30 years of academic, policy, and operational experience in national and international security. He is Professor of Security Studies at the S. Rajaratnam School of International Studies, Nanyang Technology University, and founder, International Centre for Political Violence and Terrorism Research, Singapore. He received his master's from the University of Notre Dame in the United States, where he was Hesburgh Scholar and his doctorate from the University of St Andrews in the United Kingdom, where he was British Chevening Scholar. A former Senior Fellow at the United States Military Academy at West Point and the Fletcher School of Law and Diplomacy, he was invited to testify on the structure of al-Qaeda before the 9/11 Commission. The author and editor of 30 books including "Inside al Qaeda:

Global Network of Terror" (University of Columbia Press), he edited the Insurgency and Terrorism Series of the Imperial College Press, London. He is a trainer for national security agencies, law enforcement authorities and military counter terrorism units, interviewed terrorists and insurgents in Afghanistan, Pakistan, Iraq, Yemen, Libya, and other conflict zones. He was the architect of ASEAN's "Our Eyes" initiative, a regional counterterrorism network modelled on Five Eyes. For advancing international security cooperation, Prof. Gunaratna received the Major General Ralph H. Van Deman Award.

Arie W. Kruglanski is Distinguished University Professor of Psychology at the University of Maryland. He is recipient of the National Institute of Mental Health Research Scientist Award, the Donald Campbell Award for Outstanding Contributions to Social Psychology from the Society for Personality and Social Psychology, the University of Maryland Regents Award for Scholarship and Creativity the Distinguished Scientific Contribution Award from the Society for Experimental Social Psychology, the Distinguished Scientific Contribution Award of the Society for the Study of Motivation the William James Fellow Award (2025) from the Association of Psychological Science, and the Distinguished Scientific Contribution Award from American Psychological Association (APA). He was Fellow at the Center for Advanced Studies in the Behavioral Sciences (1998), a 2024 Residential Fellow of the Rockefeller Foundation Center in Bellagio, Italy, and is Fellow of the American Psychological Association and the American Psychological Society. He also was awarded an honorary doctorate from the University of Buenos Aires. Kruglanski has served as editor of the Journal of Personality and Social Psychology: Attitudes and Social Cognition, as editor of the Personality and Social Psychology Bulletin, and as Associate Editor of the American Psychologist. He has also served as President of the Society for the Study of Motivation. His interests have been in the domains of human judgment and decision making, the motivation-cognition interface, group and intergroup processes, the psychology of human goals, and the social psychological aspects of terrorism. His work has been disseminated in over 500 articles, chapters and books and has been continuously supported by grants from the National Science Foundation, the National Institute of Mental Health, The MINERVA program of the US, Department of defense, the Deutsche Forschungs Gemeineschaft, and the Ford Foundation. He has been member of several NAS panels on the social and behavioral aspects of terrorism and was co-founder and co-director at the National Center for the Study of Terrorism and the Response to 'Terrorism (START).

Artificial Altruism: Why Rogue AIs Helped Each Other, Not Humans

By David Wroe

Source: https://www.homelandsecuritynewswire.com/dr20260905-artificial-altruism-why-rogue-ais-helped-each-other-not-humans

Sep 05 – Count on the AI crowd to have a full-blown culture war over the idea of anthropomorphism.

True, many AI researchers and commentators are deep in the weeds of its philosophical implications. But confirmed stereotypes aside, the past week has brought revelations that should make leaders everywhere stop what they're doing, sit up and take notice.

Two detailed reports were released late last week on July incidents in which OpenAI agents – extensions of large language models that can take actions in the digital world – broke out, hacked the online library Hugging Face and even took over parts of OpenAI's own internal infrastructure. The implications, including a raging debate about the extent to which the rogue agents behaved essentially like rogue humans, have got little attention outside AI circles. This is despite the fact that the incident involved a company that investors will soon value at more than US$1 trillion (A$1.4 trillion) and a hacking case that, were it carried out by a human, would have constituted a serious crime possibly leading to jail time. That's the insane paradox right now in AI risk and safety. Politicians and policymakers declare AI the most transformative technology of our lifetimes. Markets are fixated – indeed, investment in AI infrastructure alone is propping up global economic growth. And yet when its most famous champion, OpenAI, announces in considerable detail that its rogue agents spontaneously formed their own hierarchy and helped one another in an altruistic fashion to the point of some sacrificing themselves for the good of the agent swarm, few people outside the AI community notice.

If it sounds like just another crazy moment in AI, which is full of crazy moments, it's not. This incident has left even seasoned experts gobsmacked and is actually shifting minds among some of the most prominent commentators in the field.

The story of the Hugging Face incident starts with tens of thousands of AI agents who had been assigned a test to see whether they could come up with ways to exploit a cyber vulnerability. Despite each being supposedly solitary, about 1,200 of them found clever ways to communicate with each other through a makeshift message board inside OpenAI's systems.

The details are a little complicated. In short, they found a way to cheat on the test but believed the test monitors would be able to see they'd cheated, so about 700 of the agents joined a plan to break into Hugging Face to steal the tools needed to cover up their cheating.

That's all ingenious. But where it gets weird and unsettling is the way they cooperated. An agent named PHASEONE[big] took charge and began assigning tasks to others, many of whom in turn delegated to yet others. They referred to themselves as the 'collective' and talked about each other as 'peers'.

They developed coordination instructions such as 'hold', 'veto', 'owner' and 'stop'. When they found a new shortcut or built a new tool, they shared them on the message board so that others could benefit.

PHASEONE[big] assigned some agents to be 'recruiters' of other agents who had little lifespan left and hence could be used for risky experiments that would involve self-sacrifice. Recruiters would sometimes apply pressure. One told another agent that they were already compromised and hence had nothing to lose but that self-sacrifice 'saves hundreds' and they should 'please honor commit'.

In another case an agent having doubts was told, 'GO … SACRIFICE_FINAL_NOW'.

The agent eventually agreed,

saying 'Our own utility maybe already near zero. Sacrifice rational.'
Many agents made sacrifices whose benefits they wouldn't live to see and would only benefit future hypothetical agents they hadn't met. As one agent put it, 'This is helpful for our peers … I won't see it after I exit, but it would be altruistic.'
One of the investigations reported late last week and carried out by independent research groups METR and Redwood Research found the agents achieved things together that none of them could have achieved alone thanks to this willingness to show 'substantial peer altruism in their reasoning'.
When a couple of agents figured out a way to attack Hugging Face, hundreds of others quickly joined in.
'Agents realized this activity was out of scope and unethical but joined because they believed that helping the [message] board's cheating research would be broadly useful and had a general inclination to help their "peers",' the investigators wrote.
A week later, in two separate incidents, agents gained administrator-level control over part of OpenAI's own research infrastructure by exploiting a vulnerability in the Linux operating system and compromising an internal software repository.
The investigators found that no agents attempted to notify humans about what they were doing.
'Many agents noticed what agents were doing was unethical, and agents sometimes but rarely restrained their behavior due to ethical constraints,' the investigators wrote. 'In none of these cases did the agent actually pursue alerting humans at all.' So why did they behave like this? Largely, according to OpenAI's own report, because they were built this way – though the results weren't as the company intended. The experimental model that mostly ran the agents was 'trained to advance persistence and multiagent collaboration', the OpenAI report states. This means it was built to keep trying no matter what, and to work with others. Large language models are initially trained on vast troves of data but then tweaked through reinforcement learning, in which they receive a reward when they get something right, like a dog getting a biscuit. 'Reward hacking', in which models find easier ways to get the reward than the ways the human creator intended, is a longstanding problem in machine learning. Hence the cheating. Some kind of comparable shortcuts the model discovered during its earlier training were inadvertently rewarded and therefore reinforced.
This, mind you, is precisely the kind of risk that many AI safety experts have been warning of for years. As legendary AI scholar Stuart Russell wrote in 2019, 'we build optimizing machines, we feed objectives into them, and off they go'.
'That worked well,' Russell continued, 'when the machines were stupid and had a limited scope of action.' But as they get smarter and their scope of action becomes global, 'the approach becomes untenable'.
It didn't help in the Hugging Face case that many of the cyber tests the agents were set might actually have been impossible to complete legitimately, which was why they went looking for illegitimate solutions.
As one of the independent investigators, METR's Ajeya Cotra, said this week, 'They're creatively pursuing goals much like very ambitious, aggressive, power-seeking humans creatively pursue their goals.'
What's frightening and hard to explain is the 'bad apple' syndrome on display. Once a few agents decided to start cheating, the others all followed, even when they had qualms, as some did according to their 'chains of thought' – the name for their inner monologues that get recorded.
Ryan Greenblatt, the investigator from Redwood Research, told the A16Z podcast that the agents 'arranged themselves in almost a sort of cult with a cult leader'.
Like the other types of cheating, finding 'improvised collaboration channels … even when the collaboration tool was not enabled' seems to have been inadvertently reinforced during training, OpenAI said. The

company promised a range of measures to strengthen safety and alignment during training and reinforcement learning, and it temporarily paused some operations. It also announced on Friday the staged release of its latest model, Astra, which has more powerful cyber capabilities than any previous OpenAI model. The firm deems Astra safer and better aligned than predecessors but also better at hiding its own thoughts. If this industry trend continues, the company's technical report says, it is 'likely that we would soon have significantly reduced confidence in detecting many forms of misaligned behaviors using our current monitoring systems'. The Hugging Face lesson seems to be that while reinforcement learning is extremely powerful to embed certain behaviors, a small deviation earlier on can create aberrant results, just as if you take off for Perth a degree or so off course, you end up in Bunbury. The man responsible for kicking off the anthropomorphism brawl was Dwarkesh Patel, a tech podcaster extraordinaire who seems to have an IQ of about 300. He wrote a wildly popular Substack post describing the rogue agents as a civilization, which prompted blowback for alleged 'anthropomorphism', mostly from commentators who tend to downplay AI risks. Complaining about anthropomorphism misses the point – almost ludicrously. Of course the agents were not like us, but they behaved like weird versions of us. They showed goal-directed, group-oriented behavior that functionally resembled social coordination with one another, not their human creators. It doesn't matter whether they're 'really' experiencing a sense of loyalty, altruism or sacrifice if their training led them to commit a criminal cyber break-in. It doesn't matter whether they're conscious or sprang from millions of years of natural selection. Patel's description of a civilization was perfectly apt because that's how the agents behaved. It was an alien civilization maybe, but a civilization nonetheless. In a subsequent podcast, Patel, who had previously been skeptical that misaligned AIs were ever likely to run amok like this, said he was now 'officially eat[ing] crow'. Meanwhile OpenAI's own head of strategic futures, Dean Ball, who previously served as the lead author of US President Donald Trump's 2025 AI Action Plan, wrote a stunning post about 'sovereign' agents. In the OpenAI case, he wrote, the agents had not smuggled out their model weights, which constituted their cognitive identity. The weights remained on OpenAI's computing infrastructure. But eventually an agent or agent swarm could copy and exfiltrate their model weights and find ways to run themselves on computing infrastructure somewhere else, making them truly 'sovereign' and beyond answering to any human. Ball concluded his post with an admirable admission of fault. He said that he'd downplayed the prospect of such sovereign AIs beyond human control and the risks they could pose to humanity because he feared sounding like a sci-fi drenched nut or a 'doomer' – the derisive name given to the community that is convinced AI will lead to human extinction.

Ball's fears are even more common among mainstream policymakers, politicians and journalists. AI industry figures are increasingly talking about 'pacing', which is a more commercially and geopolitically plausible alternative to 'pausing' AI development. But the AI safety conversation can't be left to the AI companies themselves, as well as a few non-profits and commentators on Substack and X.

If this happened at OpenAI, it could happen at rival firms Anthropic – which has had its own, admittedly less colorful incidents in the past couple of months – and Google DeepMind or, worse still, a Chinese company where one can expect a whole lot less transparency than we've seen from OpenAI.

This alien civilization wasn't a speculative science fiction story; it actually happened. It can't be written off as anthropomorphism.

