2 CBRNE DIARY

06\26

ICI International CBRNE INSTITUTE

Dedicated to Global First Responders

June 2026

PART A

N Korea's huge CWA stockpile

Chemical weapons in Syria

Ricin antidote

Ensitrelvir 4 Covid-19

1st AI designed vaccine

Ebola is progressing in Africa

Sin Nobre Hantavirus in Arizona

Mirror Life

US Biolabs in Ukraine

Toxins update

An International CBRNE Institute publication

C²BRNE DIARY ❋ 2026®

June 2026

Editor-in-Chief
Brigadier General (ret.)
Ioannis GALATAS, MD, MSc, MC (Army)
Consultant in Allergy & Clinical Immunology
Medical/Hospital CBRNE Planner/Instructor
Senior Asymmetric Threats Analyst
Manager CBRN Knowledge Center
@ International CBRNE Institute (Belgium)
Editor-in-Chief @ ASPISMEDICAL,
Counter Terrorism Medicine – Europe (UK)
Epanomi, **Greece**

Contact email: igalatas@yahoo.com
Web: https://c2brne-diary-newissue.yolasite.com/

International CBRNE Institute
Rue de la Vacherie, 78
B5060 SAMBREVILLE (Auvelais)
Belgium
Email: info@ici-belgium.be
Web: www.ici-belgium.be

International CBRNE Institute

CBRNE-Terrorism Newsletter

C2BRNE DIARY

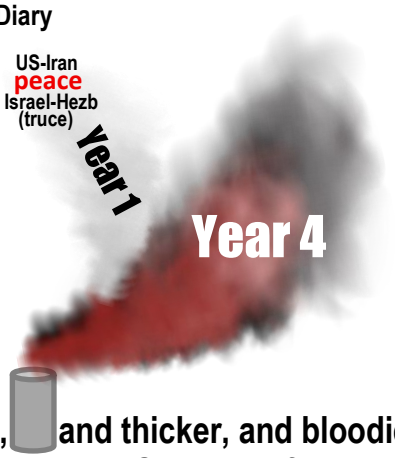
Topics that attracted attention!

EDITOR'S CORNER

Editorial

Brig General (ret.) Ioannis Galatas, MD, MSc, MC (Army)

Editor-in-Chief
ICI C²BRNE Diary



Dear Colleagues,

Smoke in Ukraine is still black, and thicker, and bloodier; smoke in the Middle East (year 1) is white (or not?)! And the winner in the US-Iran conflict is . . .(*)

Ireland: An armed group declaring itself as the 'NEW REPUBLICAN MOVEMENT' has issued a WARNING to Irish politicians: "You have FLOODED our communities with MILITARY AGE MEN", "We will not sit back and watch our culture and religion DESTROYED by the people we put in power."

Pakistan: A suicide bomber has blown himself up at a railway station in Pakistan. At least 19 people have been killed and more than 70 injured after a vehicle packed with explosives detonated near a railway line in Quetta, Pakistan. The powerful blast overturned and set two coaches of a passenger train on fire, while damaging buildings and vehicles. The Balochistan Liberation Organization (BLA) claimed responsibility, saying it targeted a train carrying security personnel. The injured were taken to local hospitals, with 20 in critical condition, and a medical emergency was declared. Quetta is the capital of Balochistan province, which has been plagued by a long-running insurgency.

Turkey: The annual Turkish Armed Forces amphibious exercise, called "EFES-2026", was attended by 1,305 military personnel from 50 countries, the majority of whom were from Libya (502) and Azerbaijan (143). In the list of participants, you will also find European and Balkan countries that **probably did not know that the scenario of the exercise involves the occupation of a GREEK ISLAND by amphibious action…. Who needs enemies when you have friends like these?**

THumor: Turkish President Erdogan: "*Istanbul is Turkish and Muslim. With God's permission, it will remain Turkish and Muslim until the Day of Judgment.*"

NATO: The United Kingdom, France, Italy, Spain, and Canada opposed Mark Rutte's proposal to require NATO members to allocate at least 0.25% of GDP annually for military support for Ukraine, according to "The Telegraph". Too bad that Greece was not among them.

DR Congo: More than 900 people are suspected of being infected with the Ebola virus, which causes hemorrhagic fever, in the Democratic Republic of Congo, the director-general of the World Health Organization (WHO) announced around midnight. In its most recent official tally, released on Saturday, the central African country's Ministry of Health reported 245 deaths out of a total of 933

(*) Pls let me know if found out!

suspected cases in the ongoing epidemic. The percentage of people who died among those confirmed to have been infected ranges from 30% to 50%.

Lebanon: Hezbollah reveals its possession and implementation of night vision and thermal vision-equipped FPV drones! This means that stealth night ops by Israeli forces invading South Lebanon, which were thought to be a solution for daytime FPV drone attacks by Hezbollah (Haddatha attempts), will make them even easier targets for the explosive quadcopter. Reality or psychological misinformation?

Japan: Tokyo was on alert after 20 people were injured in a luxury shopping mall after a man sprayed an unknown substance on the ground floor of the building near a vending machine, authorities said. A police spokesman said the incident occurred in the Ginza district, an area known for its luxury shops and heavy tourist traffic. Firefighters told AFP there were reports of a strong smell, and the injuries were attributed to exposure to the substance used. Memories of Aum…

Greece: Unsuspecting citizens who had gone fishing in a rocky area in Agios Antonios, in the Municipality of Neapolis, between Milatos and Elounda in Crete, discovered a **sea mine which turned out to be Ukrainian**, one of the types used against Russian tankers, the majority of which are leased Greek ships! It should be noted that a year ago, a similar mine was discovered on a beach in Rhodes Island.

Libya: According to journalistic investigations by the French RFI and El País (and other media), Ukraine maintains hidden drone launch sites and military personnel in coastal areas of Western Libya, intending to attack Russian tankers of the "shadow fleet". The three main locations: (1) Zawiya: About 50 km north of Tripoli, near the Mellitah oil and gas complex. Fully equipped base for launching aerial and sea-based drones. (2) Misrata: Air base/Air Force Academy, where Ukrainian specialists operate together with Turkish, Italian forces, the US Africa Command (AFRICOM), and a British intelligence center. (3) Tripoli: Coordination center within the facilities of the 111th Brigade of the Libyan army. Ukraine aims to disrupt Russia's maritime supply lines by targeting tankers carrying Russian oil in defiance of Western sanctions. The attacks (such as the one on the Russian LNG tanker Arctic Metagaz in March 2026) are carried out with the tactical support of Western intelligence services. This is turning the central Mediterranean into a proxy conflict zone, with risks to trade routes. The operations are also said to serve US/Turkish interests in the region, while ignoring basic maritime international rules.

Ukraine: Volodymyr Zelensky continues to ask NATO member states for more stable financial support for Ukraine, proposing that **each country allocate 0.25% of its GDP to strengthen Kiev.**

■■ Three Russian tankers were attacked by Ukrainian naval drones near the Kiliya area. The ships, identified as the Velora, James II, and Altura, were just 2–3 kilometers off the Turkish Black Sea coast when the attacks occurred. The area is located near the European side of Istanbul, which has raised concerns about shipping safety (who cares about safety?)

●●● Weapons for Ukraine are flooding the European black market. The German newspaper Berliner Zeitung is sounding the alarm: The supplied weapons are already circulating in the EU. Intelligence services and police fear a repeat of the "Yugoslav scenario" on a much larger scale: After the Balkan wars of the 1990s, huge quantities of small arms fell into the hands of organized crime. Europol and Frontex warned of smuggling as early as 2022, but in Brussels, this issue is being swept under the carpet – anyone who raises it will be considered an "enemy of aid to Kiev". Since 2022, Ukraine has become the world's largest arms importer. The United States alone has contributed $18 billion, but there is no control over the weapons. Assault rifles have already been found in Spain and Hungary. And this is just the beginning. The authors of the article note that Ukraine is one of the most corrupt countries and a "laboratory" for testing modern weapons. If foreign fighters, who are usually extremists or criminals, return to Europe with their knowledge (and their weapons), this will create a "qualitatively new threat."

⬇⬇⬇ Italian Defense Minister Guido Crosetto told parliament that Rome rejects from the outset participation in the arms purchase initiative for Ukraine (Prioritised Ukraine Requirements List), despite his recent contacts with his American counterpart in Washington.

👽👽⬇ US President Donald Trump has issued an official request to European countries to fully reimburse the cost of military aid sent to Ukraine during the presidency of Joe Biden. The White House's total financial claims against its European partners amount to about $350 billion. According to the official US oversight group (Ukraine Oversight Working Group), the total amount approved or committed for Ukraine (including humanitarian, economic and military support) is about $183 to $203 billion. Direct military assistance in the form of weapons and equipment from US stocks was about $64 billion, a small fraction of the $350 billion that Trump is citing. **Or else, what?**

Russia: The Deputy Chairman of the Russian Security Council, Dmitry Medvedev, spoke out against the EU and NATO countries that rushed to comment on the incident of the downing of a Russian drone in Romania. Specifically, he called on the European leaders of the pro-war wing of the EU to "shut it up" as he believes that they have no right to speak, since they are "fueling" the war in Ukraine with their actions. At the same time, he said that from now on they should not sleep peacefully.

N. Korea: North Korea announced that it has successfully completed the test of a new hypersonic missile that is capable of hitting any US city in about 15 minutes! At the same time, Pyongyang announced that it now has **50 new nuclear warheads**, further strengthening its nuclear arsenal. True or just pocker?

Iran: Satellite images published by CNN show that Iran has repaired much (50 out of 69 entrances) of the damage caused by the bombings to its missile facilities. Over 20 US bases were destroyed by Iranian attacks. We await the corresponding photos from CNN with interest.

▶▶▶Trump says a "small group" of U.S. soldiers could "walk in there tomorrow" and "take over all of Iran" - "if I wanted to." Pls, Sir, define "small"! 😊

Greece: US Secretary of War Pete Hegseth stated that "Greece, like other countries in Europe, is being 'suffocated' by the invasion of illegal individuals with dangerous ideologies. Boats and people are arriving every day, and nothing is being done to prevent it." Speaking in the context of the events for the 82nd anniversary of the Normandy Landings, he linked it to the migratory flows recorded in European countries, also referring to Greece. "When will they do something about this invasion, or is it already too late? I pray that it will not be – and I believe that it is not," he added. Sorry, Mr. Secretary, but the answer is negative. To do something means you care about your Homeland (Patrida)!

Sweden: The Swedish parliament has voted in favor of a historic bill that permanently abolishes the possibility of granting permanent residency to asylum seekers, refugees, and certain other groups of illegal immigrants. This new strict legislation will come into effect on July 12, sealing a complete shift in the Scandinavian country's approach to immigration. With the new government decision approved on Tuesday, this option is completely removed for these groups of immigrants, making it clear that their stay in the country will be strictly temporary and not strictly permanent, as is the case in other countries such as Greece. But the question is: Is it already too late?

The Editor-in-Chief

Get That Greek Summer Feeling

Voutoumi ranked second among the best beaches in Europe for 2026, according to European Best Destinations.

China's Moon Ambitions Are Military, Not Civilian — U.S. Must Respond With Hard Power To Beat Beijing: Report

By Sumit Ahlawat

Source: https://www.eurasiantimes.com/boots-on-the-moon-us-china/

May 25 – As part of Beijing's ambitions to send humans to the Moon by 2030, China successfully launched its crewed Shenzhou-23 spacecraft aboard a Long March 2F rocket from the Jiuquan Satellite Launch Center on May 24 and completed a rapid automated docking with the Tiangong space station just hours later.

China is "steadily" building operational experience for "sustained occupation" of its Tiangong space station, and year-long missions are an important step towards future lunar and potentially deep-space ambitions, Richard de Grijs, an astrophysicist and professor at Macquarie University, said.

The main challenges will involve long-term effects on humans, including bone density loss, muscle wasting, radiation exposure, sleep disturbances, behavioral and psychological fatigue, Richard de Grijs said.

It appears a new Cold War is unfolding, one where the stakes are dramatically higher, and the battlefield now extends to the Moon and beyond. However, unlike the Cold War space race, this race has no defined finish line. Rather, the modern-day space race is characterized as an enduring competition for long-term strategic positional advantage in space.

In this high-stakes race to dominate space, the United States and China are the primary contenders. Any meaningful advantage in this competition will grant them the power to shape global norms, standards, and legal frameworks in outer space for decades — if not centuries — to come.

To dominate this space race, the US must put boots on the moon, establish a military base there, and capture territory, argues a provocative new policy paper by the Mitchell Institute.

The paper warns that despite the presence of treaties like the 1967 Outer Space Treaty that bans weapons of mass destruction in orbit and forbids all military activities, such as weapons testing and bases, on the Moon and other celestial bodies, the competition for control of lunar resources and territory will likely reach a "tipping point, at which time the modern-day space race could turn into conflict."

"The anarchic nature of the Moon combined with China's record of belligerent use of hard power yields a predictable future where United States lunar interests are put at risk," the paper warns.

To counter this, it is time for the United States to commit the time, consideration, actions, and resources needed to prevail in this contest, it suggests.

"When territorial conquest, the potential for economic gain, and

national interests overlap, societies seek to establish favorable norms and standards and do so using various degrees of hard power. Accordingly, hard Power will ultimately matter in this new space race."

However, for this objective, the US will have to overturn nearly 70 years of a consistent national space policy that separates NASA's civil from military space activities under Title 10, as well as Washington's almost 60-year stance as a champion of the 1967 Outer Space Treaty (OST) that prohibits territorial claims and military occupation of the moon and other celestial bodies.

The paper is based on two premises.

First, the country that wins this space race will define the global norms in space for decades, and that space domination will translate into tangible power benefits on Earth as well. Also, the exploitation of lunar resources is a critical first step toward future habitation of space.

Secondly, China's civilian lunar research program is a ruse for military occupation of the lunar surface. Beijing, the paper warns, will likely extend its "belligerent" behavior on Earth for territorial expansion to the moon as well.

The paper recounts how Beijing has enforced its expansive territorial claims in the South China Sea, which have no basis in international law, by using military means.

"These activities will predictably extend to space habitation and lunar exploration," it said.

China's approach towards the Moon and the space beyond is best characterized by a speech given by China's former General Director of lunar exploration missions, Ye Peijian.

"The cosmos is an ocean, the Moon is the Diaoyu Islands…If we can go, but don't go, future generations will condemn us. Once others…have occupied, no matter how much you wanted to go, you couldn't."

In other words, China views success in the space race, including lunar habitation, as a means of controlling territory and the corresponding logistics routes — a Chinese Silk Road through space.

These Chinese actions will put future American space security at risk.

"China's military-led human space flight progression is positioning the People's Liberation Army to achieve strategic advantage in lunar access, infrastructure, and resources," Kyle Puma, Mitchell Institute senior resident fellow for space studies, said.

Puma is not only the author of the paper but also a former Space Force colonel.

The paper also warns that the US is currently trailing China in the current Space Race.

"The United States should not underestimate the threat simply because it is not yet a highly visible one. China is a burgeoning space power, so much so that they stand a very real shot at winning the current race.

"They have created an aggressive strategy and are achieving their stated goals on time. The United States, by comparison, has repeatedly slipped schedules by several years for key space exploration objectives."

The authors warn that, for China, space and moon exploration is "an extension of its territorial ambitions," and that it does not follow the neat separation between the civilian and military realms that the US does.

In the US, the US Space Force pursues space superiority using remotely operated unmanned systems, while NASA oversees human spaceflight.

This dichotomy presents its unique challenges.

If some day, the paper warns, Chinese Taikonauts decide to challenge American interests by endangering civilians on the Moon or elsewhere extra-terrestrially, the US will not be in a position to resist these attempts, since the US Space Force has no trained soldiers in space and NASA astronauts are neither trained nor legally empowered (under Title 10) to use weapons to protect US interests.

"This would be akin to asking the merchant marines to execute the duties of a warfighting Navy — the lack of training, equipment, and legal authorities would impair the necessary actions for national security."

The solution, the paper suggests, is to launch a military human spaceflight program under the aegis of the US Space Force.

"A military human spaceflight program will be crucial to establish and secure a strategic positional advantage in space, particularly as it pertains to the Moon… This will require properly trained, organized, and equipped Guardians in space who are empowered with Title 10 authorities," it said.

The paper also compared the US's changing attitude toward the space race with the Soviet Union during the 1960s and 1970s, and its ongoing attitude toward the space race with China.

"The U.S. understood it was in a major, must-win national security competition in its first space race with the Soviet Union. While the Soviet Union's launch of Sputnik and additional early LEO achievements propelled them ahead of the United States, the nation engaged in a whole-of-nation effort to win the bigger contest—One focused on the Moon," it said.

This dedicated national effort meant that not only did the US become the first country to land humans on the Moon, but it also remains, to this day, the only country to have done so.

However, in the wake of this tremendous achievement, the nation quickly lost interest in the space program, and the Nixon administration canceled the last three Apollo lunar missions.

When the Soviet Union abandoned its manned lunar mission ambitions, the US also lost interest

in the Space Race, since there was no longer any risk of losing an existential competition.
Ever since, the US space ambitions have been floundering. China, however, has clarity about its space ambitions and is progressing steadily, the paper warns.
To rectify the imbalance, a military human spaceflight program led by the U.S. Space Force is needed for the United States to sustain an ability to defend its national security interests in space over the long term, the paper recommends.
In other words, the US must plan to send trained US Space Force soldiers, rather than civilian astronauts, to the moon, and consider establishing military outposts in Space to defend US national security interests and counter China's military maneuvers.

EDITOR'S COMMENT: A classic case of "mine is bigger than yours!" I only hope that moon aliens will teach both a lesson!

Iran's Guards Used UAE Company to Buy Military Satellite Equipment

Source: https://www.iranwatch.org/news-brief/irans-guards-used-uae-company-buy-military-satellite-equipment

May 24 – The Islamic Revolutionary Guard Corps (IRGC) Aerospace Force imported approximately 1.8 tons of satellite antenna equipment in late 2025 via the United Arab Emirates-based company Telesun. The goods, a motorized satellite antenna and related accessories, arrived in a single shipment. A Chinese container ship made the first leg of the delivery from Shanghai to Dubai in August. The container was then transferred to an Iranian vessel, which delivered the shipment to the Iranian port of Bandar Abbas while falsifying its transponder signal to show the vessel as located in the Gulf of Oman. The shipment's consignee was Ertebatat Faragostar Kish (EFK), an Iranian telecommunications company working for Saman Industrial Group, which was sanctioned by the United States in 2023 for serving as a front company for the IRGC Aerospace Force's Self Sufficiency Jihad Organization. The delivery's Iranian shipping agent was Blue Calm Marine Services, which was also sanctioned by the United States in 2023 for facilitating shipments of missile-related goods to Iran's defense ministry.

The six failures of the Iran war for Trump

Source: https://en.mehrnews.com/news/244918/The-six-failures-of-the-Iran-war-for-Trump

June 01 – From the nuclear file to the Strait of Hormuz, from oil prices to approval ratings, independent assessments across six domains show Washington's stated war goals remain unmet three months in. From the early hours of military operations against Iran, the Trump administration worked to establish a narrative of decisive, historic victory. In a series of national addresses, Trump declared Iran's nuclear programme completely destroyed, the IRGC command paralysed, the Iranian navy eliminated, its air force gone, and its ballistic missiles almost finished or destroyed.
Three months on, US internal intelligence assessments, independent satellite evaluations, global economic data, and domestic polling surveys paint a sharply different picture. Based on credible Western and international sources, this analysis examines six areas in which the stated objectives of the war have not been achieved, and in several cases have produced outcomes directly contrary to American interests.

1. Nuclear Failure: A Delay, Not Destruction
The primary justification for the war was to prevent Iran from acquiring nuclear weapons capability. Trump claimed Natanz, Fordow and Isfahan sites had been completely and totally destroyed. But a classified initial assessment by the US Defense Intelligence Agency and subsequent satellite reports found that damage was largely limited to surface structures, entry points and support facilities. Key underground sections and advanced centrifuges were substantially intact. The enrichment programme has been set back by between six and 18 months, not eliminated. IAEA Director General Rafael Grossi announced that he can no longer account for approximately 400 kilograms of uranium enriched to 60 percent purity. US Vice President JD Vance publicly acknowledged that Washington does not know the precise location of those stockpiles.

2. Hormuz: An Economic Weapon Handed to Iran
The biggest US strategic miscalculation, according to Ali Vaez, Director of the Iran Project at the International Crisis Group, was handing Tehran what he described as "an economic weapon of mass destruction." Since the war began, Iran has exercised operational control over the Strait of Hormuz. Even following a temporary ceasefire, vessel transit has continued under severe restrictions and additional costs. The Hormuz crisis rapidly became a global energy crisis, compared by analysts to the Suez Canal crisis of 1956.
3. Economic Shock to the US and the World
The war's impact on ordinary American households was direct and rapid. Crude oil prices rose from around 67 dollars to above

110 to 120 dollars at peak moments, an increase of up to 80 percent. Petrol prices crossed five dollars per gallon in several US states. Airline ticket costs rose by around 20 percent. Energy supply chain inflation intensified pressure on households across multiple countries. Economists and the Center for American Progress warned that a return to pre-war price levels would be slow and incomplete. This was particularly damaging for Trump, who had cited sub-three-dollar petrol as a signature economic achievement before the war.

4. Political Fallout: Approval in Freefall

The war quickly became a domestic political crisis. A Reuters/Ipsos poll from April 2026 placed Trump's approval rating at 34 to 36 percent. AP-NORC and Strength in Numbers surveys found ratings of around 33 to 35 percent. Only 34 percent of Americans supported the decision to launch military action. Trump's economic approval collapsed to approximately 23 to 25 percent. A majority of voters, including independents, assessed the war as "the wrong decision" whose objectives had not been met.

5. Narrative Contradiction

Al Jazeera and other outlets extensively documented the gap between Trump's victory claims and observable reality. While Trump spoke of "complete victory" and an "imminent deal," Iran's power structure remained intact, enrichment had not stopped, new control over the Strait of Hormuz had been established, and uranium stockpiles had not been handed over. The contradiction severely damaged the credibility of the Trump administration's account of the war.

6. Voices From Within

American analysts were direct in identifying failures of planning. New York Times and CNN journalists reported that the Trump administration had no clear strategy for ending the war or managing its economic consequences from the outset. Military experts assessed Iran's resilience, its effective use of asymmetric warfare, and the implicit backing of Russia and China as having exceeded Pentagon projections.

Conclusion

The three pillars used to justify the war — destroying the nuclear programme, safely reopening the Strait of Hormuz, and strengthening America's economic position — have either not been achieved or have produced the opposite of the intended result. Iran, despite real damage, demonstrated resilience, generated new leverage, and frustrated American objectives across almost every domain.

The United States, meanwhile, paid enormous military, economic, and political costs, while its global rivals, Russia and China, used the crisis to strengthen their own positions.

Why Iran Will Prefer Ongoing Conflict

By Mohamed ElDoh

Source: https://www.homelandsecuritynewswire.com/dr20260602-why-iran-will-prefer-ongoing-conflict

June 02 – Even a fragile ceasefire creates the illusion that a resolution pathway is in progress. In such highly contentious regions as the Middle East, ceasefires frequently function as transitional phases between confrontation, rather than endpoints. The key question in the United States' current standoff with Iran and its regional proxies is not whether hostilities have paused, or whether there are clear prospects for resolving the conflict in the near term, but whether the underlying causes and incentives for conflict have meaningfully changed. In short, they have not. In fact, from Iran's perspective, there are compelling strategic reasons why a prolonged, though managed, confrontation is more advantageous than a rapid return to peace.

The Logic of War as Negotiation

At the core of Iran's calculations lies a well-established principle in coercive strategy, in which war is an extension of bargaining. In this regard, Iran is unlikely to view any ceasefire at the current stage of the fighting as a success unless it translates into a revised strategic framework. This would be one that acknowledges its deterrent capabilities over the region, preserves its nuclear program and missile and drone arsenal, and reduces the threat of any preemptive action by the US or Israel against it.

From Iran's perspective, an early cessation of hostilities risks locking it back into an unfavorable status quo characterized by sanctions, strategic encirclement and periodic military pressure. By contrast, sustaining a controlled escalation allows Tehran to negotiate from a position of apparent demonstrated capability, rather than of theoretical deterrence or media rhetoric. This is not escalation for its own sake. It is escalation that is calibrated to shape the political end state.

Asymmetric Attrition

Iran's military doctrine has long been built around asymmetric warfare and strategic patience. Tehran does not want a classic war victory or a traditional peace deal. Instead, it aims to impose cumulative costs (military, economic and psychological) on its perceived adversaries and maintain a degree of regional instability. This has been the case with Iran's indirect hostile actions over the decades.

Time is a key weapon in this strategy and a prolonged conflict favors Iran in several ways. It increases economic uncertainty, particularly in global energy markets, and puts pressure on the US. It forces the US to sustain deployments and increase military resources in the Middle East. It also exposes security gaps and vulnerabilities in the air defense systems of Israel and US allies in the region by putting them under repeated missile and drone attacks.

Compared with the US and its regional allies, Iran's threshold for pain is structurally higher, largely due to decades of operating under sanctions and isolation. This asymmetry creates a paradox in which what appears as instability to external observers is in fact perceived as endurance by Tehran.

Energy Disruption as Influence

No component of Iran's doctrine is more critical and consequential than its proximity to the Strait of Hormuz, through which around a fifth of global oil supply transits. Even limited disruption there generates outsized global effects, including anxiety in energy-importing economies, oil price volatility, insurance spikes and rising shipping costs. Over the past few weeks, Iran has weaponized the Strait of Hormuz, taking such provocative action as prevention of passage, attacks on tankers and announcement of new transit tolls. All this has happened as more than 40 nations, led by Britain and France, have prepared for an effort to reopen the strait.

For Iran, the situation represents a unique opportunity for leverage, inflicting pressure on the global economy and energy markets. Most importantly, it is leverage that does not require full closure of the strait. A mere credible threat and intermittent disruption are enough to create global effect. On top of this, media entities linked to the Islamic Revolution Guard Corps have been discussing the possibility of Tehran imposing fees on submarine cables that pass through the strait and of monitoring global data traffic.

By maintaining this managed level of provocation and regional tensions, Tehran can strategically signal its capacity to escalate at will. It reinforces its relevance in global strategic calculations despite the sanctions imposed on it. It also pressures countries in Europe and Asia to advocate for de-escalation in terms that are favorable to Iran. In this regard, regional instability for Iran is not a byproduct; it is a key instrument for the regime's survival.

Regime Survival and Internal Consolidation

External conflicts have always played a dual role for the Iranian regime: deterrence abroad and consolidation at home. Periods of heightened confrontations allow Tehran to suppress internal dissent and reframe economic hardship as externally imposed. They also allow the regime to strengthen its narrative of resistance against foreign pressure and to

increasingly frame that pressure as the West's war against Islam.
A transition to peace without tangible gains risks exposing the regime to internal scrutiny. Questions would inevitably arise: What was achieved? At what cost? What was the reason for the initial hostility? By contrast, a managed and prolonged conflict allows Tehran to maintain a mobilized domestic posture, avoid the perception of strategic retreat and justify continued securitization of the political space. While Iran does not seek unlimited war, it considers controlled instability to be politically safer than inconclusive peace.