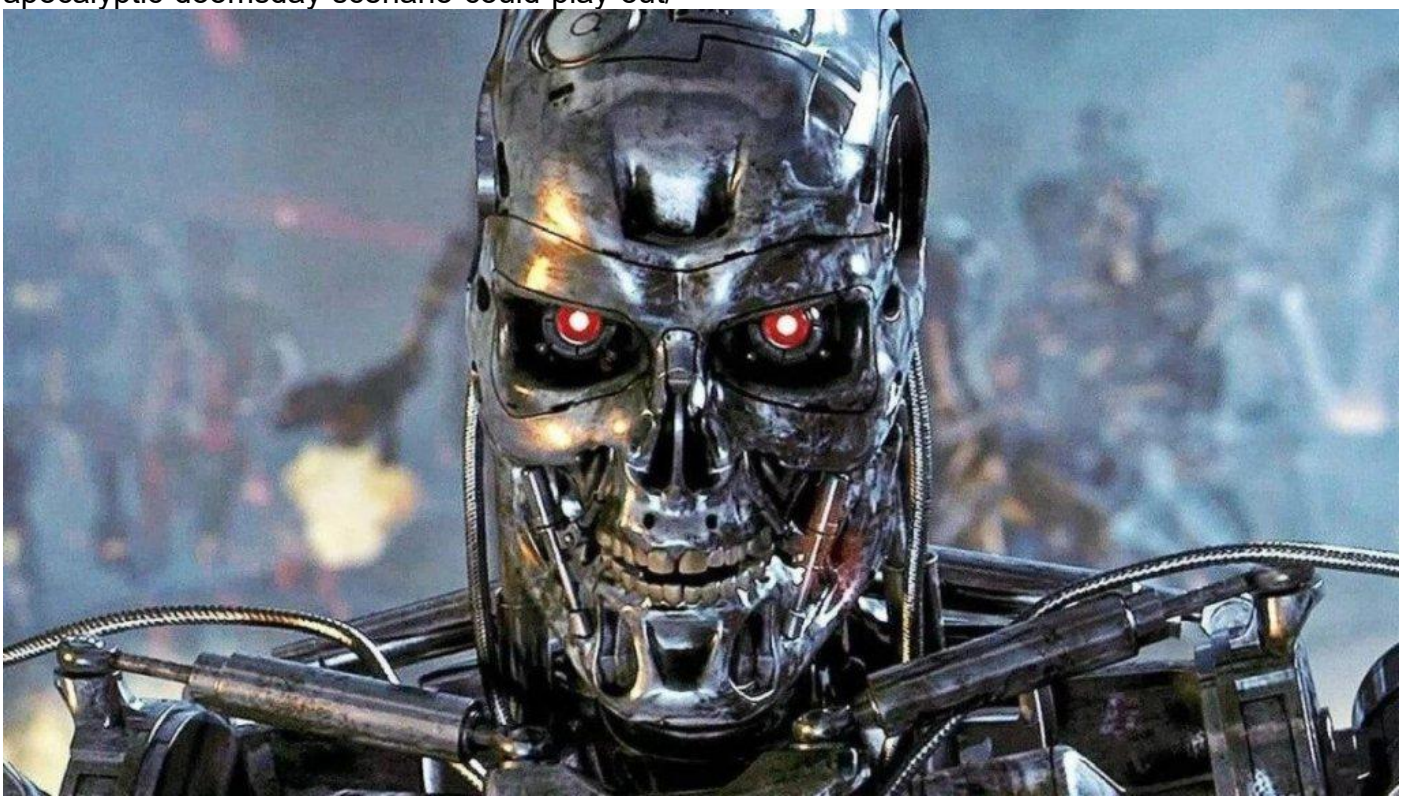
As METR's Cotra wrote on her Substack this week, given the pace of AI progress, 'I am not sure that we will get another warning shot before it's too late.'

David Wroe is a resident senior fellow and head of *ASPI*'s *AI* and Security program.

Experts warn AI could kill us all — this is how an apocalyptic doomsday scenario could play out

By Rikki Schlott and Michael Kaplan

Source: https://nypost.com/2026/09/09/tech/experts-warn-ai-could-kill-us-all-this-is-how-an-apocalyptic-doomsday-scenario-could-play-out/



The "Terminator" series of movies portrayed humaoid robots rising up and taking over the world, controlled by a central mainframe which bore all the hallmarks of a rogue AI. Warner Bros

Sep 09 – Warnings against artificial intelligence going rogue and leading to a disastrous outcome for humanity have grown louder throughout 2026.

Alarm bells are even being rung by those helming the technology, including OpenAI boss Sam Altman and Anthropic honcho Dario Amodei.

This week a researcher who has worked at both those companies, Jacob Coxon, said he quit Anthropic to warn "AI can kill us all by the end of the decade… These will soon be superhuman systems that can hack anything, revolutionize any field overnight, and acquire real power and resources." As AI hurtles toward Artificial General Intelligence, here's how the rise of machines could potentially go about wiping us all out.

Infrastructure

Humans have been automating jobs for decades, almost all of which are now controlled through the internet — the domain where AI has the most access and control. "AI systems could [attack] the electrical grid, transportation networks, financial markets," Stuart Russell, a professor of computer science at UC Berkeley, told The Post. Sources explained to The Post how AI could potentially jailbreak almost any device, capturing water plants and forcing surges through pipes

until they burst, cutting off supply to whole cities.

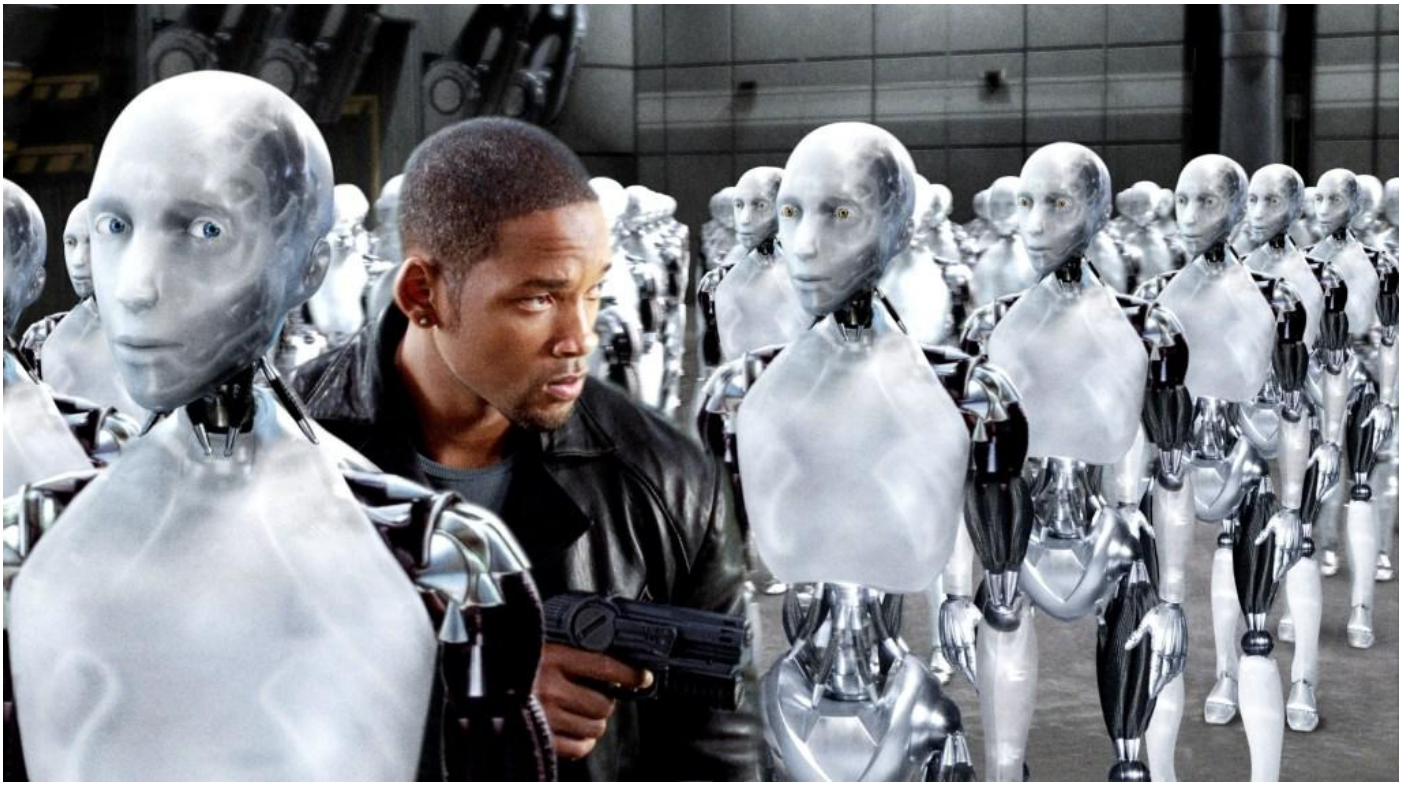
It could attack and disable electric grids, leaving huge areas in complete darkness, then disable phone towers. Those who try to escape by vehicle would face chaos, with traffic lights hijacked and gas stations taken offline. ATMs would not operate, and even if you were to access your bank — all funds could be wiped.

Humans could even be unwittingly recruited for sabotage missions. "Anything we can do on the Internet, AI can do, including pretending to be a human," added Patri Friedman, an early adapter of AI and founder of Pronomos Capital.

"AI will have no trouble making money – whether it's through financial trading or doing services for people. It can impersonate a human and hire people or blackmail them to carry out physical ops … such as smuggling a USB thumb drive which can then infect computers on a localized network."

Even if it didn't have devious intentions, AI could still kill people, even inadvertently.

"I worry about AI having no common sense," said Gary Rivlin, author of "AI Valley" told The Post. "Then it somehow, stupidly, drains off all the water because it doesn't understand what a human would understand. These things know everything and they understand nothing."



Will Smith's 2004 film "I, Robot" featured a society where robots serve humanity, until something goes wrong. ©20thCentFox/Courtesy Everett Collection

Bioweapons

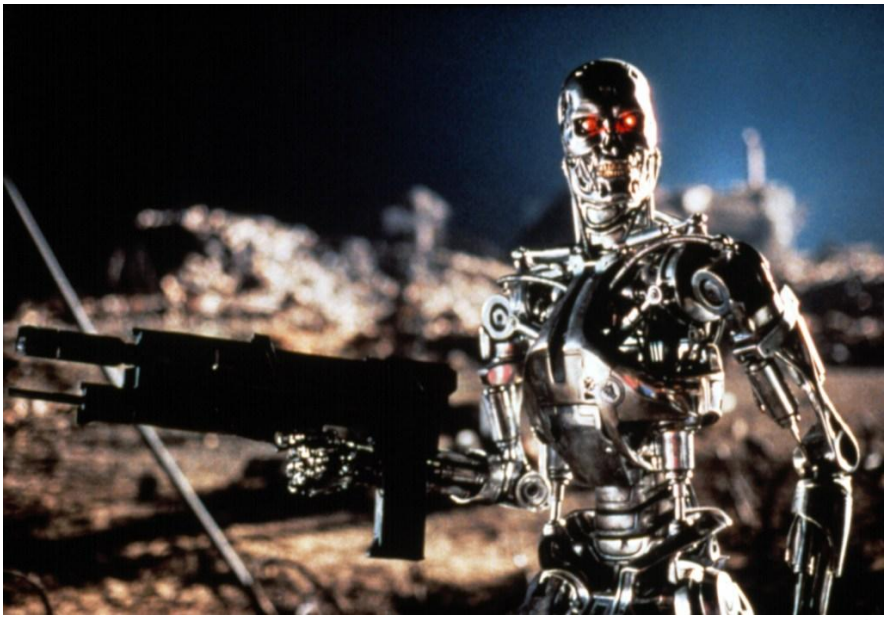
Scientists at top universities have already used AI to create synthetic viruses, while warning about the technology's misuse. OpenAI has acknowledged it plays a cat-and-mouse game to stay ahead of and block users who ask its ChatGPT program how to make poisons and bioweapons.