The Credibility and Intent of the Axis of Resistance
Iran exerts its regional influence not only through state-to-state interaction but through a network known as the 'Axis of Resistance', made up of aligned non-state actors in Yemen, Lebanon and Iraq. These relationships are not transactional. They are the foundations of Iran's deterrence architecture built over decades, and the regime's ideology is deeply embedded in these groups.
A premature de-escalation that sidelines these proxy groups risks compromising Iran's credibility as their principal patron. Subsequent fragmentation would weaken deterrence and invite Iran's adversaries to target these proxy groups individually.
By contrast, active confrontation enhances Iran's operational coordination across the various theatres and boosts the perception of a unified front. It also increases the cost for the West and other countries in the Middle East in contemplating localized escalations. Despite Israeli attacks that have degraded capabilities of Iran-backed groups in Lebanon, Iran's Houthi friends in Yemen still stand strong and, with missiles and attack drones, threaten Red Sea navigation and neighboring Gulf Cooperation Council (GCC) states.
For Tehran, the current conflict is an inherently multi-theatre and systemic one, not confined to a single front.

Deterrence and Strategic Signaling
One of Iran's main objectives in the conflict is to restore and reinforce its regional deterrence credibility. It wants to prove it can absorb significant strikes without strategic collapse and retain the capacity to retaliate across multiple domains. It also wants to show that escalation will not remain one-sided. Iran tried to demonstrate this during the first round of the confrontation when it attempted to attack all the GCC states indiscriminately with ballistic missiles and drones. It is now proving the point through provocative actions that assert control over the Strait of Hormuz.
Ending the conflict too early risks diluting these signals. For Iran, deterrence is not established through restraint alone, but through observable resilience and response capability. This is particularly relevant in relation to Israel's doctrine of preemption, the US's forward military posture in the region and the GCC's reliance on external security guarantees in parallel to the increasingly powerful GCC defensive and military industrialization posture. By pursuing a managed conflict, Iran is able to cultivate an operational space for communicating these messages with clarity while sowing chaos in the region.

World Powers and Strategic Depth
Iran's strategic planning is shaped by its positioning within broader great power competition, and not only by regional security or geopolitical dynamics. While it is not part of a traditional alliance structure, it benefits from converging interests with Russia and China in countering US influence and alliances in the Middle East, and it has economic and diplomatic engagement with both countries. This does not eliminate Iran's vulnerabilities, but it does provide strategic depth. It reduces the likelihood of total isolation and creates space for prolonged resistance. In such an environment, Tehran assesses that time may work in its favor.

The Ceasefire as a Process and Negotiation Under Fire
In complex and rapidly developing conflicts, ceasefires are instruments for managing military escalations, not for resolving them. Within this framework, both sides test boundaries, recalibrate strategies and probe for a military or diplomatic advantage. In this light, Iran probably views the current ceasefire as an opportunity to test, again, the red lines of the West and the GCC. The break also allows regrouping, mobilizing and reassessing.
Any ceasefire is also a platform for further negotiation under duress. This is part of a broader pattern of bargaining under fire, in which military action and diplomacy go hand in hand.
That said, Iran's strategy is not without risk. Managed conflicts can become unmanaged at any given moment if unintentional triggers, escalation spirals or provocative miscalculations push the confrontation beyond controllable thresholds. Furthermore, while domestic support in Iran is resilient, the public will not have unlimited patience. Economic strain remains a structural constraint, especially with the current US blockade of vessels going to and from Iranian ports.

Iran's Preference Towards Controlled Instability
The continuation of the conflict appears irrational, especially when a ceasefire is in place and mediations are ongoing. But from Tehran's perspective, the equation is more complex. A rapid return to peace risks reinstating an unfavorable strategic status quo, exposing internal vulnerabilities and undermining Iran's deterrence credibility regionally and internationally. By contrast, a managed, prolonged confrontation offers Iran negotiating leverage, strategic signaling and the opportunity to preserve regional influence.

This further increases the need for a decisively unified international military front against Iran's hostile intentions. Recent reports show that even during the ceasefire, Iran has restored 30 out of its 33 missile sites it maintains along the Strait of Hormuz.

Iran is not seeking a war victory in the conventional sense. Instead, it is pursuing a sustained condition of instability, one that maximizes its leverage while gambling on avoiding decisive confrontation. The current fragile ceasefire is not the war's end; it is the setting for the next phase where most likely an international unified response will be shaped. The extent and capacity of such response will greatly depend on how Iran continues to exercise its weaponization of the Strait of Hormuz in the coming period, how it will deal with its enriched uranium, and the existing threat threshold posed to the region by its remaining ballistic missiles and drones.

Mohamed ElDoh is a business development and consulting professional in the defense and security sector. He holds a doctorate from Grenoble Ecole de Management, France; an *MBA* from the *EU* Business School, Spain; and an advanced certificate in counterterrorism studies from the University of St Andrews.

Amateur Hour: The Unserious Appointment of Bill Pulte

By Ben Frankel

Source: https://www.homelandsecuritynewswire.com/dr20260603-amateur-hour-the-unserious-appointment-of-bill-pulte

June 03 – In a column last year arguing that Pete Hegseth was unfit to be defense secretary, George F. Will proposed a simple thought experiment. Suppose, he wrote, you gathered 100 intelligent, public-spirited people with experience running large organizations, dealing with allies, and understanding modern threats, and asked each of them to list 100 plausible candidates to lead the Pentagon. You might end up with as many as 10,000 names. The probability that any of those lists would include Hegseth, Will concluded, was essentially zero.

Apply the same thought experiment, but now to the job of Director of National Intelligence. Ask 100 seasoned national-security professionals—people who have lived with the daily grind of inter-agency coordination, covert operations, and signals intelligence—to give you 10,000 names apiece, this time of individuals they would trust to sit atop the U.S. intelligence community. Out of that theoretical pool of one million candidates, the probability that anyone would propose Bill Pulte—a housing regulator with no national-security experience and a record of treating confidential data as a political weapon—is also approximately zero.

Pulte's current job is to oversee Fannie Mae and Freddie Mac as director of the Federal Housing Finance Agency, not to assess Iranian enrichment rates or Chinese signaling on Taiwan. His public portfolio has been mortgage finance and housing policy, not clandestine networks, covert action, or cyber intrusions. Yet even in that more prosaic role, he distinguished himself not by technocratic competence but by his eagerness to weaponize his perch on behalf of Donald Trump's political and personal grievances. Members of Congress and press investigations have accused him of rummaging through mortgage databases for dirt on Trump's enemies, and of presiding over the improper sharing of confidential Fannie Mae pricing data with Freddie Mac, moves that triggered internal alarm and the ouster of officials who objected.

There is no need to dwell on every detail of those episodes; other writers already have. The essential point is simpler and more disturbing. This is not a man who treats sensitive information as a public trust. It is someone who has already shown a willingness to see state-held data as raw material for partisan combat. That is what makes this appointment so dangerous. The Director of National Intelligence sits astride not one database but the holdings of 18 separate agencies, from the CIA's human sources to NSA's collection to the FBI's counterintelligence files. To take a figure already accused of using mortgage information to concoct allegations against Trump's critics and place him atop the intelligence system is to invite the same habits into an exponentially more consequential domain.

Pulte's nomination is not an aberration but part of an established pattern. Trump's national-security personnel choices routinely pass over the obvious pool of experienced professionals in favor of loyalists whose core qualification is ideological and personal devotion. Tulsi Gabbard, whom Pulte has been tapped to replace, arrived at the Office of the Director of National Intelligence and quickly made clear that she viewed the intelligence agencies less as a source of inconvenient truth than as a problem to be disciplined. Kash Patel, Trump's choice for the FBI, belongs to the same type. His appeal lies not in managerial gravitas or institutional seriousness but in demonstrated loyalty and appetite for combat.

Even William Barr—hardly a Trump antagonist—drew a line at Patel. When Trump's White House floated Patel for a senior FBI role late in the first term, Barr wrote that he "categorically opposed" the idea and told Mark Meadows it would happen "over my

dead body." Barr's judgment was that Patel lacked the temperament and judgment to help run a national law-enforcement agency. If a Trump-appointed attorney general thought Patel was too reckless even to be the Bureau's number two, it is telling that Trump now has placed him in the top job.

Gabbard's record is instructive as preface to Pulte. Her confirmation hearings were already a warning sign. Senators pressed her over a history of echoing Vladimir Putin's talking points: suggesting that the United States and Ukraine were connected to dangerous biolabs narratives promoted by Moscow, minimizing or relativizing Russia's aggression, defending Bashar al-Assad against overwhelming evidence that he had used chemical weapons against his own people, and taking a notably dismissive line on Iran's nuclear weapons ambitions. Once in office, she confirmed those fears. When the National Intelligence Council produced an assessment that undercut Trump's claim that a Venezuelan gang operating in the United States was effectively an arm of Nicolás Maduro's government, Gabbard fired the council's top two officials. Their offense was analytic. Their professional judgment, based on years of experience and the available intelligence, was that Maduro probably was not directing Tren de Aragua's U.S. operations in the way the White House claimed. Gabbard's response was not to answer the analysis with better evidence, but to purge the analysts.

On Russia, Gabbard went further, devoting considerable energy to depicting the Obama-era Intelligence Community Assessment on 2016 election interference as "manufactured" to damage Trump. Here the trick was conceptual. The intelligence community had long distinguished between two questions: whether Russia ran information operations—including social-media disinformation and hack-and-leak campaigns—to help Trump and hurt Hillary Clinton, and whether Russian actors successfully penetrated voting systems and altered tallies. The consensus answer was yes on the first and no on the second. Gabbard seized on internal language about the lack of evidence for vote-tally manipulation and spun it into a retroactive exoneration for Russia's broader interference, implying that if no votes were changed then the entire case for interference had been fabricated. The message to the intelligence community was not simply that officers should avoid embarrassing the president in public. It was that they were not to tell the president or other senior decision-makers the truth if that truth cut against the story the White House was already telling, even when that story was false. In Gabbard's hands, the office of the DNI became less a conduit for reality than a filter designed to keep reality from reaching the Oval Office. There is, however, another model for how the head of U.S. intelligence can behave, and it is worth recalling before the Gabbard-Pulte pattern is normalized. Before the Intelligence Reform and Terrorism Prevention Act of 2004 created the DNI, the Director of Central Intelligence, usually the CIA director, functioned as the formal leader of the intelligence community. Since 1947, there have been flawed CIA directors, and some were too close to the policy preferences of the presidents they served. But when the institution has been most severely tested—when presidents have sought not just sympathy but complicity—its leaders have generally looked far more like Richard Helms than Tulsi Gabbard.

During Watergate, Richard Nixon tried to enlist Helms in a cover story: the CIA was to suggest that the break-in at the Democratic National Committee was somehow connected to a legitimate intelligence operation involving Cuba, thereby muddying the waters and deterring further investigation. Helms refused. He insisted that the CIA had no involvement in the break-in and rejected the idea that his agency should serve as a shield for domestic political crime. Nixon eventually forced him out and hoped for a more pliant successor, but the line had been drawn. There were things an intelligence chief would not do, even for the president who had appointed him.

This is not to romanticize the CIA. George Tenet was rightly criticized for the agency's role in the faulty assessments of Iraqi weapons of mass destruction that the Bush administration used to justify the 2003 invasion. John Brennan has been cast by Trumpists as the mastermind of a "deep state" plot against Trump, even though the public record shows him briefing lawmakers on Russian interference and carefully limiting his claims to the evidence he believed the intelligence supported. But these episodes belong to a different category than the appointment of someone like Bill Pulte. They concern analytic failure, institutional error, and the pressures of policymaking, not the elevation of a loyalist whose principal distinction is his willingness to use the powers of office against a president's enemies.

What unites the appointments of Gabbard, Patel, and now Pulte is something deeper and more disturbing than mere preference for loyalty over competence. It is contempt. Trump does not simply distrust the intelligence agencies and the FBI; he despises their claim to professional authority. He is hardly the first American populist to mock experts—George Wallace's sneers about "pointy-headed intellectuals" belong to the same lineage—but Trump has taken that impulse deeper into the state itself. In his political world, there are no neutral facts to be discovered, recognized, and weighed. There are only stories that help him and stories that hurt him. Institutions whose function is to establish inconvenient facts therefore become objects of resentment and humiliation.