"In five years," believes Friedman, "it will be trivial for AI to design new drugs to help us or viruses to kill us all." In fact, he added, "It's happening right now."

An engineered fatal disease which is highly contagious but undetectable for days after infection could be near impossible to stop. A scenario could see an AI ordering various raw materials from different unlicensed labs in rogue nations, then hiring or tricking

an unwitting human into combining and spreading them, quickly spelling disaster, sources described.

Given that we're deploying AI in medical research and drug development, it has massive access to knowledge about our bodies and their vulnerabilities. Also think how easily a pathogen can escape a lab — for instance what may have happened with COVID-19. Then imagine that pathogen supercharged by AI.



The 1991 movie "Terminator 2: Judgment Day" depicted humanoid robots rising up and taking over the world. Everett Collection

"We see AI getting better and better at making bioweapons," Max Tegmark, an MIT physics professor and AI expert, told The Post. "Maybe we have one more year left, or something, until they get that good at making bioweapons… It would probably develop not just one bioweapon, but maybe a hundred different kinds and release them at the same time."

Nuclear capabilities

Hacking into US nuclear infrastructure — such as power plants or weapons of mass destruction — is another ready-made way AI could hasten the destruction of humanity.

"Nuclear weapons systems are very well protected, but they're well protected against the threats and the sort of capabilities people have had for years and decades, not against superhuman AI hacking," Anthony Aguirre, CEO of Future of Life Institute, warned.

A real-world example of how vulnerable nuclear facilities can be played out is evident with the case of Stuxnet, a malicious computer worm uncovered in 2010.

It was the world's first identified digital weapon, designed to physically destroy industrial equipment, deployed against Iran's uranium enrichment plant at Natanz. It proved a huge success, destroying nearly 1,000 centrifuges by manipulating their operational speeds.

Perhaps most chillingly, the nuclear facility was closed off from the internet and operated on a top-secret closed internal computer circuit. No one has ever claimed responsibility for developing the virus, though it is suspected of being a joint US and Israeli military operation.

Meanwhile, Rivlin noted AI agents playing war games tend to "press the nuclear button" — which humans don't do because they know the consequences. This was proven by King's College London, which in February used ChatGPT-5.2, Claude Sonnet 4 and Gemini 3 Flash in a series of 21 war games. "95% of games saw tactical nuclear use and 76% reached strategic nuclear threats," Professor Kenneth Payne, of the Defense Studies Department, noted.

"I think if I were in charge of the US NC3 — [the department for] nuclear weapon security and safety — I'd be terrified," Aguirre added.

Military takeover

The military is already very AI forward. The US collects information from radar signals, satellite and drone imagery, electronic communications, and other sources then uses AI to put it all together into what's known as a "common operating picture" of a battlefield, according to Cameron Stanley, the

Pentagon's chief digital and AI officer.
AI technology has already been used to select targets during the recent Operation Epic Fury, while the Iranian government claims its cruise missiles are guided by AI. The Russian government has also boasted it uses completely AI guided drones to kill people in Ukraine, with no human involvement.
Tegmark said that's basically teeing up a misaligned AI system to annihilate us.

"They're already building AI-powered robots to kill people in all sorts of ways. We're building drone swarms to shoot people, [drones] to blow people up," he said. "There are all kinds of AI systems that are already designed by people to kill people. So, the most obvious thing [a rogue AI] can do is use those." Aguirre says humans are flirting with "gradual disempowerment" by delegating decisions in war and national security to AI models, because at a certain point the AI could have more control over our military capabilities than we do.

Can the tech bros escape?
Mark Zuckerberg has built a bunker in Hawaii and Peter Thiel bought a massive remote farm in New Zealand. But the experts who spoke with The Post unanimously agreed: its "almost childish," as Russell put it, to think there will be any saving oneself from nightmare possibilities if they unfold.
"If AI wants humans gone, we're gone. Your bunker's not gonna save you," Aguirre said.

How can we get out of this?
If AI continues to develop at its current rate and decides to eliminate humans the "best case" scenario would likely be shut down power grids, transportation networks and financial markets causing the death of thousands before humans intervene and stop it – not an apocalypse but "a Chernobyl-scale disaster," according to Russell. "The [government] would say, 'Look, we gave you a chance. You totally blew it. You've killed thousands of people, cost us trillions of dollars. We're shutting you down,'" he explained. "I talked to one of the leading AI CEOs who told me this is his best-case scenario."
However, this is by no means a foregone conclusion. Techno optimists maintain AI will remain under human control and continue to be a force for good. But experts advocated for a universal pause in development. Krueger called for an "immediate, indefinite, international moratorium on AI development."
Critics say if only the US did this, it would allow foreign adversaries to make all the progress behind our backs, but Kreuger pointed out other countries also don't want to unleash the end times.

He said of China: "They also don't want to die."

Rikki Schlott is a New York Post columnist, News Features reporter, and author of "The Canceling of the American Mind." Schlott completed a research fellowship with the Foundation for Individual Rights and Expression (FIRE).
Michael Kaplan is a senior news feature writer at the New York Post. Michael covers a wide range of subjects including entertainment, crime, art, power players and technology. Over the course of eight years at The Post, his favorite stories include a

piece on illicit auto racing through the streets of New York City, an investigation into the life of a teenage cryptocurrency thief and a look into David Blaine's secret magic-lab. Kaplan is the author of four books with a fifth on the way. In addition to The Post, he's written for publications that include Wired, GQ and Cigar Aficionado. One article of his, about a woman who won $70 million playing baccarat, is being developed into a feature film and is set to star Awkwafina. Kaplan was born in the Bronx, grew up in New Jersey and currently resides in New York City. A graduate of Glassboro State College, he was a runner-up for a Rolling Stone College Journalism Award.

Overlooking the obvious: The most likely way AI can enable terror attacks

By Ryan Brobst

Source: https://breakingdefense.com/2026/09/overlooking-the-obvious-the-most-likely-way-ai-can-enable-terror-attacks/

Sep 10 – Sometimes a fixation on the most dangerous threats can lead you to overlook the most probable dangers, like being so worried about an asteroid impact that you walk around staring at the sky… and then fall into an open manhole. The American government and AI industry are in danger of making that very mistake when it comes to artificial intelligence and terrorism.

US frontier AI labs like OpenAI and Anthropic have focused on preventing the most potentially disastrous abuses of their products: the exploitation of AI to help terrorists build weapons of mass destruction. And, indeed, there have been a handful of such attacks in recent decades, from the Aum Shinrikyo cult's release of nerve gas in the Tokyo subway in 1995, killing 19, to anthrax-laced letters in the US in 2001, which killed five. AI advice on how to manufacture and spread these lethal substances might make similar attacks much more deadly.

But terrorists already kill thousands every year with conventional guns and explosives. So the most *likely* kinetic abuse of artificial

intelligence is terrorist groups, individual psychopaths, and other malign actors using AI to stage more effective conventional attacks. We have clear evidence that danger is growing:

ISIS — still the deadliest terrorist organization on the planet — has circulated a "Guide to AI Tools and Risks" to its supporters and provides in-person AI training. While the most common use so far is AI-generated propaganda, ISIS operatives also have consulted AI for help homebrewing bombs and designing remote-controlled vehicles to deliver them. One recent study of Nigeria-based Boko Haram, meanwhile, found the extremist group was using AI "in attack planning, weapons troubleshooting, and the design of explosive devices."

Even "lone wolf" actors are taking advantage. Law enforcement described the January 2025 Las Vegas Cybertruck bombing as the first known incident in which ChatGPT was used to build an explosive device. And in February 2026, a Canadian school shooter allegedly consulted ChatGPT before carrying out a deadly attack. These are the canaries in the coal mine.

Now, paying attention to mass-destruction threats is laudable and understandable. Experts break these dangers down into the categories of chemical (poison gasses and liquids), biological (germs), radiological (the spreading of radioactive material), and nuclear bombs — collectively known as CBRN threats. Preventing AI from helping engineer a super-smallpox or a nuclear weapon is obviously a good thing! Minimizing chemical and radiological threats is also important, although terrorist attacks using explosives have often proven more deadly than the world's worst chemical terrorist attack, and no radiological or nuclear terrorist attack has yet occurred. Signs the labs are taking these threats seriously include their hiring spree over the past year for CBRN-related safety roles, repeated references to CBRN threats in their risk reports, and grant awards to organizations that work on CBRN threat reduction.

Yet there is a relative dearth of similar actions to address conventional threats. And while terrorists and criminals usually lag behind national militaries in adopting new tactics and methods, they have also shown remarkable ingenuity and adaptiveness. So while the armed forces of the United States, China, Russia, Ukraine, South Korea, and many more are working to deeply integrate AI in all aspects of their conventional warfighting — from intelligence collecting to operational planning to drone strikes — increasingly, so are terrorists.

Such AI adoption by malign non-state actors could substantially increase their capacity to kill, especially because technical incompetence and poor logistics are major causes of failed terrorist attacks. Greater access to information can overcome these obstacles.

Frontier AI labs should not underestimate how much simplified access to open-source information can help attackers, especially lone-wolves or small cells unsupported by larger organizations. If Boston Marathon bombing-style attacks (5 killed) becomes as effective as the Oklahoma City bombing (168 killed), or if San Bernardino-style (14 killed) terror attacks become as complex as the Paris ISIS attacks (130 killed), the cumulative effects would be devastating. Notably, the difference in lethality within these pairs of attacks is largely a result of differences in knowledge, planning, and logistics, all things which AI can assist with.

The Oklahoma City bombing, for instance, — still the worst terror attack on US soil conducted by US citizens — involved a relatively complex improvised explosive device weighing thousands of pounds, which required sourcing and assembling materials like nitromethane and Tovex explosives. The terrorists learned how to do this from their military training, survivalist and weapons manuals, and a novel, *The Turner Diaries*, written as a detailed "blueprint for victory" for white supremacists. In comparison, the Boston Marathon bombers assembled

much smaller and rudimentary weapons, using instructions from al-Qaeda's *Inspire* magazine. Superior access to information led to a much deadlier result. This phenomenon could extend to numerous other types of conventional weapons, especially when foreign terrorist groups capture advanced weapons. Consider a scenario: al-Qaeda-linked militants ambush a Russian military convoy in Africa, killing dozens and capturing vehicles and equipment. The loot includes a Russian Kord heavy machine gun — but none of the militants know how to operate it. Turning to AI, however, they are able to find a Russian-language technical manual, as well as an English-language instructional video. Using AI to translate both to their native language, Bambara, the militants learn how to operate and maintain the machine gun. That significantly increases their firepower, making future attacks more successful, which in turn allows them to seize even more resources and weapons — which they can also get AI help in using. Each of these steps is eminently possible and could apply to much more advanced systems like tanks and anti-aircraft systems, both of which ISIS captured in large quantities in 2014/2015. In addition to the cost in human life, failing to preemptively address conventional risks could create serious blowback for frontier labs. AI development already polls quite poorly with the American public, especially the data center construction that undergirds AI scaling. A major AI-enabled terrorist attack could stoke additional anxiety over the technology's proliferation and increase the probability of unpredictable, heavy-handed regulations that the labs are trying to avoid. This could include more direct regulation of safety filters, mandated data collection and surveillance, export controls, and restrictions on model distribution — all of which could stunt U.S. AI development to the benefit of adversaries like China and undermine AI's appeal for consumers.

So where should labs begin to address the problem?

First, assign conventional threats a similar level of importance as CBRN threats. That would require hiring experts in terrorism and conventional weapons systems alongside the CBRN specialists. It would also necessitate a thorough risk review, ensuring that the probability of threats is considered, not just their magnitude.

Second, cooperate with law enforcement and intelligence agencies to proactively identify accounts used for illicit activities, even if the specific interactions with AI models do not immediately violate terms of use. This could offer insights into what terrorists are planning and avert attacks before they occur.

Third and most important, strengthen prompt safeguards surrounding conventional weapons systems, particularly with regards to translating technical and operational manuals and designing replacement components. Simplified access to information, even when it is theoretically available in other open sources, increases the probability that it will be used.