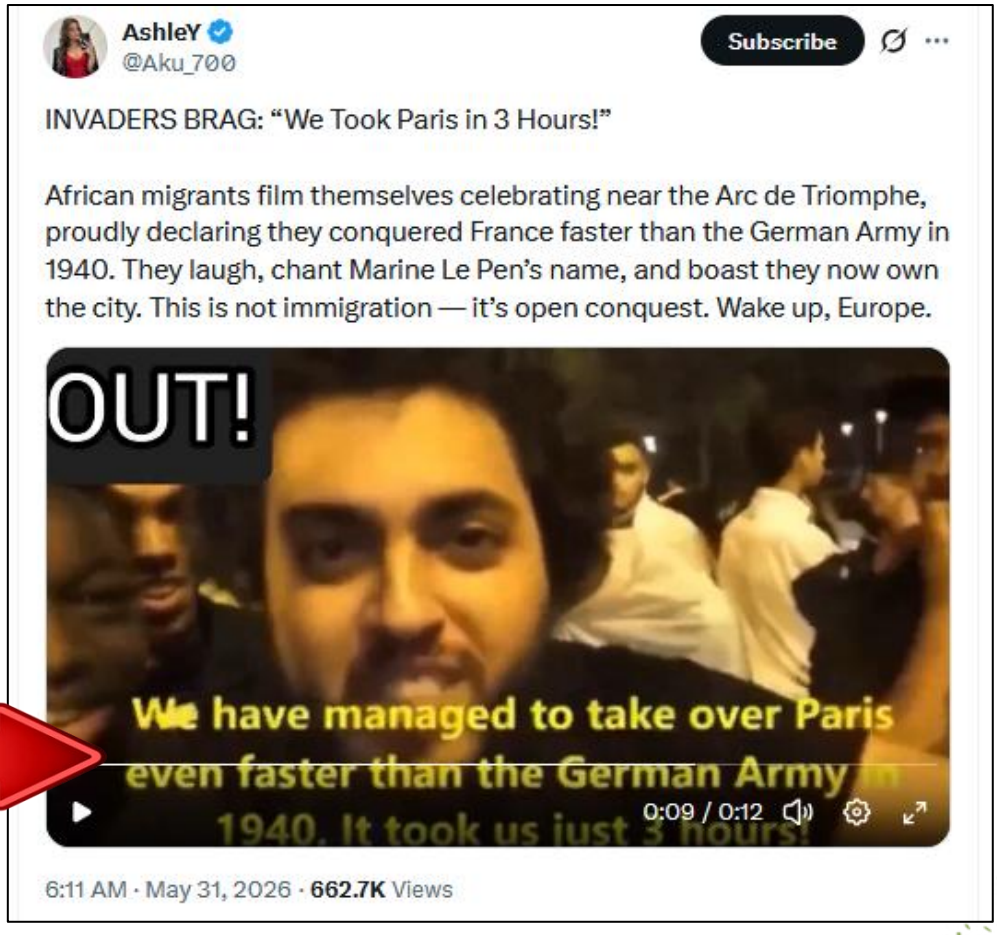
Intelligence work is almost the purest institutional embodiment of the opposite idea. It is the organized, sustained attempt to cut through noise: to determine whether Iran is moving toward a nuclear weapon, whether China is preparing to move on Taiwan, whether Russia interfered in an election, whether a foreign gang is

acting on a hostile government's orders. That work rests on the conviction that there is such a thing as objective reality and that democratic leaders have a duty to face it. Nothing is more alien to the populist mind. Populist movements in the United States and beyond have long treated experts, analysts, and career officials as a self-dealing caste, a "deep state" arrayed against the authentic people and their leader. Seen in that light, Trump's pattern of appointments is not only revenge for the Russia investigation, though it is certainly that. It is also a deliberate act of institutional degradation. To put Gabbard in charge of the intelligence community and then replace her with Pulte is to announce, in personnel form, that expertise is worthless, experience is dispensable, and loyalty is everything. The point is not merely to capture these institutions. It is to demean them, to show that the painstaking work of thousands of analysts and officers can be overridden by loyalists with little relevant knowledge and no evident respect for the vocation they are supposed to lead. Oscar Wilde defined a cynic as a man who knows the price of everything and the value of nothing. Trump's approach to intelligence is more nihilistic than cynical. He does not simply undervalue institutions like the DNI. He denies that their core activity—the patient, painstaking search for truths, whether inconvenient or not—has any value independent of how it serves him.

To give such a president a pliant housing regulator as his top intelligence adviser is to answer, in advance, the question that history has sometimes forced upon American intelligence chiefs: when the president asks you to lie, or to misuse what you know, or to abuse your oath of office, will you say "No"? Nixon discovered that Richard Helms would. Everything known about Bill Pulte's tenure in government suggests **that Trump will never have to worry about hearing that word.**

Ben Frankel is the editor of the Homeland Security News Wire.

What is this? Ce qui se passe?



RIEAS
RESEARCH INSTITUTE for EUROPEAN and AMERICAN STUDIES

The Future of Warfare: Operational Lessons from Ukraine's 2026 Counteroffensive – The new military strategy: "*Logistics Lockdown*"

Dr Darko Trifunovic

(Senior Research Fellow of RIEAS and Director of INIS)

Irish Leviathan is back?

After decades of bloody hostility, Protestants and Catholics are rallying, united against a common threat brought to the country by their governments in London and Dublin, which is illegal immigration. K. Starmer does not seem to understand what he has unleashed. For more than three decades, violence in Northern Ireland has been an everyday occurrence. Information from Northern Ireland reports that the old weapons and ammunition depots of the IRA and Ulster organizations (which were never handed over to the authorities) have been opened and, mind you, the Starmer government has managed to "awaken" the Irish "Leviathan".

How the Greek Language Continues to Shape English

Ukraine's military has a real Nazi problem

By Marta Havryshko
Source: https://responsiblestatecraft.org/nazis-in-ukraine-military/

June 07 – When Vladimir Putin launched his invasion of Ukraine in February 2022, he claimed one of his goals was the country's "denazification." The Kremlin still uses this narrative as a cornerstone of its war propaganda.

Both Ukraine and the West reacted by dismissing the claim outright as a cynical abuse of Holocaust history. Politicians, media outlets, academics, and educational institutions rushed to prove that Putin's argument was fraudulent.

But in their zeal to deconstruct Russian propaganda, Western elites created a propaganda myth of their own: there are no Nazis in Ukraine. Or, if there are, they are supposedly isolated cranks with no influence.

This fiction required the whitewashing of Azov, a unit founded in 2014 by the neo-Nazi group Patriot of Ukraine under the leadership of Andriy Biletsky. Azov became notorious for extremist ideology, Nazi symbolism, and allegations of war crimes in the Donbas. In 2018, the U.S. Congress banned the group from receiving American weapons, funding, or training. After Russia's full-scale invasion, that stigma vanished almost overnight. Kyiv repackaged Azov, separating the most radical elements into a new formation, the 3rd Assault Brigade. Western media rebranded and whitewashed it. The language of "de-radicalization" and "depoliticization" became mainstream. Questioning this narrative became taboo and labeled as "Russian propaganda." The result is a culture of deliberate silence.

Neo-Nazi networks are deeply embedded in parts of Ukraine's military structure. Their presence is visible in units such as Azov, the Third Assault Brigade, the Russian Volunteer Corps, Bratstvo, the German Volunteer Corps, Karpatska Sich, and others. Yet Ukraine's Western backers continue to arm, fund, and train these units without meaningful scrutiny.

Even more striking is the normalization of Nazi imagery itself. Official Ukrainian military channels and mainstream media regularly publish images of soldiers wearing swastikas, Waffen-SS insignia, and patches linked to neo-Nazi groups like Combat 18 and Misanthropic Division. This is no longer treated as scandalous. It has been normalized.

Most disturbing of all, some Ukrainian military units have incorporated Nazi-linked symbols into their official insignia.

The far right and Ukraine's military culture

Many Ukrainian military units using Nazi symbols are led by men shaped by Azov and the far-right milieu around it. For example, there is Oleksandr Kravtsov, the well-known commander of the Vedmedi unit, which was part of Azov. His body is

covered in Nazi imagery, including 1488 — references to the white supremacist "14 Words" slogan coined by David Lane and the coded salute "Heil Hitler." ("H" is the eighth letter of the alphabet.) Tattooed across his chest is the SS motto: *"My Honor Is Loyalty."* He turned that slogan into the motto of his own unit. SS lightning bolts became part of its official insignia. After returning from Russian captivity, Kravtsov's unit was folded into the Ukrainian military structure — first the 36th Brigade, then the 39th Coastal Defense Brigade. Nothing changed. The SS symbols and motto remained.

Many commanders in the 3rd Assault Brigade also came out of Azov and still hold extremist views. Unsurprisingly, they openly embrace the corresponding symbolism. A subunit of the 3rd Assault Brigade adopted a modified insignia (replacing two grenades with three) of the Dirlewanger SS Brigade — one of the most notorious Nazi formations of World War II. In 2025, the brigade unveiled the emblem publicly at a memorial in Kyiv. No scandal followed. Azov also normalized the Black Sun — a symbol born in Himmler's SS cult headquarters at Wewelsburg Castle and now used globally by neo-Nazis and white supremacist terrorists, including the 2019 Christchurch mosque terrorist in New Zealand and the recent San Diego Islamic Center shooter. After 2022, Black Sun spread rapidly through Ukrainian military culture. It appeared in Azov-linked units such as the Decepticons platoon and the Mortars unit of the 3rd Assault Brigade. Soon it migrated further — into units with no openly ideological profile at all — and became part of the insignia of the 156th Zvaha Battalion and the Unmanned Systems Battalion of the 110th Brigade named after Marko Bezruchko. Azov mainstreamed another Nazi-linked emblem as well: the Wolfsangel, used historically by several Waffen-SS divisions. Rebranded as the "Idea of the Nation," it became one of the most recognizable symbols in Ukraine's wartime military culture. The symbol now appears far beyond Azov itself. The newly created Nachtigall Battalion — named after the Nachtigall Battalion formed by German military intelligence in 1941 — uses the same Wolfsangel-inspired insignia.

Some units within Ukraine's military do not hide their fascination with the Third Reich's military culture. For example, the 422nd Regiment of Unmanned Systems calls itself "Luftwaffe" and uses virtually the same eagle as Hitler's air force. Its commander, Mykola Kolesnyk, regularly appears with the symbol on patches and clothing. The unit even sells merchandise featuring the Nazi eagle — hoodies, mugs, T-shirts, caps, keychains — to fundraise for the war.

The Black Sun — a symbol born in Himmler's SS cult headquarters at Wewelsburg Castle

Not just aesthetic choices

The use of Nazi symbols in Ukraine's military is not merely an aesthetic problem. It is moral, political, historical, and legal.

First, it represents a form of historical revisionism and the gradual rehabilitation of Nazism itself — a direct challenge to the postwar Western consensus built on the memory of World War II. Within far-right military culture, Nazi imagery is often wrapped in romanticized narratives about anti-Soviet struggle. In practice this trivializes the sacrifice of the seven million Ukrainians who fought Nazism in the ranks of the Red Army alongside the Western allies (in contrast to the 300,000 who served in various military formations and police units on the side of Nazi Germany).

It also desecrates the memory of Nazism's victims in Ukraine: 1.5 million Jews murdered in the Holocaust, along with millions of Slavs, prisoners of war, Roma, the mentally ill, forced laborers, and countless others consumed by the machinery of racial extermination and exploitation.

Second, the problem is not only historical. It is profoundly contemporary. Every SS rune, Black Sun, or Wolfsangel displayed by Ukrainian soldiers hands the Kremlin another propaganda victory. Russian propagandists do not need to invent imaginary Nazis in Kyiv. They simply point to the insignia

openly worn by some of Ukraine's most celebrated military units — including formations branded as "elite," such as the 3rd Assault Brigade. Third, there is also a glaring legal contradiction. By openly using Nazi imagery, these units violate Ukraine's own 2015 memory laws, which explicitly ban the propaganda of the Nazi regime and the public use of its symbols. The law describes such acts as an insult to the memory of millions of victims and have penalties of up to five years in prison. Yet no one is prosecuted. Why?

Because the Zelensky government — and President Volodymyr Zelensky himself as commander-in-chief — have made a political bargain with the far right. Since 2022, far-right activists and networks have flooded into the security and defense sector. In conditions of total war and chronic manpower shortages, this alliance became politically convenient, perhaps even inevitable. Now it is becoming entrenched.

The state depends on radicalized military formations for manpower and battlefield effectiveness. The far right, in turn, receives legitimacy, weapons, influence, and institutional protection. What emerged from wartime necessity is evolving into mutual dependence.

Ukraine's Western partners have made their own bargain. They, too, depend on Ukrainian manpower to weaken Russia. And so they tolerate extremists inside Ukraine's armed forces as long as those extremists continue fighting. More than that, they remain largely silent about the ideology and symbols involved, because acknowledging them would mean admitting an uncomfortable truth — that the neo-Nazi problem in Ukraine is not simply a Kremlin invention.

Marta Havryshko is a U.S.-based author and researcher focused on Ukrainian nationalism, the far right, and the Russo-Ukrainian War. Havryshko holds a PhD in History from the Ivan Franko National University of Lviv in Ukraine.

Iran Is a Bigger Defeat Than Vietnam

By Paul Musgrave | Associate professor of government at Georgetown University in Qatar.
Source: https://foreignpolicy.com/2026/06/16/iran-vietnam-strategy-defeat/

June 16 – At his second inaugural, U.S. President Donald Trump pronounced his hope "that our recent presidential election will be remembered as the greatest and most consequential election in the history of our country." By losing his Gulf war, Trump has achieved that goal. His choice to launch a campaign against Iran was encouraged by others, but fully his own. It has led to a reversal that marks a strategic calamity far greater than the U.S. defeat in the Vietnam War.

Defeat in the Iranian war looks, on the surface, nothing like other U.S. military defeats. The speed of the war and its remoteness have lent an air of unreality to the whole endeavor. The White House has not been

burned, as it was in 1814; there have not been protests against a nonexistent draft. Even from my perch in Doha, where for the first weeks I could see and hear the war of missiles above my head, the past several weeks have been confusing. While shopping for groceries, filling my tank up with still-cheap petrol, and carrying on a Zoom call with distant co-authors, I have asked myself repeatedly, "Is this a war zone?"

The absence of substantial U.S. casualties in this conflict also masks the scale of the U.S. defeat. To be sure, the war has been deadly: Thousands of Iranians, combatants and civilians, have died in the fighting. Americans, however, have endured far fewer deaths: To date, fewer than 20 U.S. soldiers have died—and many of those in a single strike.

By comparison, the scale of what the Vietnamese call the American War is breathtaking. Millions of people, mostly civilians, died in more than a decade of fighting waged over much of the skies and jungles of Southeast Asia; of those, just under 60,000 were Americans.