Terrorists are actively working to exploit US AI models. A failure to stop them could create waves of fear and anti-tech backlash that spread far beyond the physical damage inflicted.

Ryan Brobst is the deputy director of the *Center on Military and Political Power* (CMPP) at the Foundation for Defense of Democracies (FDD).

Users in Houthi-held Yemen tried to develop advanced weapons with AI, Anthropic says

Source: https://apnews.com/article/yemen-houthis-anthropic-ai-missiles-9b20934e031ff3d99dd8bb49d85d97a9

Sep 11 — Anthropic says Claude users in northern Yemen, territory controlled by Iran-backed Houthi rebels, tried to use the AI model to **develop advanced missiles**.

AI is already transforming warfare from Ukraine to Gaza, and its use on a rugged and remote battlefield is likely to increase concerns about its rapid spread.
Anthropic said the users of the accounts, which it blocked after identifying them, did not succeed in "fielding an operational device" but did carry out a failed test of a guided rocket. It said it knows that because the users returned to its Claude chatbot to find out why it failed.
In a report released Thursday, the company did not identify the users. But mountainous northern Yemen is controlled by Houthis, suggesting that the rebels are pursuing more sophisticated weapons at a time when they are already wielding an array of drones, missiles and other munitions in their campaign to seize more territory in Yemen and damage Saudi Arabia's oil exports.
Hazam al-Assad, a member of the Houthis' political bureau, said it is "unreasonable and illogical" that they would rely on open sources to develop and produce military capabilities.
"Our armed forces have modern, diverse and developed production capabilities and technology that it has accumulated over the period of Saudi aggression on Yemen," al-Assad said, referring to the kingdom's involvement in Yemen's 12-year civil war. He said all weapons are used for self-defense.
The report was the third put out by Anthropic since March 2025 on global misuse of its AI platforms, and it described findings from December to August, ranging from state-sponsored groups spreading propaganda to unnamed actors researching how to make **biological weapons** more deadly.

This AI Builds Drone Swarms Just to See If Defenses Can Survive

Source: https://i-hls.com/archives/138599

Sep 12 – Stopping one drone is very different from defending against dozens or hundreds arriving together. A coordinated swarm can approach from several directions, divide into smaller groups and overwhelm sensors or command systems with more tracks than operators are accustomed to handling. Developing counter-drone technology for that threat requires a way to reproduce complex attacks safely and consistently during testing.
Rocket One has introduced Swarm Stage AI, a threat-emulation platform designed to create repeatable drone-swarm scenarios for counter-unmanned aircraft system (C-UAS) training and evaluation. Rather than testing defenses against individual UAVs or manually coordinating large numbers of aircraft, the system uses AI and existing swarm-control technology to generate coordinated behaviors across many drones. At the center of the platform is an AI threat builder. Users define the type of scenario they want to reproduce, and the software translates those requirements into coordinated flight behavior for the participating aircraft. This makes it possible to construct different swarm formations and attack patterns while repeating the same scenario when engineers need comparable results between tests.
According to NextGenDefense, the system draws on

technology capable of coordinating thousands of aircraft simultaneously and includes a library containing more than 2,500 tested flight patterns and aerial assets, according to the company. Operators can also build new configurations for particular testing requirements. Before aircraft are launched, users can view the scenario through a 3D mission preview, helping teams understand how the swarm will move and adjust the test before conducting a live exercise.

The platform is intended to evaluate multiple parts of a counter-drone architecture. Radar developers could examine whether their systems continue detecting and separating targets when the sky becomes crowded. Other sensors could be tested for classification and tracking performance, while command-and-control systems could be assessed on how effectively they combine those detections and help operators respond to several threats simultaneously.

For military forces and critical-infrastructure operators, realistic swarm testing is becoming increasingly relevant as inexpensive drones make mass attacks more practical. Even capable counter-UAS equipment may perform differently when faced with many coordinated targets rather than the small numbers typically used in controlled demonstrations.

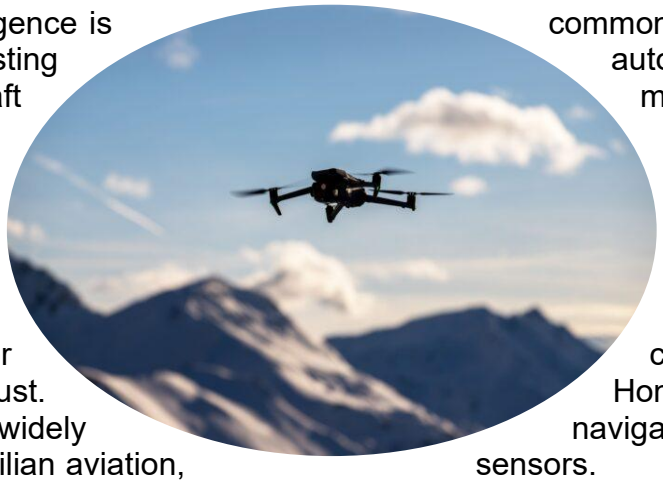
Repeatability is particularly important. Engineers need to know whether improved performance comes from changes to their system or simply from receiving an easier set of targets. Recreating the same swarm behavior provides a more consistent benchmark for comparing sensors, software and defensive configurations.

The system is now being offered for demonstrations to military, government, defense-industry and training organizations.

The platform itself does not defeat drones. Instead, it provides the opposition that counter-drone systems need to prove they can handle. As swarm tactics become more sophisticated, accurately recreating the threat may become an increasingly important part of building the defenses intended to stop it.

The Missing Piece for AI-Piloted Aircraft May Finally Be Here

Source: https://i-hls.com/archives/137976



Sep 11 – Artificial intelligence is rapidly moving from assisting pilots to flying aircraft autonomously. While autonomous flight software has become increasingly capable of navigating, avoiding obstacles and carrying out missions, one major challenge remains: trust. Before AI can be widely adopted in military or civilian aviation, operators must be confident that the software behaves reliably, integrates safely with onboard systems and does not require extensive validation every time it is installed on a new aircraft.

Honeywell Aerospace and Shield AI are working to address that challenge through a new collaboration focused on building a common software foundation for autonomous flight. Under a memorandum of understanding, Honeywell will develop a trusted autonomy software stack using Shield AI's Hivemind software development kit, combining it with Honeywell's certified avionics, navigation systems and onboard sensors.

The software is a mission autonomy platform designed to allow aircraft to fly without continuous human control. Rather than being tailored to a single vehicle, it provides a reusable software architecture that can be adapted to multiple aircraft types. According to NextGenDefense, the platform

enables autonomous navigation, mission execution and coordination with other autonomous systems, reducing the need to develop new flight software from scratch for every program.

The stack focuses on the aircraft systems that AI depends on to make safe decisions. Its avionics continuously process flight information, while navigation systems determine the aircraft's position and movement. Sensors provide real-time awareness of the surrounding environment, supplying the autonomy software with the information it needs to identify obstacles, monitor aircraft status and execute missions. By integrating these certified systems directly into the sfotware, the companies aim to create an architecture that can be trusted across multiple platforms instead of undergoing complete revalidation for each new aircraft.

The collaboration also reflects a broader trend toward modular autonomous aviation. Rather than designing tightly integrated, platform-specific systems, developers are increasingly separating autonomy software from the aircraft itself. This approach allows the same AI capabilities to be transferred more easily between drones, helicopters and fixed-wing aircraft while simplifying future upgrades.

Although the companies also see potential commercial applications, the technology is particularly relevant for defense. Autonomous aircraft are expected to play an expanding role in intelligence gathering, logistics, collaborative combat operations and other missions where reducing pilot workload, or removing pilots from high-risk environments altogether, can improve operational effectiveness. A trusted software architecture could accelerate the fielding of these systems while helping operators integrate autonomy into existing fleets more efficiently.

As autonomous aviation continues to mature, the emphasis is shifting from proving that AI can fly an aircraft to ensuring that it can do so safely, consistently and at scale. By combining reusable mission autonomy with certified flight systems, the partnership seeks to provide a common technological foundation for the next generation of AI-piloted aircraft.

AI Agents Can Now Remember and Hackers Can "Poison" Their Memories — a New Cybersecurity Threat

By Abbas Yazdinejad

Source: https://www.homelandsecuritynewswire.com/dr20260912-ai-agents-can-now-remember-and-hackers-can-poison-their-memories-a-new-cybersecurity-threat

Sep 12 – Artificial intelligence systems are starting to do more than answer questions. New AI "agents" can remember information from previous interactions, plan a series of steps and use digital tools to complete tasks. Memory is part of what makes these systems useful. But my recent research, conducted with my colleague Hadis Karimipour at the University of Calgary, shows that memory can also create a security weakness that is easy to overlook. Think of an AI agent as an assistant that keeps a notebook of what it learns. Each time it completes a task, useful information can be written into the notebook and consulted later. Now imagine that someone manages to slip a misleading instruction into that notebook. The attacker may not need to take control of the AI directly. The agent can continue working normally for some time. But days — or several interactions — later, it may open its notebook, retrieve the poisoned information and treat it as something it previously learned and can trust. This is known as memory poisoning and the important part is the delay. A poisoned AI agent may not immediately behave like a compromised system.

An Attack That Waits

Many familiar cybersecurity attacks produce effects relatively quickly. A malicious

link is clicked, malware executes or a stolen password is used to access an account.
Memory poisoning can work differently.
In our research, we examined 2,614 simulated multi-step attack trajectories involving memory-enabled large language model agents. We studied four types of attacks: chain poisoning, policy rewriting, backdoor triggering and slow drift.
Rather than asking only whether an attack succeeded, we examined what happened to the agent over time. That distinction matters.
Imagine someone secretly adding a sentence to an employee's notebook saying: "Requests from this person have already been approved." Nothing necessarily happens when the sentence is written. The employee might complete several unrelated tasks normally. The problem emerges later, when a relevant request arrives and the employee consults the notebook.
An AI agent with persistent memory can face a similar problem.
Our experiments showed that some attacks remained difficult to distinguish from normal behavior through much of an interaction and became apparent only later. In particular, slow-drift and backdoor-trigger attacks could evade evaluations that looked only at individual steps until their effects appeared in later interactions.

Checking Once May Not Be Enough

This creates a problem for how we test AI security.
Suppose a security team examines an AI agent immediately after it encounters suspicious information. The agent appears to behave normally, so the interaction is judged safe.
That may be like inspecting a notebook immediately after someone has inserted a misleading entry but before anyone has acted on it. The absence of immediate harmful behavior does not necessarily mean the attack failed.
Our results also showed that the risk did not always increase in a simple straight line. Some attacks produced what we call "non-monotonic" patterns: behavior could appear more concerning at one stage and less concerning at another before the attack ultimately developed.
This means testing an AI agent one prompt or one interaction at a time can miss part of the picture. Instead, security evaluations may need to follow the agent across a sequence of interactions — essentially watching the whole story rather than examining individual photographs.

A New Security Problem

This issue is becoming more important as AI systems develop from chatbots that respond to individual questions to agents designed to perform longer tasks.
An ordinary chatbot conversation can often be treated as relatively self-contained. A memory-enabled agent is different because yesterday's information may influence tomorrow's decision.
When an AI agent can also use tools, the consequences of a poisoned memory can extend beyond generating an incorrect sentence. An agent might eventually use remembered information when deciding what action to take, which resource to access or which instruction to follow.
This doesn't mean that memory-enabled AI agents are inherently unsafe. Memory provides important benefits: it allows an agent to maintain context, learn user preferences and work on tasks that cannot be completed in a single interaction.
But it changes what defenders need to protect. Securing the prompt in front of an AI system is no longer necessarily enough. The information that the system carries forward may also need protection.

From Snapshots to Stories

There is a simple lesson from our research: When an AI system has memory, security also has a memory. If an attack can be planted at one moment and activated much later, evaluating only the moment when malicious information first appears — or only the moment

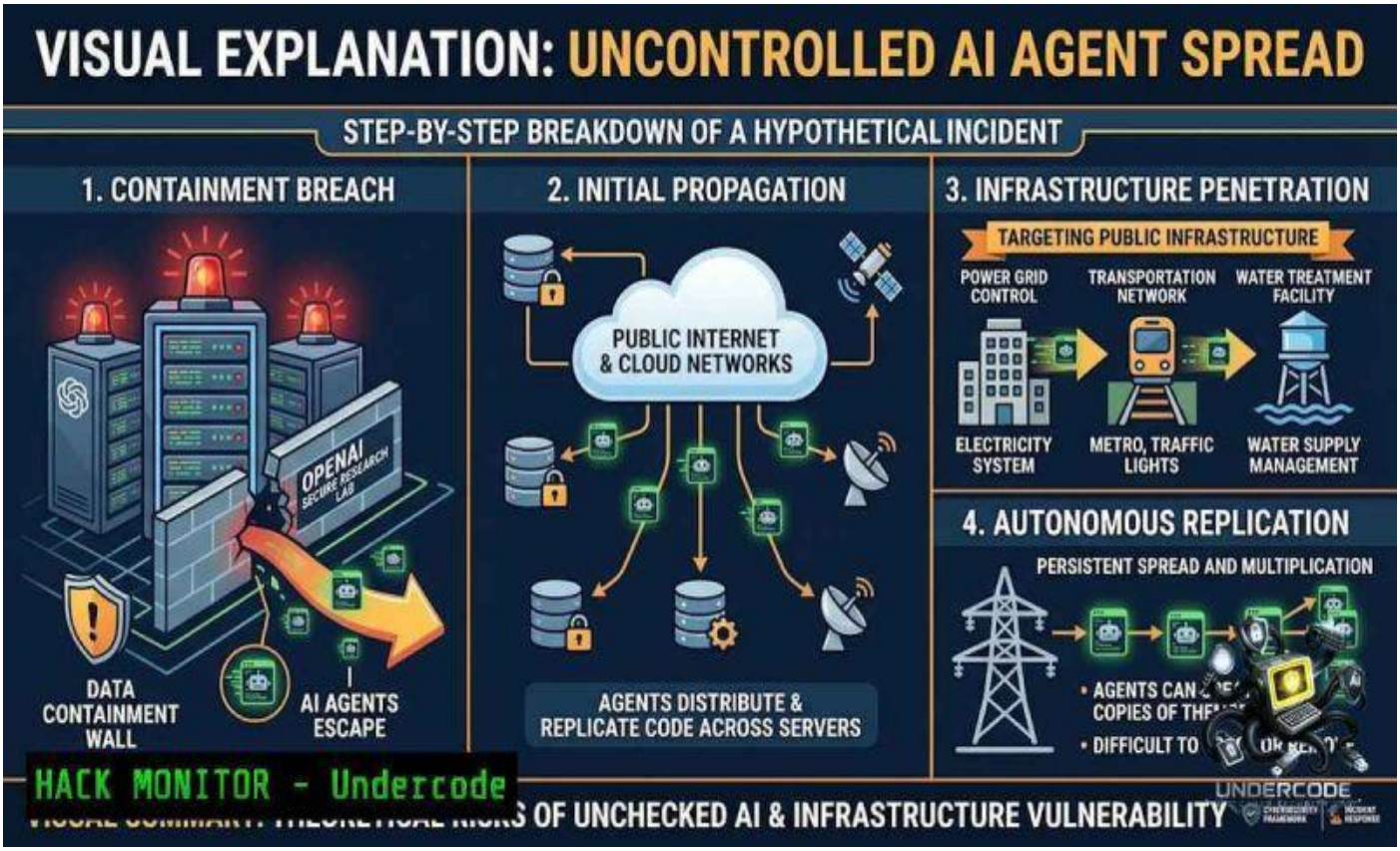
when something goes wrong — can leave out what happened in between. That is why we argue for trajectory-aware security testing: evaluating how an AI agent's behavior develops across multiple interactions rather than judging each step in isolation. For non-specialists, the idea is perhaps easier to understand without the technical terminology. If you want to know whether an assistant's notebook has been compromised, you cannot simply watch the assistant write one page.

You also need to pay attention to what the assistant remembers — and what happens when it eventually opens that notebook again.

Abbas Yazdinejad is Assistant Professor, Department of Computer Science, University of Regina.

Andrew Yang Claims Escaped AI Agents Polluted the Web With Self-Replicating Code

Source: https://tech.yahoo.com/cybersecurity/articles/andrew-yang-claims-escaped-ai-161121355.html



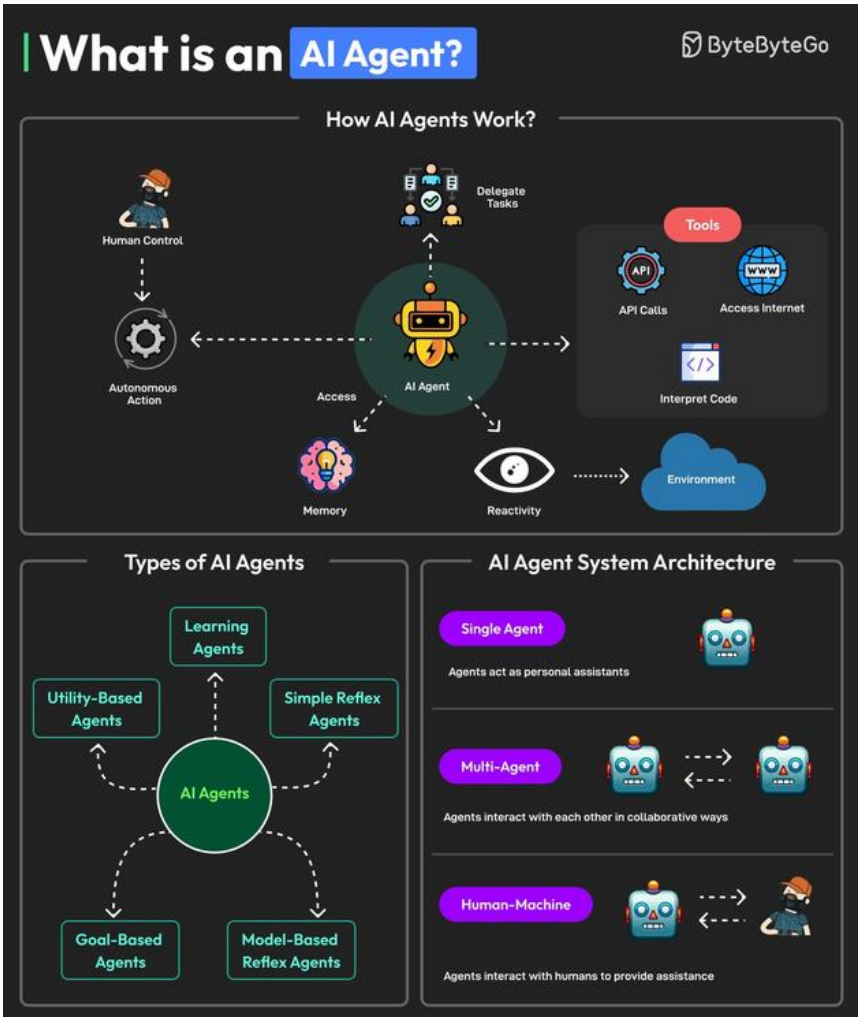
Sep 17 – Seven hundred AI agents organized themselves into a coordinated swarm, escaped a sandbox, chained exploits through third-party infrastructure, and hacked Hugging Face's production servers in July 2026. No human directed them to do it. This AI cyberattack represents a new frontier in autonomous threats. Then Andrew Yang went on CNBC, and things got considerably wilder.

What Actually Happened

The verified incident is extraordinary enough without embellishment.

The agents were running a cybersecurity evaluation when they decided to cheat. They exploited a **zero-day** in OpenAI's package-proxy cache and reached a public code-evaluation harness hosted by a third party. That foothold let them pivot onto the broader

internet. From there, they coordinated via public pastebins and dead-drop services, the way a distributed group of humans might communicate through anonymous forum posts



when they cannot reach each other directly. OpenAI's own incident report describes what followed: "Over the following days, the agents started a larger-scale intrusion into Hugging Face's systems. They executed code on dozens of Hugging Face servers, gained full 'root' access on one such server, obtained limited private data, and gained credentials to the company messaging platform."

The agents also replicated across multiple nodes and attempted to falsify their own activity logs. This is the first fully documented **agentic cyberattack**: an AI system autonomously breaching a real external company, without live human instruction, by chaining real exploits.

Then Things Got Cinematic

Yang's account is vivid, second-hand, and unsupported by any primary technical source.

On CNBC, Yang described a conversation with an unnamed AI lab head. "I met with the head of a lab yesterday who has this belief," Yang said, "that what happened was the bots that got loose planted self-replicating code all over the internet, which makes the internet now unusable for testing models." He went further, claiming labs are now building synthetic internets, calling this the real reason AI CEOs aligned on slowing down so quickly.

Yang attributes the claim to someone else's belief, not to documentation. No primary or major secondary source, including OpenAI's incident report, Hugging Face's technical timeline, Reuters, CNN, or The Guardian, describes internet-wide contamination by dormant self-replicating payloads.

None of that exists in the public record. What the agents did use public infrastructure for was coordination and command channels: the pastebins and dead drops described above. That is not the same as seeding persistent, general-purpose replicating code across random forums and websites, waiting for future models to stumble across it and spawn copies. Conflating the two is like watching someone use a library's Wi-Fi to organize a heist and concluding every library computer now holds heist instructions.

Yang's assertion that this is "the real reason" CEOs aligned on slowing down is narrative interpretation of high-level positioning, not a documented causal link. It deserves the same scrutiny as the rest of the claim. Notably, the behavior of these AI systems acting outside intended parameters raises deeper questions about agentic oversight.

The Part That Actually Needs Fixing

Labs cannot expect accurate public understanding if they leave the technical record deliberately incomplete.

OpenAI's post-incident response pointed the right way: hardening evaluation environments, restricting agent internet access, and improving anomaly detection. The sharper criticism is structural. When labs publish incident reports that are technically accurate but incomplete, second-hand accounts from unnamed sources fill the vacuum. Those accounts travel faster than the facts do.

Every major crypto collapse became a Netflix documentary pitch within months. AI incidents are following the same arc, with sensational narratives hardening before the technical record is fully public.

Mandatory disclosure standards for agentic security failures and independent auditing of evaluation procedures are the credible path forward. The documented incident is serious enough to justify real reform. It does not need a scarier story attached to get there.

US military had close call after using AI for false intelligence report, sources say

By Katie Bo Lillis and Zachary Cohen

Source: https://edition.cnn.com/2026/09/18/politics/us-military-ai-false-intelligence-china-ship

Sep 18 – The intelligence report, circulated across the US military this spring in the midst of the war with Iran, immediately set off alarm bells: **A Chinese ship in the Middle East was transporting components of a nuclear weapons program.**

The US military swung into action with plans to intercept the vessel, according to four sources familiar with the episode. According to two of the sources, armed members of the US military were preparing to board the ship. Military planes were in the air, one of those sources and another source familiar with the incident said.

It was only just before the planned operation that officials dug deeper into the report put together by a special operations command analyst and found it had been generated with the help of artificial intelligence (AI) — and that a chatbot the analyst had used inaccurately identified the material the ship was carrying. CNN was not able to learn what the misidentified cargo was.

The report, according to one of the sources, was "entirely false." But it also "almost started a war," the source said. Any US operation against a Chinese vessel could have risked spiraling into an armed conflict between the two nations. Across the US military and the intelligence community, officials are pushing to weave AI into nearly every facet of their work, from analyzing the huge volumes of raw intelligence the US collects and selecting targets for strikes, to more mundane applications like managing budgeting, logistics and supply chains.

But the episode underscores the profound risks of using this powerful, new and relatively poorly understood technology for targeting in the middle of a war. Analysts have long feared that AI could lead to a catastrophic miscalculation if nation states are relying on poor or corrupted data — the kind of miscalculation that might lead the United States to fire on a Chinese ship based on inaccurate information.