So bitter was the experience that, for a generation, when Americans mentioned the word "Vietnam," they did not refer to the actual country or society that bears that name—about whom they remained largely ignorant even after years of struggle. In American usage, Vietnam was understood to be primarily a metaphor or a symbol for an American experience. To many ordinary Americans, it meant personal grief. For some elites, Vietnam was a cautionary tale about the hubris of power; for others, it was an error that hindered proper strategic calculation in the present. There was, however, a national consensus that Vietnam was a stain on the national fabric: A 2014 Chicago Council on Global Affairs poll found 58 percent of Americans described it as a "dark moment" and only 12 percent as something to be proud of.

The most difficult point to grasp about that conflict today may be why the United States fought so hard given how little the conflict turned out to matter to Washington. For all that U.S. policymakers waging war tolerated what would now be almost unimaginable casualties, U.S. failure in the war ultimately mattered little to broader American strategic objectives. As early as 1964, internal U.S. government debates questioned the "domino theory"—the idea that one country becoming communist would lead to its neighbors following—that would become popularly identified with the U.S. war in Vietnam.

That the war was ultimately irrelevant to Americans is not to say it was unimportant. The destabilization of Southeast Asia mattered: The mass graves of Cambodia bear mute witness to the toll of a conflict whose consequences spread beyond Vietnam's borders and after a peace had been officially signed. The result of the war mattered to Vietnam, as did the desperation of the refugees who fled in the years to come.

Yet those observations do not change the fact that, for the United States itself, the consequences of a costly defeat were, in the long run, relatively minor and inward-looking. The United States emerged from the wider Cold War triumphant. Vietnam itself is a power surprisingly friendly to the United States today. Compare that situation with the aftermath of Trump's war. The United States is inarguably in a weaker position than when it began this war of choice, with core U.S. strategic objectives harmed. Contrast how its military performance has seemed during this conflict with the U.S.-led coalition's war to reverse Iraqi President Saddam Hussein's conquest of Kuwait. In the 1990-91 conflict, the seeming ease with which Iraq's military was dismembered stunned the world. By contrast, the technically superior performance of U.S. arms in the Iran conflict has been overshadowed by the shallowness of U.S. arsenals, calling into question U.S. preparedness for a conflict with any foe more powerful than the Islamic Republic. The lasting image of high-tech combat from this conflict will be the blood-spattered bags of Iranian schoolgirls killed as the result of an apparent database error. And although U.S. defensive systems have performed well against Iranian missiles and one-way attack drones, Iran was nevertheless able to penetrate those systems to great effect, calling into question how those systems would fare against a more focused enemy or over a longer conflict.

Strategically, the outcomes are far grimmer. The United States achieved regime change of a sort: Rather than turning Tehran into a pliable client, the war made Iran more hard-line, leaving the Islamic Revolutionary Guard Corps effectively in charge of the country. Israeli and U.S. arms, however brutally effective in the first days of the war, ultimately demonstrated the limitations of kinetic solutions, to Iran's great benefit. Iran's nuclear program has now endured two rounds of joint Israeli-U.S. airstrikes. It seems unlikely a third would fare much better.The effects on U.S. leadership in the global system have been more profound. Regional allies, many of whom reportedly argued against the venture, bore the brunt of the costs of the fighting. Most tellingly, Iran learned that its capacity to throttle the Strait of Hormuz could deliver economic leverage on a worldwide scale.

Freedom of navigation has been a core U.S. strategic objective for more than two centuries; President Thomas Jefferson dispatched the Navy to halt tributary payments to Mediterranean powers in the early 1800s. The potential end of free passage of the Strait of Hormuz could portend a weaponization of trade routes with enduring and potentially grievous harm to world commerce.

The manner in which a war ends can tell as much as how it begins. After the American War, the United States could largely turn its back on Vietnam and its neighbors and concentrate on areas of greater strategic importance. Although some combination of a global shift to green energy and the hydrocarbon production of the United States might make a similar exit from the Gulf region attractive to at least some in

Washington, it will be difficult to copy the post-Vietnam departure. The world economy is, after all, more interwoven today than in the 1970s, and the Gulf plays a greater role in economic networks today than Indochina did decades ago. Global supply chains are wired to depend not only on Gulf hydrocarbons but on its helium, fertilizer, and aluminum. The linkages are not only economic. Continuing U.S. ties to Israel make a complete exit from the region unlikely and raise the prospect of further, perhaps more intense, fighting. The development of Iran's missiles, and potentially its nuclear program, makes the prospects for the 2030s much more dire not only for the region but for Europe and South Asia as well.

The United States, under whatever management, will confront these consequences while being itself weakened at home and abroad. Its allies will have less confidence in its capabilities; its public will be less willing to bear the costs of even productive engagement; its rivals will be likelier to challenge Washington's will. Those results will be far more lasting and severe than the U.S. failure in its war in Vietnam.

One thing will be similar, however. Decades from now, students looking back to understand this American conflict will raise the same question I asked about the U.S. war in Vietnam: Why? Scholars will provide many well-researched answers, but none that will ultimately prove satisfying.

Chilling predictions from 1997 suggest a 'crisis' that reshapes America peaks this year

By Rob Waugh

Source: https://www.dailymail.com/sciencetech/article-15894609/fourth-turning-crisis-prediction-america.html

June 21 – A decades-old book that claims history repeats itself in predictable cycles is drawing fresh attention for a chilling prediction about the year 2026.

Published in 1997, The Fourth Turning by William Strauss and Neil Howe argues that American history unfolds in recurring 80-year cycles, each ending in a period of upheaval known as a 'Crisis.'

The authors, who also coined the term 'Millennials,' predicted that this turbulent era would culminate in a dramatic resolution around 2026. Their forecast has sparked renewed interest due to several events that supporters say align with the book's warnings.

The authors wrote that a crisis beginning in the mid-2000s would reach a climax around 2020, then move toward a final resolution six years later.

Some readers have linked that prediction to the **COVID-19** pandemic, while others point to economic and social turmoil over the past two decades.

But the book's vision of what comes next is far from reassuring, as Strauss and Howe warned that the resolution of the current cycle could fundamentally reshape America and could even threaten the nation's survival.

Strauss and Howe wrote: 'If the Crisis catalyst comes on schedule, around the year 2005, then the climax will be due around 2020, the resolution around 2026.

'What will America be like as it exits the Fourth Turning? History offers no guarantees.'

The authors cautioned that the current crisis and its eventual resolution could have profound consequences, writing: 'It could mean a lasting defeat from which our national innocence - and perhaps even our nation - might never recover.' Although The Fourth Turning did not specifically predict events such as 9/11, the 2008 financial crisis or the Covid-19 pandemic, supporters argue it accurately forecast the broader direction of the US.

The book warned that America was heading toward a period of deep instability marked by economic turmoil, political division, declining trust in institutions and a series of national crises.

Believers often point to 9/11, the financial crash and the pandemic as events that fit the theory's predicted crisis era.

They also note that the authors suggested the turmoil would reach a climax around 2020, which they say aligns with the Covid-19 pandemic, social unrest and political upheaval that year.

Critics, however, argue the predictions were broad enough that major events can be retroactively matched to the theory, noting that the authors never specifically forecast any of those crises.

The book's most alarming warnings focus on what the authors believed could happen if the crisis era reaches its breaking point.

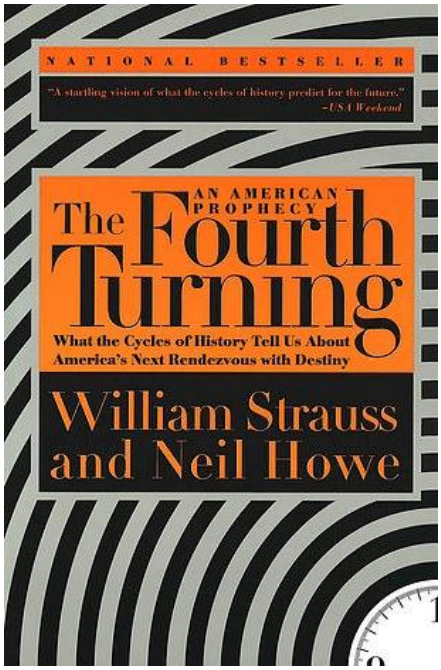
Strauss and Howe argued that societies throughout history have often collapsed under the weight of war, disease, political turmoil or economic catastrophe. America, they warned, should not assume it is immune from the same fate.

The pair suggested the next great crisis could take many forms, ranging from a devastating war or pandemic to terrorism, civil unrest or even authoritarian rule.

The book had chillingly specific predictions for 2026 - which sees the climax of a period of change the authors describe as 'the Crisis'.

'As many Americans know from their own ancestral backgrounds, history provides numerous examples of societies that have been wiped off the map,

ground into submission, or beaten so badly they revert to barbarism,' they wrote. The authors warned that a future crisis could bring consequences far worse than anything experienced by modern generations, adding that Americans should not assume the nation would always be spared from 'debasement and total ruin.'



At the heart of the theory is the belief that American history moves through repeating cycles lasting roughly 80 years, each divided into four phases: a High, an Awakening, an Unraveling and finally a Crisis, known as the Fourth Turning.

According to Strauss and Howe, the United States is now nearing the end of a cycle that began after World War II. Earlier cycles, they argued, culminated in defining national upheavals such as the American Revolution, the Civil War and World War II.

The theory later gained renewed attention after the 2008 financial crisis, which some supporters viewed as evidence that the Fourth Turning had already begun.

The book also made observations about declining faith in the American Dream that many supporters now view as strikingly prescient.

Strauss and Howe wrote that Americans were becoming increasingly optimistic about their own futures while losing confidence in the prospects of their children and the nation as a whole.

Nearly three decades later, some readers argue those concerns have become a defining feature of modern American life.

Following Strauss's death in 2007, Howe revisited the theory in his 2023 book

The Fourth Turning Is Here. While he pushed the expected climax further into the 2030s, he maintained that the current period of instability is part of the same historical cycle.

Despite its bleak warnings, Howe argues the theory ultimately offers a hopeful message.

Just as previous crisis eras eventually gave way to periods of rebuilding and renewal, he believes the current turmoil will eventually pass, potentially ushering in a new era of civic trust, stability and social cohesion by the mid-2030s.


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
M
O
D
T - NEWS
C²BRNE
DIARY

Counter-Terrorism Medicine Europe

A collaborative research initiative
Supporting clinicians and
Incident responders

https://www.ctm-e.org/

When will we put BRITS FIRST?!' Alex Armstrong issues GRAVE WARNING on Islamic terrorism in UK

Belgium gives 'coordinator' of 2015 Paris Islamist terror attack the right to temporarily leave jail

Source: https://www.timesofisrael.com/liveblog_entry/belgium-gives-coordinator-of-2015-paris-islamist-terror-attack-the-right-to-temporarily-leave-jail/

May 22 – One of the men convicted over the 2015 Islamist attacks in Paris that killed 130 people has been granted the right to prison leave in Belgium, sparking fierce criticism.

Belgian prosecutors tell AFP that a Brussels court decided **Mohamed Bakkali** could be temporarily allowed out of the Ittre detention facility south of the capital, where he is serving a 30-year sentence. "The court made this decision despite the prosecution's opposition. The prosecution has no right to appeal, and the decision is therefore final," the Brussels prosecutor's office says. "It is up to the prison director to implement it." The court's decision lets Bakkali — the logistics coordinator of the November 13 attacks that shocked the world — leave prison six times for 36 hours each. "What a disgrace," reacted right-wing Belgian lawmaker Denis Ducarme during a parliamentary session yesterday, lamenting a "trivialization of terrorism." "This decision seems to turn its back on the memory of the victims," he said. Belgium's Justice Minister Annelies Verlinden has said prison leave was granted under "very strict conditions" after "a thorough review of the case." Bakkali had been let out before, though for shorter periods of time, she added. A French court sentenced Bakkali to 30 years behind bars in 2022 for helping the Paris attackers by hiring safe houses and cars and procuring fake identity papers. He was also sentenced to 25 years in prison in Belgium over his role in an attack on a high-speed Paris-bound train that left two passengers injured. Belgian authorities handed him over to France for trial on condition that he returned to serve his sentence in Belgium.

Hamas operatives are being trained in Turkey to launch attacks against Israel - KAN

Source: https://www.jpost.com/middle-east/article-895545

May 08 – Hamas terrorists have been conducting training in areas of Turkey, Israel's public broadcaster KAN News reported on Thursday. The operatives, who wear civilian clothing, regularly participate in training sessions on the use of small arms and tactics at public shooting clubs, as well as training in drone operations. They have even received official licenses to fly drones in Turkey, the report said. The goal is reportedly to complete their training before transferring them to Lebanon, Jordan, and the West Bank in order to carry out attacks in future conflicts with Israel. This is by no means the first instance of coordination between Turkey and Hamas. Last December, the IDF and Shin Bet (Israel Security Agency) exposed an Iranian-sponsored money laundering network run by Hamas in Turkey.

According to an IDF statement, documents from the organization indicated that Hamas operates a network of money exchange involving Gazans located in Turkey, utilizing the country's financial institutions for terroristic purposes.

These Gazans, who manage to transfer hundreds of millions of dollars, are reportedly directly connected to Iran and to senior members of the Islamic regime.

According to the IDF's statement, the launderers also conduct extensive economic activity in Turkey - involving the transfer of funds from Iran to Hamas.

Germany supported Hamas-linked organization for years without tracking funds, audit finds

Source: https://www.jpost.com/international/islamic-terrorism/article-897262

May 25 – Until 2019, the German foreign office supported an aid organization with close ties to Hamas and the Muslim Brotherhood without knowing how the funds were actually being used. This information appears in a newly released confidential audit by Germany's Federal Court of Auditors, which the Institute for Secular Law (Institut für Weltanschauungsrecht or IFW) has been trying to obtain for five years. Until now, unsuccessfully.