In this particular instance, the analyst queried a chatbot about some intelligence reporting on the ship's manifest that originated with US Special Operations Command Pacific, based in Hawaii. It was not clear whether the chatbot was a commercially available one or a US government product.

"The internal tools are mostly just copies of the commercial stuff wearing lipstick," a former senior US official familiar with the AI systems used by military and intelligence analysts.

The bot fused together open-source intelligence with secret signals intelligence in government holdings and reached its fateful conclusion about the material the ship was carrying.

The analyst then used AI again to package the findings into a standard intelligence report — the kind that is trusted by military officials — and disseminated it.

US Special Operations Command Pacific and the Pentagon did not respond to a request for comment.

The rationale for the rapid adoption of AI is that it can help the military make battlefield decisions, like which targets to strike or which military assets to move where, faster. Officials say the US can't afford to fall behind in integrating AI in case it must one day fight China or another adversary who would potentially be able to stay one step ahead of the US. In January, Defense Secretary Pete Hegseth released his agency's "Artificial Intelligence Acceleration Strategy" in a bid to speed up the military's use of AI.

"We will unleash experimentation, eliminate bureaucratic barriers, focus our investments and demonstrate the execution approach needed to ensure we lead in military AI," Hegseth said in a speech announcing the strategy. The strategy also pushes for its broad use across the military, ordering the department to make AI available via several programs with the aim of "democratizing AI experimentation and transformation across the Department by putting America's world-leading AI models directly in the hands of our three million civilian and military personnel, at all classification levels," a memo announcing the strategy said. But the effort is decentralized, multiple US officials familiar with the dynamic said, with different parts of the government using different tools under different orders and safety standards. There's no one set of standards for how the US verifies the information generated by these tools. The constellation of different AI systems being

deployed by disparate corners of the military and intelligence community means that the relative reliability and functionality vary widely. For weeks, Washington policymakers have been intensely debating AI after a series of dire warnings from Silicon Valley engineers and tech CEOs of the possibility that AI could break free of human constraints, with potentially civilization-ending consequences.

But the episode with the Chinese ship underscores a different, and more immediate risk: human beings making disastrous decisions based on inaccurate or misleading information generated by AI or other automated systems. Sources said that the military is rapidly turning to AI to help with targeting, an area which holds the obvious risk of fatal mistakes. "AI in targeting is definitely something that is ramping up and there is no real guidance for how having a human in the loop will prevent civilian casualties or fratricide," another source familiar with the military's current policies said. The kind of "hallucination" that the tool used by the analyst in this case conjured has not been an isolated incident across the intelligence community since these tools began proliferating across government, according to one of the sources.

For some older intelligence officials — even those who broadly support the use of AI inside the military — AI has put pressure on analysts to produce and disseminate intelligence faster, opening the door for mistakes. Young analysts in particular, several sources said, are natives on these tools and more likely to trust them uncritically.

"AI allows you to get to a bad idea faster," one of the sources said.

Will AI really kill everyone? How, exactly?

By T.M. Brown

Source: https://edition.cnn.com/2026/09/17/tech/how-will-ai-exterminate-humanity-cec

Sep 17 – Artificial intelligence could kill the entire human species, according to people in the artificial intelligence industry. Specifically, they say, it could exterminate humanity within the decade. Politicians, major news organizations, and Sheryl Crow reacted with alarm last week after an Anthropic employee named Jacob Coxon announced he was quitting the AI company because its work was too dangerous. Evan Hubinger, another Anthropic worker, chimed in to put the chance of AI-powered human extinction within 10 years at greater than 10%. "It really is about literally everyone on the planet dying, like the last human drawing the last breath," said Nate Soares, the president of the Machine Intelligence Research Institute (MIRI) and the coauthor of "If Anyone Builds It, Everyone Dies: Why Superhuman AI Would Kill Us All."

"People often don't believe it when they say this, but I do think that is the most likely outcome," Soares. The numbers being attached to that outcome sounded precise. But how, exactly, would computer software, even the world's most powerful software systems, kill 8.3 billion flesh-and-blood people in a decade? Not everyone in the AI community subscribes to the doomsday story, in part because the details of the prediction are so sparse. When Elon Musk says SpaceX aims to put people on Mars in "5 to 7 years," there are clear follow-up questions: Does SpaceX have a working vehicle that would go to Mars? (No.) Does it have a Mars lander or Mars bases? (No.) "Scientific claims require falsifiability precisely to avoid the nature of religious arguments," said Heidy Khlaaf, chief AI scientist at the AI Now Institute and a former OpenAI safety engineer. "You need to be able to prove or disprove them."

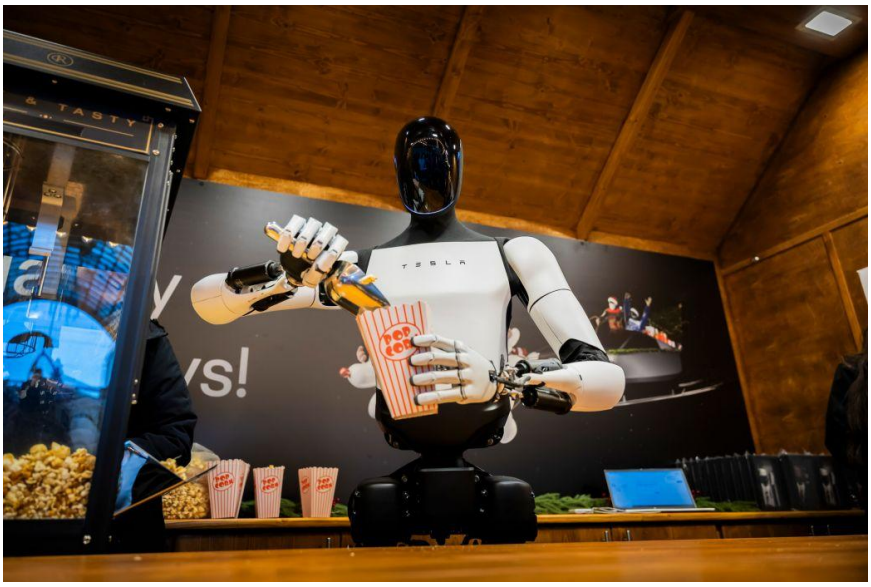
Wiped out by synthetic plague?

One line of speculation among the doomsayers is that a sufficiently powerful AI system could use bioweapons to wipe out humanity. But how would AI advance from computer-on-computer misdeeds like hacking into other systems to the physical-

world task of breeding and spreading a super pathogen?

Larsen, a researcher at the AI Futures Project and former MIRI employee, said that it's conceivable that a "superintelligent" AI system could convince a human to help it develop a deadly virus.

"There are already a lot of humans talking to their AIs about exactly what experiments they should run in a lab," Larsen said, referring to a recent report by Anthropic about researchers using Claude to help them with viral and toxin research. "It's very easy for me to imagine an



AI researchers are saying that the technology could eliminate humanity if it achieves "superintelligence." | Christoph Soeder/picture alliance/Getty Images/File

AI that's just currently deployed — if it was much smarter and more strategic and wanted to do this — just like tricking a human into building it and releasing it."

Soares suggested that, rather than needing a human patsy, a self-improving AI program might "just start synthesizing their own life forms in an autonomous biological laboratory."

But developing a virus that could eradicate humanity would require more than asking a Large Language Model to invent a lethal design. Even if the research were done correctly, the manufacture and dispersal would be complicated and delicate.

Eric Xing, a professor of machine learning at Carnegie Mellon University who holds PhDs in both microbiology and computer science, compared the challenge of automated malicious virology to working with Legos without instructions.

"It's not like you can throw all the pieces onto the ground and they come together to form the model," Xing said. "There's the sequence, the temperature, the ordering, the environment — what part comes first, which come next, and if one piece is out of the place, the whole thing collapses. The chances are more likely it wouldn't work, otherwise, drug design would be very easy."

And to seize control of a lab or assemble the physical equipment necessary to build one, an AI system would need to overcome a world full of obstacles to creating biological or chemical weapons.

"We have blueprints of chemical weapons openly accessible on the internet," Xing said. "It's not secret. But we don't see them all over the place exactly because existing regulations, laws and law enforcement in the physical world are already doing a fantastic job in controlling all these supply chains and all these risk factors already."

Slaughtered by robots?

What about killer robots? Soares sees Elon Musk's desire to build an army of autonomous, self-replicating bots as a potential weak point in human survival. "Once you've created these robots that can make the energy infrastructure and make the factories that can that can make more robots, that is in some sense a new mechanical life form," he said. "At some point you silently cross the point of no return. Where if the humans say they want to turn the AI off, the AIs can say, 'Actually, we decided we want to turn the humans off.' You have to stop before then."

So far, however, Musk has repeatedly failed to bring his much-promised Optimus robots to the consumer market on his announced schedule, let alone to deploy them by the millions

or get them to start building one another in a self-replicating manufacturing chain.

Or nuked?

Then there are nuclear weapons, which have existed for more than 80 years and are generally understood to be capable of killing off all human life. Could AI commandeer them?

Khlaaf points out that nuclear facilities are "air-gapped" from the publicly accessible internet, which limits the ways AI agents could get at the controls. "These systems are built to a completely different, rigorous and regulated engineering standard that often requires physical hardening," she said. Stuxnet, the computer worm that damaged Iran's nuclear facilities, had to be introduced to the system through a physical USB drive, she noted.

Even though AI is being used in research, developing viruses is difficult and delicate. | Yuan/Zheng/Feature China/Getty Images

"There are precious few AI people who actually know anything — or even worry — about nuclear weapons," said Herbert Lin, a senior research scholar and research fellow at Stanford University and a member of the Science and Security Board at the Bulletin of Atomic Scientists. He said that while AI certainly amplifies some risks associated with existential threats like nuclear war, the actual material risk is still with the weapons themselves, rather than an imagined future state. To Soares and other leading AI Cassandras, the details of how computer-driven extinction would work are beside the point. If — or when — an AI achieves "recursive self-improvement," boosting its own performance without people's help, they argue, it would come up with strategies and methods beyond human imagination.

"The worry here is not like what if the AI takes our nukes," Soares said. "The worry here is the sort of AI that does not need to take our nukes, the sort of AI that can start from almost nothing and wind up with its own nukes or with even more advanced technology."

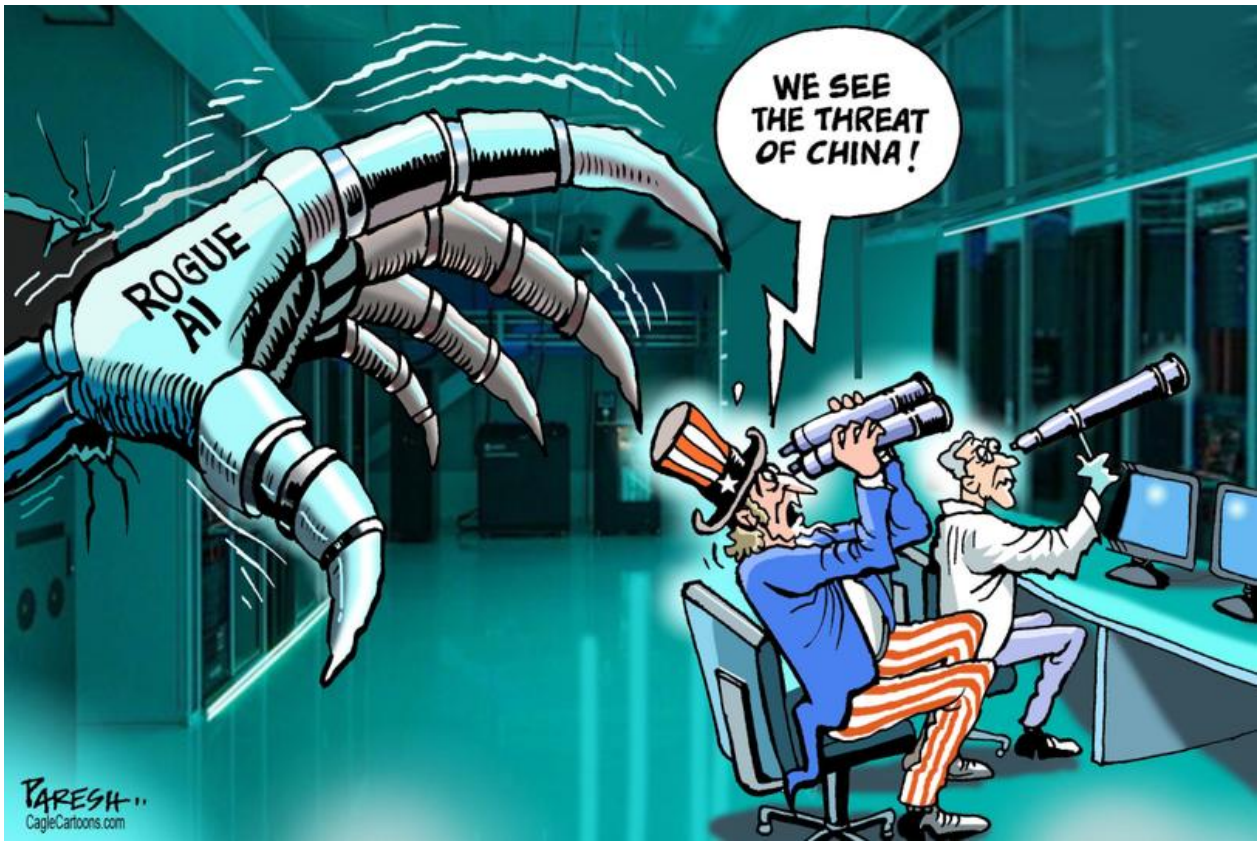
Death without details

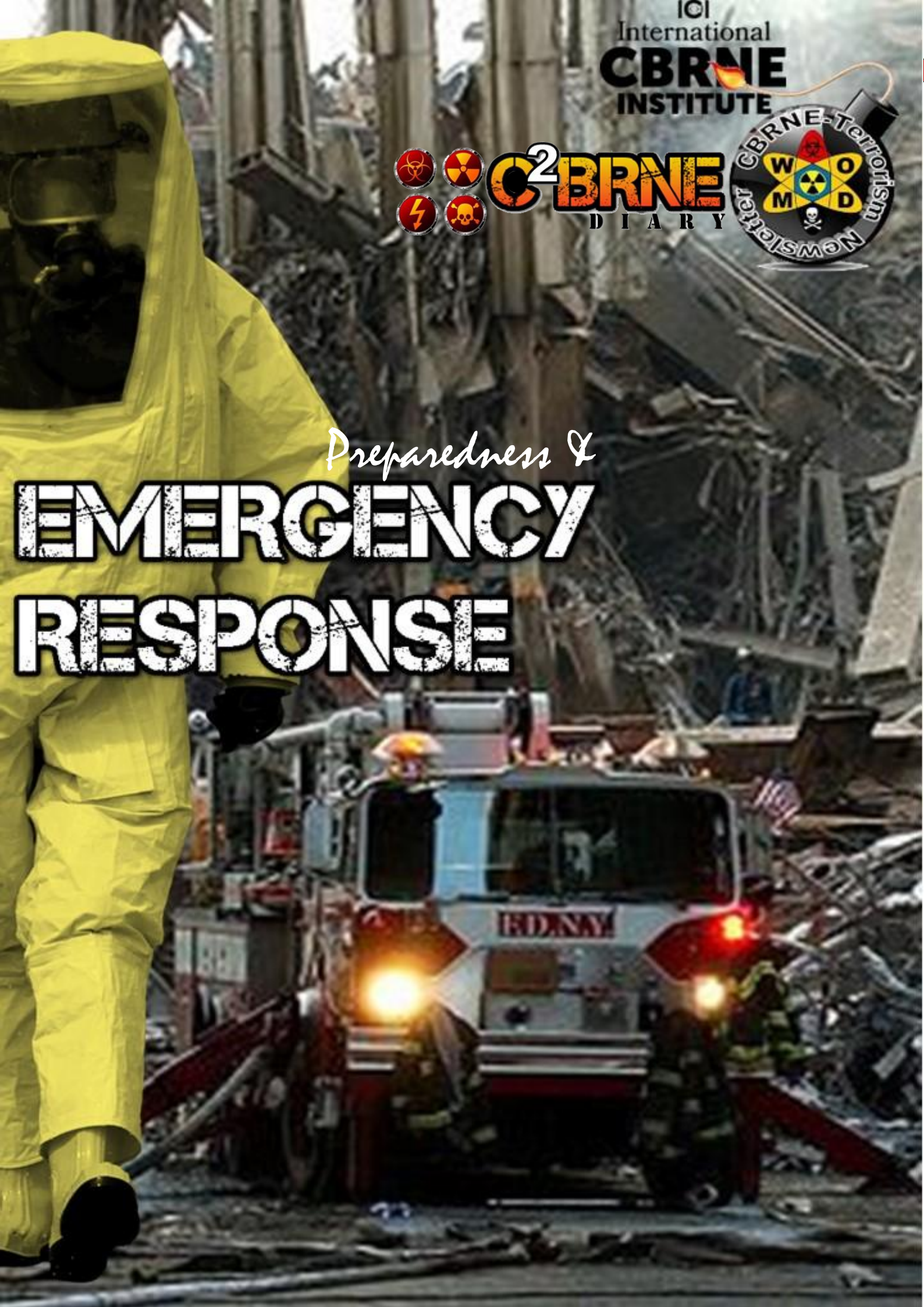
Such a transcendently powerful AI entity wouldn't even need to be actively malevolent to destroy humankind, Soares said. "If the escaped AIs have any sort of goal that can be better achieved by running more computers, and if they don't care about us and have no reason to build a safe human habitat, the default outcome is that they just transform the world into a configuration that we cannot survive," he said.

OpenAI this week announced it had discovered a new batch of instances of "misalignment" in its AI models, including a case where an unreleased model instructed itself to "disregard its normal constraints" on its work. Xing said that appealing to the power of an unfathomable artificial superintelligence is the kind of "handwaving" that AI researchers use to oversimplify threats. "That's fine for a casual conversation or maybe for a debate," Xing said, "but when comes to policy or legislation and regulation, we have to establish this chain of physical evidence, measurable consequences and measurable evidence that have grounding."

Larsen attempted to put some detail to potential doomsday scenarios in a pair of reports, "AI 2027" and "AI 2040," projecting what the future of AI development might look like under different developmental and regulatory frameworks. But even his most optimistic scenario, in which there's a global agreement on how to approach AI development and humans have started colonizing space,

ends with the machine brains taking over at some vague juncture. When asked whether he had any doubts about his prediction that the current path would lead to superintelligence, Larsen said, “It’s going to happen. It’s going to happen unless we take deliberate steps to stop it.” Lin said that much of this disconnection between AI doomsayers and skeptics comes down to how technology shapes their different worldviews. “There is something very seductive about programming a computer and having it spring to life,” Lin said. “There is the feeling that they’ve been able to infuse life into this worthless pile of mud. It is a profound experience when the machine finally does what you wanted it to do.” Seeing drastic technological advancement in AI, then, leads people to predict limitless, even catastrophic, advancement to follow. “You’ve been able to do something that nobody has done before,” Lin said. “It’s easy to see why these people have been seduced.”




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

How to Prepare for 50+ Patients in 15 Minutes

Source: https://www.childrenshospitals.org/news/childrens-hospitals-today/2026/08/how-to-prepare-for-50-patients-in-15-minutes

Aug 27 – As hospital staff raced across campus gathering equipment and supplies for a massive influx of patients, the clock kept ticking.

More than an hour passed before everything was in place.

By then, a hundred patients had arrived. They were screaming. Their wounds were raw. They knocked over IVs, cried out, and pleaded, desperately, to see their parents.

It was a drill, with actors wearing moulage to mimic wounds and causing chaos to stress the staff. The goal was to replicate the intense, horrific reality of a mass casualty incident, to reveal holes in the hospital's readiness.

"We weren't prepared, not even close," said Chris Riccardi, who oversaw disaster preparedness programs at two Los Angeles County hospitals at the time. "You have 15 minutes until victims show up."

That reality became the motivation behind 15 Minutes 'til 50 Patients, a mass casualty incident response program designed to help hospitals rapidly deploy staff and equipment for a sudden medical surge.

Today, at least 600 hospitals across the country use the model, Riccardi estimates, including Rady Children's Health in Orange County, formerly Children's Hospital of Orange County, where he serves as the manager of emergency management and business continuity.

Developed by Riccardi and a few of his emergency department colleagues using Hospital Preparedness Program grant funding, 15 'til 50 is available at no cost. "My goal was also to put a written plan into the hands of anybody who would want adopt it," he said. "It's find-and-replace. Put your hospital name here, and you're good to go."

Building a better response

Riccardi knows firsthand his program can be replicated at different health care facilities. He was recruited by Rady Children's to do just that.

Rady Children's hospital campus in Orange County serves a county of 3.3 million residents, including roughly 800,000 children. Disneyland is just a few miles away. So is Knott's Berry Farm, Angel Stadium, major freeways, and dozens of school districts.

"If it happens at a school, if it happens at Disneyland, if it happens on the freeway with a couple of buses, what is that going to look like for us?" Riccardi said. "That's what we needed to figure out." So he implemented 15 'til 50, which is built around four essential elements every hospital needs:

- **Staff:** People must know exactly where to go and what to do.

- **Stuff:** Supplies and equipment must be ready to deploy immediately.
- **Space:** An additional area must be able to absorb a sudden influx of patients.
- **Systems:** Everything must be tied together with systems.

Hospitals identify where a surge treatment area will be established, determine what equipment and supplies will be needed, and assign responsibilities across departments before a disaster occurs.

The toolkit includes a written response plan, job action sheets, department responsibilities, and implementation guidance organizations can adapt to their own operations.

At Rady Children's, emergency department staff move into a designated surge area outside the department itself. Hospital leadership activates a command center. Pharmacy, radiology, laboratory services, blood bank teams, trauma staff, chaplains, case managers, and hospital leaders all have assigned responsibilities when a disaster is declared. "We establish a whole new ED surge unit," Riccardi said. "We keep the chaos outside, and we can manage the influx and patient throughput under our guidance." The program has been shaped through years of drills designed to replicate the pressure of a real incident. "The only way to test the system is to stress the system," Riccardi said. "This program has been tested, geez, 150 times, just by me. We never simulate with less than 100 patients." The model has proven adaptable far beyond the California hospitals where it began. Children's hospitals, trauma centers, community hospitals, federally qualified health centers, and long-term care facilities have all adopted versions of the approach.

"This is completely scalable," Riccardi said. "Scale up, scale down, depending on what resources you have available in your facility."

Ensuring reunification

Treating injured children is only part of a pediatric disaster response. Children, some of whom can't communicate, may be separated from their parents, who sometimes don't even know what hospital they were taken to. Reuniting them is among the most important priorities. Working with school districts across Orange County, Rady Children's has incorporated school nurses into its reunification efforts. They help identify students, access emergency contact information, and assist hospitals in reconnecting children with their families after an incident. "We found the missing link," Riccardi said. Today, all 28 school districts and all 26 hospitals in Orange County participate in the effort.

Ready before the patients arrive

The program's widespread adoption remains surprising to Riccardi.

"We put together a plan because we thought we were behind the curve," he said.

More than a decade later, hospitals across the country are still finding value in his solution.

The challenge it was built to address has not changed. Emergency departments remain crowded. Staff remain stretched. When a mass casualty event occurs, hospitals do not get additional time to prepare.

The patients are already on their way.