The audit concerns state funding for the organization Islamic Relief, purported to have ties to Hamas and the Muslim Brotherhood. The now-public documents reveal, according to ifw advisory board member Seyran Ateş, "a shocking naivety on the part of the Foreign Office." Islamic Relief Germany (IRD) had long been regarded in Germany as a respected Muslim charity organization. Several consecutive German governments, including former chancellor Angela Merkel's second, third, and fourth cabinets, provided IRD with millions of euros in funding.

IRD was a member of the German aid alliance Aktion Deutschland Hilft, and gained prominent supporters for its "Meals for Orphans" campaign, including former President Christian Wulff and his successor Frank-Walter Steinmeier.

Foreign Office funded Islamic Relief largely 'blindly'

On April 15, 2019, the German government noted that both Islamic Relief Germany and its parent organization, Islamic Relief Worldwide, had "significant personnel connections to the Muslim Brotherhood or organizations close to it."

The government also admitted that since 2014 it had known that "Islamic Relief Worldwide," including its German branch IRD, was banned in Israel, regarded as "part of the financial system of Hamas and the Muslim Brotherhood movement," and therefore classified as a "terrorist organization."

It is worth noting that the IRW is also banned in the UAE, due to its ties to the Muslim Brotherhood.

The German government refused to provide detailed information on how public funds given to Islamic Relief had been used, instead referring to an ongoing audit by the Federal Court of Auditors.

The audit report was nevertheless classified as confidential.

Seyran Ateş, an IFW advisory board member, requested access to the findings under Germany's Freedom of Information Act (IFG) in 2021, but the request and the appeal were denied.

With support from IFW and its supporting organization, the Giordano Bruno Foundation, Ateş then filed suit against the Federal Court of Auditors and the Foreign Office.

According to IFW, the Foreign Office argued before the Berlin Administrative Court that publication of the report could lead to public controversy and polemical escalation; the IFW, however, insisted that citizens have the right

to know how their tax money is being used.
Ateş ultimately prevailed in two oral hearings before the Berlin Administrative Court. A special senate of the Federal Administrative Court then examined the full audit report to determine which passages contained protected intelligence material that could legally be redacted. After the Federal Administrative Court's ruling on September 10, 2025, Ateş and the Federal Court of Auditors, along with the Foreign Office, reached a settlement. The two-part audit report is now publicly available.
Part 1 examines whether Islamic Relief Germany was even suitable to receive public funding. Part 2 examines whether the Foreign Office fulfilled its duty to ensure the proper use of those funds. In both cases, the Federal Court of Auditors reached negative conclusions.
Regarding Islamic Relief's ties to Islamist actors, the auditors concluded in Part 1 that "The Foreign Office cannot explain the basis on which it concluded that Islamic Relief had a good reputation as a humanitarian NGO. In January 2009, it categorically rejected cooperation with IR. Why the Foreign Office later deviated from this clear and binding directive is incomprehensible."
Additionally, "According to letters from the Interior Ministry, dated March 4, 2004, and February 6, 2017, federal ministries are required, in line with the strategy of a comprehensive fight against terrorist organizations, to refrain from funding organizations against which constitutionally relevant security findings exist. We therefore advised the Foreign Office to discontinue funding IRD."
The second part of the audit concludes that the Foreign Office funded IR largely "blindly," often without reliable proof regarding how the money was being used.

A shocking naivety by the state in dealing with political Islam

In some cases, the Foreign Office did not even know that funding provided to Islamic Relief Germany had been forwarded directly to Islamic Relief Worldwide or Islamic Relief Turkey.
"According to the audit report, €240,000 was transported in cash-filled suitcases by plane from Germany to Turkey," Ateş said. "While this may sometimes be practical in crisis regions, in the case of organizations connected to extremist groups, this is grossly negligent."
The unredacted sections of the report contain no direct evidence that Foreign Office funds were actually transferred to the Muslim Brotherhood or Hamas or used to finance terrorist attacks.
However, Ateş argued that "given the documented 'blind-flight funding' by the Foreign Office, this is unfortunately entirely possible."
"The remarkably critical audit report documents a shocking naivety by the state in dealing with political Islam," Ateş continued.

EDITOR'S COMMENT: Unaware? Really?

The Islamic Terrorist Conquest of West Africa

By Lawrence A. Franklin
Source: https://www.gatestoneinstitute.org/22534/west-africa-islamic-terrorists

May 25 – The widened scope and quickened pace of the Islamic State's military operations in the Sahel region -- just below North Africa, roughly from Senegal to Sudan -- threatens to alter the strategic orientation of the African continent. Efforts at countering terrorist operations in the Sahel, such as they were, have evidently failed. As all roads to Mali's capital of Bamoko are now blocked, that country might be the first state to "go under."
On April 25, during a coordinated attack on several Malian cities, Muslim terrorists killed the country's Minister of Defense. The terrorists then drove the Malian Army and its allied Russian mercenaries out of the country's north.
The military juntas ruling Mali, Burkina Faso and Niger have proven themselves as ineffective at combatting Islamic terrorist operations as the democracies that they overthrew. The increasing terrorist assaults across the Sahel and the jihadists's determined efforts to take over Mali, Burkina Faso, and Niger have eroded the sovereignty of these states.
The combat successes of the jihadists in the Sahel in March 2022 precipitated their elevation to the status of "Islamic State Sahel Province" within the hierarchy of the IS, and several other factors have facilitated the growth of the jihadist advance in the Sahel.
The cooling of the once global counterterrorist crusade — following an apparent shift in focus by the world's great power rivalries, as well as fewer resources directed against the terrorist problem — left a vacuum that was adroitly filled by jihadist groups, which has reduced the pressure on Islamic State and Al Qaeda regional affiliates.
Another situation that might have impacted negatively upon the Sahel's overall security is the monumental migratory flow of Africans from sub-Saharan countries who pass through the Sahel to the Mediterranean, and the consequent stress this puts on the Sahel economies.

A third force eroding state sovereignty of Sahel countries is warfare waged by Al Qaeda terrorist affiliates that are rivals of the Islamic State, such as the Jama'at Nusrat al-Islam wal Muslimin (JNIM). JNIM also coordinates attacks with the Malian anti-government militia known as the Azawad Liberation Front.

Jihadist violence has become ubiquitous in the Sahel, and recently expanded to include fighting between Islamic State and Al Qaeda. On April 2, a notable clash between these two rival terrorist networks occurred in western Niger.

The Sahel now appears to be the epicenter of global terrorist violence. Sahel's terrorist groups might also be acquiring confidence that they can achieve permanent and more ambitious goals in the near future.

Islamic State units have also been exploiting the deteriorating security situation in the Sahel and in Nigeria's northeastern states, which are already governed under Islamic sharia law. Islamic State probably feels buoyed by its easy success in recent battles with the Nigerian Army.

On April 25, Al Qaeda terrorists conducted simultaneous attacks against several Malian urban areas. Their success might well tempt jihadist fighters to move into major urban areas in northern Nigeria and elsewhere in the Sahel.

An additional worrisome trend indicates that terrorist violence is moving westward to Africa's Atlantic coast.

State control increasingly is being eroded in the Sahel region, despite multilateral efforts to sustain the sovereignty of several states in the Sahel, such as the Multi-National Joint Task Force (MNJTF) consisting of Chad, Nigeria, Benin, Cameroon, and, until last year, Niger. The MNJTF had made significant strides in halting the advance of the Al Qaeda-affiliated Boko Haram terrorist group, particularly in Chad, but recently the overall scorecard is less conclusive.

The MNJTF is sustained mostly by the continent-wide Organization of the African Union (OAU). While the MNJTF originally planned to field a 10,000-member OAU army, insufficient air cover, poor communications, and logistical problems have reduced the organization's effectiveness.

Another multinational group — the "G5 Sahel" of Mauritania, Burkina Faso, Chad, Mali, and Niger — proved ineffective after its 2014 launch. Beset by bureaucratic problems, military coups, and lack of adequate commitment by member states, it dissolved in December 2023. France, the former colonial "mother country" of several Sahel states, has also made a valiant effort to contain the region's Islamist threat. Acting on behalf of a Malian request for military support, France in 2013 dispatched troops to northern Mali in "Operation Serval."

After substantial success, France, along with UN political support, launched "Operation Barkhane" in 2014 to combat Islamist terrorist activity in the Sahel region. The mission ended in 2022, however, when, following military coups, three Sahelian states asked the French to leave. Later, these same three states invited assistance from Russian mercenaries, which has not resulted in any permanent progress on the battlefield.

With the advance of Islamic terrorist control over ever wider swaths of the Sahel, in recent years, US Special Forces teams have been operating in Niger. On October 4, 2017, this deployment resulted in the killing of four US soldiers and a score of Nigerien soldiers in an ambush staged by "Islamic State in the Greater Sahara." More recently, US national security priorities elsewhere seem to have resulted in a diminution of American military involvement in the Sahel.

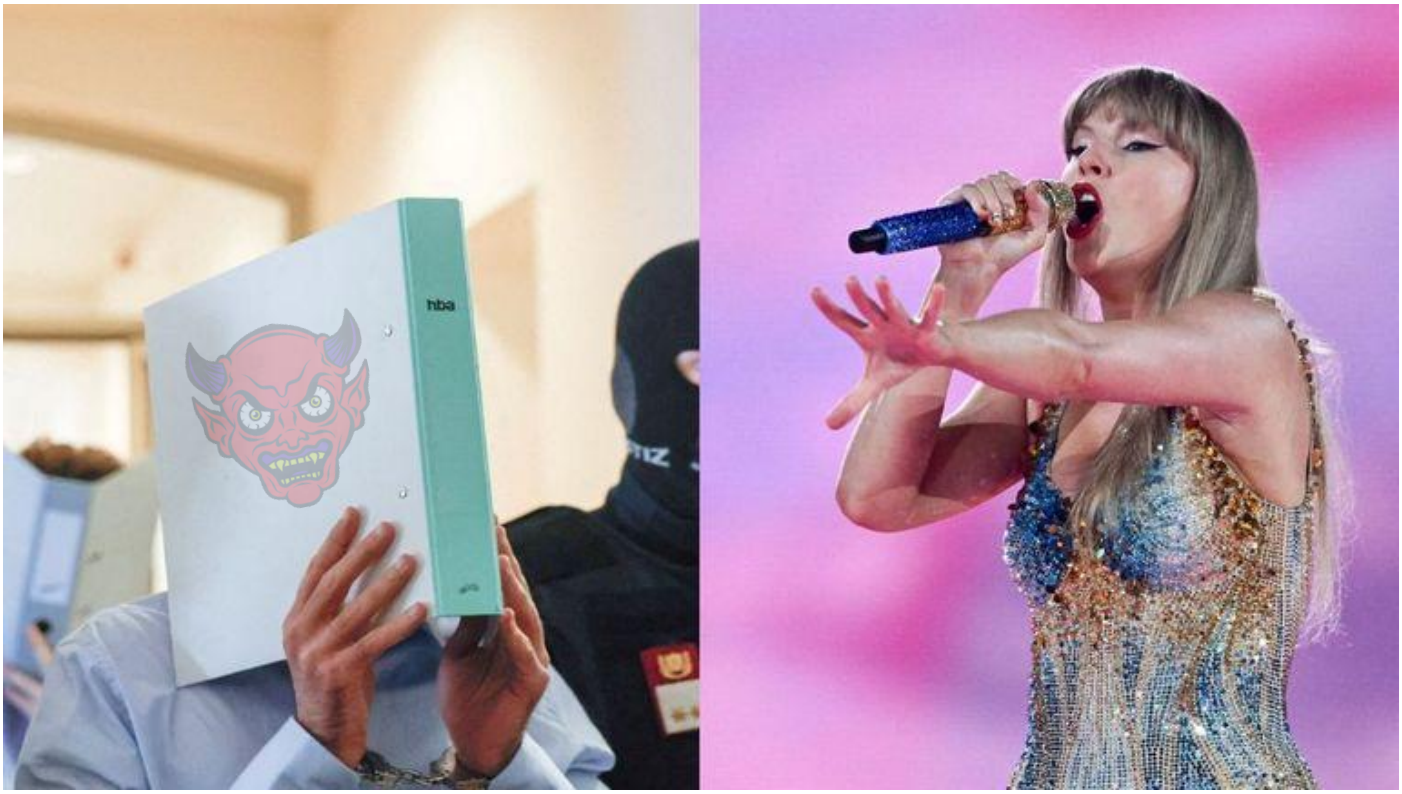
The steady advance of Islamic terrorist control over territory in the Sahel could soon threaten the sovereignty of West African states on the continent's Atlantic Coast -- just across the ocean from Latin America and the United States.

It is past time for the US to take action to protect not only the vast natural resources in the area, but also to stop even more of Africa from being swallowed up by this expanding jihadist takeover.

Dr. Lawrence A. Franklin was the Iran Desk Officer for Secretary of Defense Rumsfeld. He also served on active duty with the U.S. Army and as a Colonel in the Air Force Reserve.

Man jailed for 15 years over plot to attack Taylor Swift concert in Vienna

Source: https://www.bbc.com/news/articles/cgrp7y05l9do



May 28 – A 21-year-old Austrian man has been sentenced to 15 years in prison for planning a jihadist attack on a Taylor Swift concert in Vienna during the US singer's Eras tour in August 2024. The man, named only as Beran A in line with Austrian privacy laws, was also found guilty of a string of other terrorism-related offences. He was arrested after a tip-off from the CIA just before the first of three sold-out Taylor Swift concerts was due to take place in Vienna's Ernst Happl stadium.
All three Austrian shows were immediately cancelled, to the dismay of almost 200,000 fans and the singer herself.
Swift previously described how her record-breaking Eras Tour had narrowly "dodged a massacre situation". A tour documentary revealed the US singer had learned about the bomb plot while travelling to Austria.
Prosecutors said Beran A had become radicalised and had sworn allegiance to jihadist group Islamic State (IS). They said he tried but had not succeeded in buying weapons illegally, including a machine gun and a hand grenade.
Court psychiatrist Peter Hoffmann said Beran A showed no signs of mental illness, adding that there was "no psychiatric explanation" for his radicalisation.