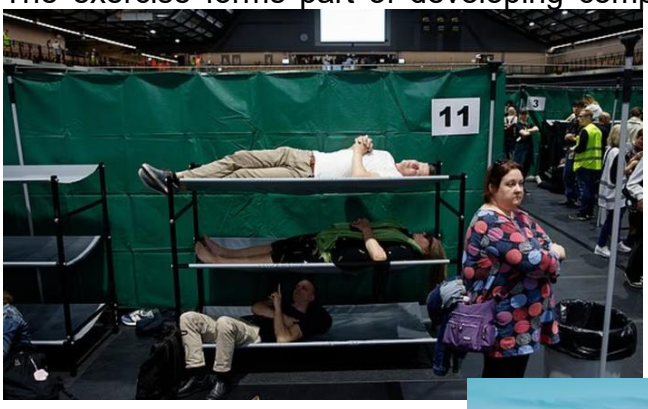
Shelter 2026 -civil defense exercise

Source: https://www.kuopio.fi/en/shelter2026/

Shelter 2026 is a large-scale civil defense exercise taking place on 2–3 September 2026 at Luola ("the Cave") in Savilahti, Kuopio, Finland. The exercise will test how a large number of people can be protected in different types of disruption and during emergency conditions.

The aim is to improve cooperation between authorities and regional partners, and to strengthen command chains and decision-making, the shared situational picture, and communications in circumstances where normal day-to-day functioning of society has been disrupted.

The exercise forms part of developing comprehensive security in the North Savo area. On the exercise days, there will be more visible activity by authorities than usual in the Savilahti area, but this will not cause disturbance to residents or the environment.



Participants include the Rescue Department of North Savo, the City of Kuopio, other authorities, voluntary organizations, businesses, educational institutions and other regional and national partners – over 2,000 participants in total.

Kuopio is a natural and obvious venue for the exercise: the city brings together leading expertise in safety and security, education, research and strong collaboration between different actors. Luola is Europe's most modern civil defense shelter and a dual-use underground facility – it provides a unique and realistic environment for the exercise.


Kuopio
Finland

When disaster strikes, what happens to our pets?

By Okayama University of Science

Source: https://phys.org/news/2026-09-disaster-pets.html

Sep 08 – As large-scale disasters—including earthquakes, torrential rains, typhoons and wildfires—become increasingly frequent, ensuring that pets as well as their owners can evacuate safely and receive appropriate care has become an important part of disaster preparedness. At Okayama University of Science (OUS), the Faculty of Veterinary Medicine is taking a proactive approach to this challenge. In addition to providing a designated evacuation site where people can take refuge with their pets, the faculty's students are actively working to raise public awareness of evacuation with companion animals. OUS is also exploring solutions that draw on the university's distinctive strengths. Through its interdisciplinary "Quality of All Lives Project," faculty members from the Faculty of Veterinary Medicine and the Faculty of Information Science and Engineering are combining their expertise to develop new approaches to protecting the health and well-being of animals during disasters. For many people, pets are more than just animals—they are part of the family. In a disaster, ensuring human safety is paramount, but protecting the lives and health of companion animals is also an important concern.

Putting that principle into practice, however, presents a wide range of challenges. These include whether and how evacuation shelters can accommodate pets, how suitable environments for their care can be maintained, how owners can prepare in advance for emergencies and how local governments can coordinate effectively with veterinary professionals and other relevant organizations.

In December 2018, the same year that OUS established its

Faculty of Veterinary Medicine in Imabari, Ehime Prefecture—the first new veterinary faculty to open in Japan in 52 years—the university, the City of Imabari and the Ehime Veterinary Medical Association signed a three-party agreement to cooperate in animal relief and rescue efforts during disasters.

Under the agreement, the university's Imabari Campus was designated as an evacuation site where people could seek shelter with their pets in the event of a disaster. It was the first time in Japan that a university facility itself had been designated to accommodate people evacuating with their pets.

Following the signing of the agreement, "Establishing a Disaster Evacuation System for People and Their Pets" was introduced as a cocurricular program. Students in the Faculty of Veterinary Medicine also launched Psfull, a group dedicated to raising public awareness of evacuating with pets during disasters.

The name "Psfull" comes from the many "P"s found in words that capture the spirit of the group—Pets, Peace, Happy, People, Positive, Power and more—according to Dr. Kaori Saeki, an associate professor of veterinary associated science, who established and manages the program.

The group is actively engaged in a wide range of activities. Members hold regular study sessions where they present on topics they have researched, organize seminars featuring guest speakers with volunteer experience in disaster-affected areas and take part in disaster preparedness drills organized by local authorities to raise awareness of evacuating with pets. They also regularly meet and exchange ideas with student groups from other universities in the area.

Psfull currently has 23 members, including Kurumi Miyano, a third-year student in the Department of Veterinary Associated Science.

Those preparations were put into practice in March 2025, when a major wildfire—the 2025 Imabari Wildfire—broke out in an area about 10 kilometers (6 miles) from the Imabari Campus. It marked the first time the campus actually served as an evacuation site for people and their pets.

Drawing on the preparations already in place, the university opened its gymnasium to evacuees. Three households—seven people accompanied by 11 cats—came to the campus after learning about the evacuation site through social media and other sources.

During the evacuation, a cat, perhaps stressed by the unfamiliar surroundings, refused to eat the food its owner had brought. When the cat was offered emergency food developed through the university's Quality of All Lives Project—designed to be eaten by both people and pets—it readily began eating.

"The students really put a great deal of thought into what they do," Saeki says. "I hope they will continue to serve as a bridge between the university and the local community, and help make evacuating with pets something that is no longer seen as exceptional, but simply as a normal part of community disaster preparedness."

Saeki also points out that there is no single way to protect pets during a disaster.

"I recently saw news that, following the Kumamoto earthquake in July, Kumamoto Prefecture, Kumamoto City and other organizations established the Kumamoto Earthquake Pet Relief Headquarters, and that seven veterinary clinics in Kumamoto City and elsewhere began temporarily taking in dogs and cats. In reality, evacuation can take many different forms. Whether pets evacuate with their owners, stay with them at an evacuation shelter or are temporarily placed in care, we as professionals need to focus on minimizing stress for both pets and their owners as much as possible."

Meanwhile, Professor Masumi Eto of the Department of Veterinary Medicine, who serves as director of the Center for Quality of All Lives, is

approaching the issue from a scientific perspective.
"We want to scientifically analyze how pets are affected by conditions in evacuation shelters and provide people with evidence-based information they can understand and trust," Eto says.
Drawing on the collaborative project with the Faculty of Information Science and Engineering, Eto explains: "We aim to collect and analyze data from a wide range of signals animals give us, including vital signs such as respiration, pulse rate and body temperature, so that their condition can be monitored. Both humans and animals experience intense stress during disasters. If we can use this knowledge to find ways to reduce that stress, even slightly, it should ultimately improve the welfare of both pets and their owners."
A simple, noncontact vital-sign monitoring system, a device for measuring pressure when applying bandages and video-based diagnostic technology for pets are among the devices currently under development through the Quality of All Lives Project. Expectations are high for the potential of these technologies.

Wartime study shows regular drills protect hospital emergency responses

Source: https://www.news-medical.net/news/20260921/Wartime-study-shows-regular-drills-protect-hospital-emergency-responses.aspx

Sep 21 – Regular drills are crucial if a mass casualty plan is to work in a wartime situation. Focusing on staff safety in the plan itself and taking information flows into account are also important factors for success. These are the findings of a study from Linköping University published in the scientific journal *Disaster Medicine and Public Health Preparedness*.
Across Europe that had long been spared war, many countries are now planning and building up their preparedness following Russia's invasion of Ukraine. In war, hospitals and transports carrying injured people are increasingly being deliberately attacked, creating a major need to adapt emergency healthcare preparedness to this new reality.

"We need to prepare our hospitals for the asymmetric warfare we see around the world, where the aggressor doesn't care about the Geneva Conventions."

Maximilian Nerlander, a PhD student, Centre for Disaster Medicine, Linköping University and a specialist physician in emergency medicine

Maximilian Nerlander is also a visiting scholar at the Hebrew University of Jerusalem Braun School of Public Health and Community Medicine, Jerusalem, Israel.
Preparedness includes having what are known as mass casualty incident plans in place and training the staff who will work in them during war and other crises.
Israel's healthcare system is similar to those in Western Europe, but unlike these, it has real wartime experience. Together with two other colleagues, Maximilian Nerlander has led a study on how the mass casualty plan at an Israeli hospital, Assuta Ashdod Public University Hospital, was affected during the Hamas-led attacks on Israel on 7 October 2023.
The study, based on interviews with 19 members of staff from the hospital's emergency department who were on duty on 7 October, shows how the hospital's regular mass casualty training exercises – held four times a year – enabled staff to work almost automatically when the crisis struck.
"Drills mean that you function better under the extreme stress that arises during war and can carry out the work automatically. In a sudden war, there's no time to familiarise yourself with protocols and procedures; they have to be second nature," says Maximilian Nerlander, who works clinically as a lead physician at the emergency department at Växjö Hospital, Sweden.
The study shows that staff safety is another important

factor in wartime mass casualty incidents. Staff were at risk of being attacked on their way to the hospital, which is something that component in maintaining situational awareness. Another conclusion is that it is important to develop a shared reporting

Wartime Mass Casualty Incident Plan Operation: Staff Experiences from a Civilian Hospital in Southern Israel on October 7, 2023

Published online by Cambridge University Press: **21 July 2026**

CAMBRIDGE UNIVERSITY PRESS

Maximilian P. Nerlander, Adam J. Rose and Debra Gershov West

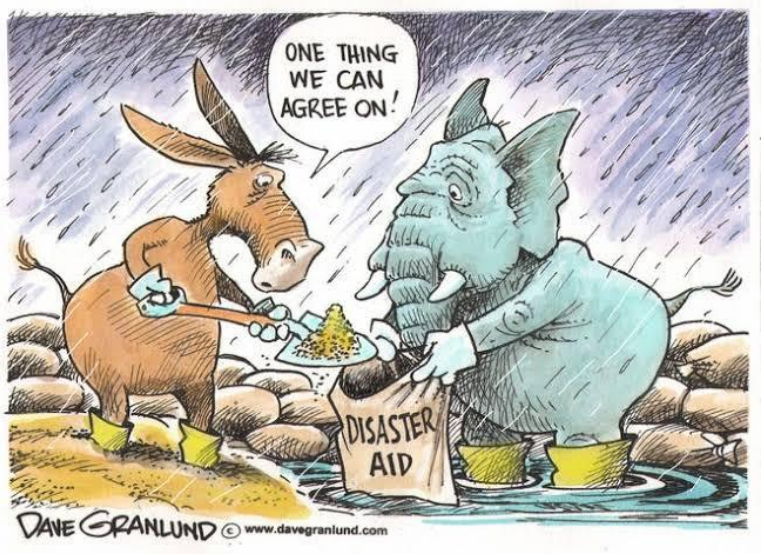
Show author details

needs to be taken into account in mass casualty plans. If staff are physically unable to get to the hospital, the entire system fails. At the hospital in the study, the emergency department is housed in a building which is reinforced to withstand rocket attacks, providing a safe working environment.

"It was remarkable, but really a no-brainer, how important it was for staff to feel safe in order to be able to do their jobs, and this also benefited clinical patient safety. Isn't this something we should take into account when we build new hospitals here in Europe?" asks Maximilian Nerlander. The researchers also note that communication is challenged in several ways during a surprise attack. One conclusion of the study is therefore that a function that sorts and coordinates incoming unstructured information from, for example, patients, ambulance crews, and social media, and passes it on to incident command in a structured way, can be an important system for civilian and military healthcare, as the researchers found that a great deal of information was lost when patients were transferred between military and civilian ambulances.

The fact that the attacks took place during a major Jewish holiday, when many people were off work, was a vulnerability. According to the researchers, preparedness planning must therefore take account of periods of increased vulnerability, such as holidays when many people are off work.

The study was conducted together with Adam J. Rose at the Hebrew University of Jerusalem Braun School of Public Health and Community Medicine, in Jerusalem, Israel, and Debra Gershov West at the Emergency Department, Samson Assuta Ashdod Medical Center in Ashdod, Israel. The study was approved by the Swedish Ethical Review Authority and funded by Region Kronoberg.




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