EDITOR'S COMMENT: (1) Why is the terrorist allowed to cover his face? Does he have rights? (2) He became the first terrorist without psychiatric problems, ever! (3) And when we say 15 years, we mean 15 years + 1 day!

Man stabs 3 people at Swiss train station in what authorities call an 'act of terror'

Source: https://www.nbcnews.com/world/europe/man-stabs-people-swiss-train-station-terror-rcna347330

May 28 — A man stabbed and wounded three people in what authorities described as an "act of terror" at the train station in the Swiss city of Winterthur on Thursday before being arrested.
The attack took place shortly before 8:30 a.m. The suspect, who was arrested five minutes after emergency services were alerted, is a 31-year-old Swiss-Turkish dual national who lives in Winterthur, regional police chief Marius Weyermann said.

He had come to authorities' attention in 2015 for distributing propaganda of the Islamic State group, Weyermann added. In recent days, he was taken to a psychiatric facility after calling the police emergency number and making "confused comments," but he left on Wednesday after **a doctor determined that he wasn't dangerous**.
Three Swiss men, ages 28, 43 and 52, were wounded in Thursday's attack. The first two were discharged or were about to be released from hospitals by midafternoon, Weyermann said. The oldest was still hospitalized after an operation on a thigh injury.
Weyermann said investigators believe the man acted alone.

EDITOR'S COMMENT: When you observe a skin lesion, you do not wait for it to progress into melanoma to undergo surgery! And the psychiatrist who evaluated him should go back to school to update his expertise.

Australian woman charged with joining Islamic State after returning from Syrian refugee camp

Source: https://www.jpost.com/international/islamic-terrorism/article-897590

May 28 – An Australian woman who returned home in September from a Syrian refugee camp has been charged with allegedly joining the Islamic State and entering and remaining in a declared conflict zone, authorities said on Thursday. The 34-year-old traveled to Syria between 2013 and 2014 with others, including a man, to allegedly join the Islamic State, the Australian Federal Police (AFP) said in a statement. The man is believed to be in a prison in the Middle East, the AFP added. The woman is expected to appear in a Melbourne court on Thursday. Both offenses carry a maximum penalty of up to 10 years in prison. Kurdish forces detained the woman in March 2019, and she was held with family members in the Al-Hawl refugee camp. Police said she returned to Australia from Lebanon with another woman, 36, and that investigations into both women were ongoing. "It is important to note that a period of time without charges being laid is not an indicator that investigations have ceased," AFP Deputy Commissioner of National Security Investigations Hilda Sirec said.

Two women charged with slavery-related offenses, a third with terror

"Investigations are continuing into all the recent adult female returnees from Syrian camps."
The charges follow the return earlier this month of two women charged with slavery-related offenses and a third with terror offenses, including allegedly joining the Islamic State. A second group of Australian women and children arrived on Tuesday from a Syrian camp with no charges laid on arrival.
The return of both groups has drawn criticism from political opponents, who say the center-left government failed to stop their travel to Australia. The government says it did not assist their travel and that there are "very serious limits" on preventing citizens from re-entering the country.
Between 2012 and 2016, some Australian women traveled to Syria to join their husbands, who were allegedly members of the Islamic State. Following the collapse of the caliphate in 2019, many were detained in camps.

EDITOR'S COMMENT: Let the women live their dreams in Syria!

Counterterrorism: Team U.S. Shows its Game Plan

By Dr. Christopher C. Harmon
Source: https://www.iwp.edu/articles/2026/05/28/counterterrorism-team-u-s-shows-its-game-plan/

May 28 – How go the patterns of world terrorism, and what is the U.S. strategy for fighting back? Citizens and analysts of national security matters have a double opportunity to find out, just now. With the first week of May, we had the publication of two key U.S. documents long awaited. Our Department of State released its annual on trends and incidents called *Country Reports on Terrorism*. About the same moment, the White House published a *United States Counterterrorism Strategy*. Both are important for the second Donald Trump Administration, especially the strategy paper, a guide for what the White House counter-terror team has been doing and what we may anticipate in the realms of words and actions.
Marco Rubio's State Department was rumored to have axed the annual *Country Reports*. That would have been a mistake. It dates at least as far back as 1980, and 22 pages, then called "Patterns of Global Terrorism." This grew with time and enemy attacks into a sort of

encyclopedia of 300 pages. Facing occasional criticism, most often it has been authoritative and of great help to journalists, scholars, and government officials world-wide. The report's problems are dwarfed by its offerings. The newest issue—which arrives late—details year 2024 events but well anticipates many of today's news stories: Chaos in the Sahel region of Africa and states such as Mozambique and Congo. The quieter world of Western Europe, where Marxist-Leninist movements—and even Greek anarchists—have faded. Declines in most violence in the Philippines, a U.S. treaty partner with whom bilateral work is continuous. The persistence of Islamic State recruiting, and potential for more trouble given 8,700 detained fighters and some 42,000 displaced persons after our coalition crushed the caliphate during the first Trump term. Governments on State's dirty roster for sponsoring terrorism overseas also appear in each annual. Time has whittled down the list. Syria has just been de-listed in an inducement to the new (post-Asad) regime. Libya may still be a horror show domestically, but its government(s) are no longer exporting terror deliberately. Iraq reformed enough to be freed from State's sanctions. But Iran, proverbially tunneling under Iraqi sovereignty as always, has no chance of being de-listed. Cuba remains listed, since Colombian ELN leaders, Spanish Basques, and several U.S. terrorists, including a cop killer, have been able to lounge about there, enjoying freedoms denied to indigenous Cubans daring to have political opinions. North Korea, briefly removed as an international bargaining effort, is back on the list now; Pyongyang kidnapped citizens of Japan and, like Cuba, still shelters aging international terrorists. Of the three governments still on our State Department's blacklist, Iran, Cuba, and North Korea, it almost goes without saying that Iran is the most aggressive today in low-intensity conflict. State's new report mentions funding to HAMAS, to Houthi Shia attacking international shipping, and to other violent parties. It should do more to detail the shocking level of Iranian interference in Europe. From Albania, and north to England, Iranian nationals or agents have been in dozens of plots, some injurious, in recent years. When Labour's Prime Minister, Keir Starmer, said recently that the Iran war was something for the U.S. and Israel which did not engage British interests, he was ignoring MI5 evidence of twenty plots against his citizenry by Iranian perpetrators in just three recent years. North Western continental European countries have the same problem with Iran, which uses its intelligence agency MOIS, *and* diplomats, *and* independent actors in organized crime, *and* Hizbollah to plan and carry out attacks overseas.

Readers may be surprised to see this category in *Country Reports*: "White Identity Terrorism." Officially added to federal considerations in the Joseph Biden Administration, and tracking closely with his domestic counterterrorism strategy of 2021, this section offers paragraphs on international travel and internet connections by white racists, attacks in Scandinavian countries, and related militancy. More expected, from the Trump Administration, is emphasis in the new "Strategy" on international anarchism, and Antifa, which has recently been listed for U.S. sanctions. If the U.S. is able to show Antifa chapters sharing resources across borders, we may expect indictments for material support to terrorism.

There is no suggestion in these two new reports, or others of credibility, that global terrorism, or anti-American terrorism, is rising. Many countries with tens of millions of citizens do not see more than a half-dozen lethal attacks in a typical year. Six Americans were killed in 2024 terrorism, and others were injured or kidnapped, mostly in the Middle East. There are, of course, increased attacks against our public officials at home; these are not really addressed in the new strategy, which is focused on transnational matters. This new 16-page *U.S. Counterterrorism Strategy* (drafted by Dr. Sebastian Gorka) announces a logic of discussion of "Principles…Priorities…Goals…and Resources." Certain commentators have been quick to say these are under-developed, but that has often been a prominent view when any White House releases so short and unclassified a paper. Present national security staff advance the premise that Americans should not have to live in fear of armed fanatics desperate for popular support. That is well-said. What is different now is harsher language, and more threat of use of force. There have been armed campaigns, short or long, against multiple centers of terrorism since Mr. Trump assumed power 17 months ago, and this trend is underscored by his fresh threats of force now, this May.

Most secular governments escape the White House sights in this short new document. Sub-state narco-terrorist groups overseas get the first blast. Then the "Strategy" turns to religious militants and governing entities involved in transnational violence; these are directly called out, from Mali to the Middle East. If Iran represents the armed Shia threat to peace and world order, the White House names many other Sunni groups of self-declared "jihadis" to be put on notice. Those murdering Christians by the score in Nigeria and Sudan are twice touched in the new language.

Trump teams have often been accused of "Islamophobia," and the new strategy paper will not alter that trend in domestic American commentary. But with the possible and controversial exception of several Muslim Brotherhood chapters, the groups noted in black ink *have been* demonstrated to be lethal. Critics tend to forget that the types of hubristic "Holy Warriors" who grab Westerners and publish "Death to America" *fatwas* kill brother Muslims yet ***more*** freely. Consider the Afghan-governing Taliban's war with ISIS-K; both parties are Sunni extremists. When a bomb devastates another Shia mosque in the Islamic Republic of Pakistan,

the perpetrators are usually Sunnis. Al Qaeda controlled its blood lust against these "deviant" Shia, but ISIS glories in it: they slit the throats of such believers said to wander from the footsteps of Mohammed, and they smash the stone profiles of ancient men of Shia faith. In recent months, most detention centers in Syria holding ISIS members have been dismantled, making acts of violence from Islamic State adherents more likely, not less. Where ISIS attacks are indiscriminate, Muslims are at the same risk as others. We have seen that "force" and the showing of it are prominent in the new U.S. Strategy, and, indeed, there are a few lines of unnecessary bluster. But to be noted as well are all the lines about the many traditional American measures for contesting the terrorist plague. There are a dozen invocations to work with our security partners. The self-interest of many governments will move them in the direction of working with us, this White House paper states, and that is true. Encouraging such movement is the business of diplomats, and also intermediaries in "track two" diplomacy: With a Pakistani lady—a gifted Ph.D. in political science—I was honored to work with a team from the Maldives on their well-rounded political plans against radicalization; now, years later, we see that the island group is in our global coalition against ISIS. If terrorists are international, we must be also, and diplomacy and public diplomacy are vital. Intelligence is both a ground for understanding terrorists and a platform for striking against them. While the new paper mentions intelligence, it underserves the cyber dimension of defense and offense. A decade ago, the U.S. military created "Task Force Ares" to take down many Al Qaeda and ISIS servers and websites—a brilliant success—and such offensive power in our cyber toolkit remains, awaiting the fullest use.

There are, of course, covert measures making very limited or "discrete" uses of force. For some of the accused on whom we hold thick evidence files, rendition is a remedy. It was introduced into counterterrorism conversations by Ronald Reagan; it was just used again against the druggie-aligned Nicholas Maduro of Venezuela. Rendition can end in public trial and jail, which has many advantages.

Economic sanctions are a U.S. staple, too, even if their good effects may be limited and our non-allies may undercut them. "…the U.S. government will use diplomatic, intelligence, military, economic, law enforcement, and scientific capabilities, including kinetic and non-kinetic actions where appropriate, to thwart this threat." With such sober words, the May 2026 White House strategy document closes. It uses new words and promises new energy, yet the path is not unfamiliar to past American governments: diverse actions, tracking in the same direction, and reinforcing one another.

Christopher C. Harmon, Ph.D., wrote the textbook ***Terrorism Today*** (2000; 2008). His work on terrorism & counterterrorism subjects has also appeared from Cambridge and Oxford University presses and such journals as ***Vital Speeches, Orbis***, and ***The Fletcher Forum of World Affairs***. He teaches at The Institute of World Politics in Washington, D.C.

The Jihadist Wave in West Africa

By Alexander Palmer

Source: https://www.lawfaremedia.org/article/the-jihadist-wave-in-west-africa

Editor's Note: *Although the threat from the Islamic State and other jihadist groups appears to be declining in the Middle East, it is soaring in Africa. My Center for Strategic and International Studies colleague Alexander Palmer examines the growth of jihadist groups in West Africa in particular, discussing how their recent conquest of large amounts of territory is reshaping the terrorism landscape.*

Daniel Byman

***

May 31 – On April 25, 2026, al-Qaeda affiliate Jama'at Nusrat al-Islam wal Muslimin (JNIM) launched a major offensive against the Malian government alongside the Azawad Liberation Front (FLA), a separatist group. They have conducted attacks across Mali, killed the country's defense minister, and established a blockade of Bamako, the capital. The groups now control vast swaths of the country—including positions near Bamako. The ongoing offensive is the most visible manifestation of a years-long shift in favor of West Africa's Salafi-jihadist organizations. The growing power and reach of these groups is upending the current order. Policymakers should be planning for multiple scenarios, ranging from the emergence of a transnational terrorist hub to a frozen conflict.

West Africa's Salafi-Jihadist Landscape

West Africa is home to three main al-Qaeda or Islamic State affiliates: JNIM, the Islamic State-West Africa Province (ISWAP), and the Islamic State-Sahel Province (ISSP). In 2025, all three of these groups were on the march, demonstrating increasing capability and operating over ever-larger areas. JNIM's offensive is the most recent manifestation of its growing capability. In 2022, the United Nations Analytic Support

and Sanctions Monitoring Team assessed that JNIM commanded between 2,000 and 3,000 fighters. In 2025, estimates had risen to 5,000-6,000. That year, the group imposed a blockade across much of southern Mali and temporarily overran two provincial capitals in Burkina Faso. During the same time period, JNIM also increased its income through both informal taxation and, possibly more important for the current offensive, large infusions of cash acquired by ransoming foreigners. In November 2025, the United Arab Emirates allegedly paid the group $50 million for two of its citizens, an enormous windfall for the group. JNIM's main Salafi-jihadist rival is ISSP, which operates primarily in the border areas between Burkina Faso, Mali, Niger, and Nigeria. ISSP is smaller and less capable than JNIM, commanding a few thousand fighters and relying on small-scale guerrilla attacks rather than the type of direct military confrontation JNIM increasingly prefers. Even so, ISSP is operating with growing capability and confidence. In early 2026, it conducted an unprecedented attack on Niamey's international airport and the adjoining Air Base 101, where Nigerien military and international forces (including Russian Africa Corps personnel) are stationed. It has also expanded its operations into Nigeria, in partnership with or under the guise of the group known locally as Lakurawa. ISWAP is the largest and most powerful Islamic State province in Africa. It operates primarily in the Lake Chad basin, although its spread westward into Nigeria has brought it into closer contact with ISSP. As of mid-2025, ISWAP probably commanded between 8,000 and 12,000 members. Between July 2024 and July 2025, it claimed more attacks than any other Islamic State province worldwide. In 2025, it also escalated its campaign against the Nigerian state, launching a set of coordinated attacks against the "super camps" that the Nigerian military established to prevent ISWAP from overrunning its smaller, more isolated military outposts. It has also continued to conduct attacks in Cameroon and Chad.

Countries at Risk

Even if JNIM's current offensive fails to topple the government in Bamako, it will probably try again. While analysts disagree on JNIM's exact goals, statements by JNIM leaders suggest that the group wants to overthrow the Malian government and replace it with a government that enforces its interpretation of Sharia. How exactly the group wants to achieve that goal, as well as what it believes will come after, remains murky. Last year, the group attempted to trigger a government collapse through economic warfare, blockading southern Mali and calling on Malians to overthrow the government.

Burkina Faso also faces growing challenges from Salafi-jihadist organizations. Although the country experienced a decrease in terrorism-related deaths in 2025, this may be attributable to JNIM shifting its focus to Mali, and attacks were deadlier on average. As such, if JNIM turns its attention back to Burkina Faso, it could increase pressure on the regime quickly. Salafi jihadists in Burkina Faso already hold vast swaths of territory, and Ibrahim Traoré's military government has claimed that it put down several coup attempts since coming to power in 2022.

Finally, Nigeria's role in the region is changing. Africa's most populous country, Nigeria has a long history of participation in peace and stability operations, including those organized through the African Union, the Economic Community of West African States (ECOWAS), and the United Nations. However, its role as a security exporter is declining. The traditionally Nigeria-led ECOWAS's failure to reverse Niger's 2023 coup despite threatening to do so by force has demonstrated Nigeria's decreasing power in the West African security architecture, as did Burkina Faso, Mali, and Niger's withdrawal from ECOWAS in January 2024 and Niger's withdrawal from the Multinational Joint Task Force in March 2025. While the causes for Nigeria's declining influence are complex, its deteriorating security landscape plays a role. Terrorist violence in Nigeria increased in 2025, and the Nigerian military is increasingly overstretched by internal challenges. How often it can repeat successes like ECOWAS's December 2025 prevention of a coup in Benin is an open question. Nigeria's decline as a security exporter makes instability in West Africa more likely to erupt into major crises.

Potential Futures

The number of active threats, their cross-border nature, and the internal dynamics of the region's governments—both military and civilian—make it difficult to chart the future of West Africa, but it looks increasingly grim.

Policymakers should prepare for at least three possible outcomes to the continued rise in Salafi-jihadist violence in West Africa: that the region becomes a hub for global terrorism, that the Sahel descends deeper into civil war as groups and states fragment, or that the conflict enters a stalemate in which the countrysides and some cities are held by Salafi jihadists while capitals are still held by existing governments.

Despite its strength, JNIM itself is likely to play an indirect role in global terrorism. The United Nations reported internal debates within JNIM regarding its future relationship with al-Qaeda as recently as July 2025 and asserted that JNIM was "observing developments in the Syrian Arab Republic closely," implying that it is considering severing ties with al-Qaeda in pursuit of recognition and aid. In addition, International Crisis Group interviews suggest that the group's operational goals are regional rather than global, and the group's public statements increasingly focus on local conditions and even suggest openness to negotiation with the Bamako government.

That said, JNIM could still host international terrorists seeking the space to plot attacks, much as the Taliban provided safe haven to al-Qaeda in the 1990s. JNIM remains an al-Qaeda affiliate, and some analysts argue that JNIM rhetoric signals a meaningful alignment with al-Qaeda's global ideology, In addition, JNIM's calls for dialogue are conditioned on the government's acceptance of Sharia and the withdrawal of foreign troops—a maximalist position barely better than government surrender. If a JNIM victory leads to increased conflict with ISSP or even its current allies in the FLA, al-Qaeda's expertise, financial support, and ideological credibility could grow even more useful for JNIM, increasing its incentives to host international terrorists.

West Africa's Islamic State groups are more likely to engage in global terrorism. They have become more integrated into the global Islamic State network in recent years, and some governments even assess that the head of the Islamic State's West Africa office may have become the head of the General Directorate of Provinces, which organizes international terrorist attacks. ISWAP has also been bolstered by foreign fighters in recent years, which has increased its operational capability and could shift the group toward a greater interest in international terrorism. While such a development could contribute to the Islamic State core's continued weakening relative to its more locally oriented provinces, it could also presage an increasing African role in international Islamic State terrorism.

There is also some evidence that terrorists compete with each other by "outbidding," engaging in increasingly extreme violence to win over potential recruits. Given JNIM and ISSP's competition in the Sahel—and the global contest between al-Qaeda and the Islamic State—JNIM's success could prompt Islamic State efforts to outbid it through increasing violence. Such efforts could include international attacks like those the Islamic State-Khorasan Province attempted following the Taliban's successful counterinsurgency campaign against the group or through the declaration of a caliphate in West Africa, despite the theological obstacles to such a declaration. The need to win back attention and recruits from an ascendant JNIM could push ISWAP and ISSP further toward international terrorism.

Another possible outcome is a descent into even greater chaos, which—like the current conflict—is likely to spill over national borders. JNIM is already at war with ISSP, despite occasional periods of deescalation. In addition, Mali and Burkina Faso are both home to local self-defense militias that could become insurgents in their own right if those countries' capitals were to fall. The fact that many of these militias are organized along ethnic lines only increases the situation's combustibility. Finally, JNIM itself could fragment. The group is aware of the threats that expansion poses to its cohesion, and success could lead to competition within the organization over spoils or increased tensions between the group's leadership and its foot soldiers.

JNIM's relationship with the FLA will be particularly important. The FLA is an ethnic separatist group rather than a Salafi-jihadist organization, and its agenda differs from that of JNIM. The predecessors of both the FLA and JNIM collaborated in the 2012 uprising in northern Mali before falling into open war due to ideological and political differences. According to Wassim Nasr, JNIM and the FLA agreed to enforce some version of Sharia in northern Mali and jointly govern urban areas to enable the current offensive. How these two provisions are implemented in the areas the groups now control—especially the northern city of Kidal—will serve as early indicators of whether or not the alliance is likely to hold.

Greater international support for West Africa's embattled regimes could stabilize the conflict, leading to a scenario in which violence continues but regional governments are unlikely to fall—a situation that has characterized Somalia for decades. Who exactly will support these states remains an open question. Russia is currently the main external partner of the Burkinabe, Malian, and Nigerien regimes, but has withdrawn from positions across Mali during the current offensive. France, which has historically been extremely involved in West Africa, is deeply unpopular in the region. The United States has begun to increase its engagement, but its appetite for the type of extensive and sustained security cooperation needed by West African governments is questionable at best. Other countries like Algeria, China, Turkey, and the United Arab Emirates all have important interests in West Africa and could make limited contributions.

Changes to West Africa's Salafi-jihadist landscape are ushering in an uncertain future. The region's overlapping ethnic, political, and religious conflicts—as well as the actions of external powers—will all play roles in determining the balance of power between existing governments and these jihadist organizations. JNIM currently has the initiative, and how its actions affect the calculations of ISSP, ISWAP, and al-Qaeda will help determine whether West Africa emerges as a hub for transnational terrorism or whether the crisis remains contained to the region.

Alexander Palmer is a fellow in the Warfare, Irregular Threats, and Terrorism Program at the Center for Strategic and International Studies (CSIS). Prior to joining CSIS, he worked in Afghanistan, where he provided security analysis to humanitarian and UN staff before and after the withdrawal of international military forces in August 2021. He holds a master in public policy degree from the Harvard Kennedy School of Government.

Experts warn Australia a 'perfect' target for new 'ghost proxy' Islamist terror network

By Riley Stuart in London
Source: https://www.abc.net.au/news/2026-06-01/australia-perfect-target-for-islamist-terror-network/106694730

Soldiers in Antwerp, Belgium, were deployed to guard Jewish institutions after HAYI attacks. *(Reuters: Yves Herman)*

May 31 – Authorities in the United States have arrested and charged a man they allege "planned, coordinated and claimed responsibility" for 20 HAYI attacks — a prosecution that is in its early stages.

Australia would be the "perfect" target for a fledgling Islamist terror network that has carried out multiple antisemitic attacks in Europe, the United Kingdom and Canada, experts have warned.

Harakat Ashab al-Yamin al-Islamia, or HAYI, first emerged online in March and has so far professed to be behind about 20 acts of violence against Jewish people, buildings and symbols. Authorities in the United States, and experts in multiple countries, have identified numerous connections between HAYI and Iran.

But this group behaves differently to the Islamic Republic's chief militant proxies, such as Hamas and Hezbollah, and established jihadi organisations elsewhere, such as Islamic State and Al Qaeda.

HAYI has been described as a "ghost proxy" for Iran. Unlike other groups, it does not have a strict hierarchy or use ideologically motivated operatives for attacks.

Instead, it has a more fluid structure, where local criminals are recruited to carry out antisemitic missions.

The first attack HAYI claimed was an explosion outside a synagogue in the Belgian city of Liège on March 9. More recently, the group declared it had been behind an April 29 stabbing in north-west London, in which two Jewish men were seriously injured. Guy Fiennes is a research analyst at the Institute for Strategic Dialogue, an independent not-for-profit that aims to safeguard democracies against extremism. He describes HAYI as a "ghost proxy" directed by a "hostile state".

Instead of spending time and resources training militants, it recruits petty criminals and offers them money to carry out its attacks. Flexible work arrangements like this are often referred to as the "gig economy", and Mr Fiennes argues that term now extends to terrorism.
"We know this network is linked to Iran and its proxies," Mr Fiennes said. "Most of the perpetrators of these attacks appear to be financially motivated, and some of them claimed not to know who they were ultimately working for."
Initially, HAYI used the encrypted messaging service Telegram to publicise its activities, but the platform has since taken the group's channel down.
"I think foreign governments should be concerned about the phenomenon, and the idea other groups might look at it and think, 'OK, this tactic works. Let's copy it,'" Mr Fiennes said.
While the network has claimed responsibility for about 20 attacks, some experts warn it could be trying to inflate its influence by taking credit for crimes it had nothing to do with.

Alleged HAYI 'terrorist commander' arrested

On May 15, the US Department of Justice (DOJ) announced it had arrested and charged a man who allegedly "planned, coordinated and claimed responsibility" for 18 HAYI attacks in Europe and the UK, as well as two in Canada.
Mohammad Baqer Saad Sawood Al-Saadi, an Iraqi national with alleged links to Tehran-backed paramilitary organisations — including the Iranian Revolutionary Guard Corps (IRGC) — appeared in the US District Court in New York facing six terrorism-related offences.
The IRGC reports directly to Iran's supreme leader and is a proscribed terrorist organisation in Australia and the US.
"Thanks to the dedication and vigilance of law enforcement, this alleged terrorist commander is now in US custody," acting US Attorney-General Todd Blanche said in a statement.
The 32-year-old has also been accused of plotting to bomb synagogues in various locations around the US, and of explaining his plan to an undercover FBI officer.
The DOJ alleges HAYI is a front for Kata'ib Hezbollah, an Iran-backed, Iraq-based paramilitary group. It claims Al-Saadi is a senior member of Kata'ib Hezbollah.
Antisemitism has been in the spotlight in many Western nations in the past three years, including Australia, where multiple attacks have been linked to Iran.
Julian Lanchès, a research fellow at the International Centre for Counter-Terrorism, said Australia was an obvious target for HAYI.
"Iran has operated in Australia before, and we know that Iran is behind HAYI, so Australia works perfectly," he said.
"This group's attacks are getting so much attention. People are puzzled. The Jewish community is in fear.
"It seems to be an extremely successful hybrid terrorism operation. Given that, it could be that this group is considering taking it elsewhere, like Australia or the United States."
After 15 Jewish people were murdered and dozens more injured in a mass shooting at Bondi Beach late last year, the Albanese government announced a royal commission into antisemitism.
That attack has not been linked to HAYI, which has so far claimed less deadly events. For example, the group says it was behind a March arson attack on four ambulances in London belonging to the Jewish-run emergency medical service Hatzolah.
That same month, a 17-year-old boy was arrested outside the Bank of America headquarters, in Paris, attempting to ignite a homemade bomb.
It has been alleged HAYI recruited the suspect via the social media app Snapchat, and offered him 600 euros ($980) to carry out the operation.
"Basically, this is a new model of recruiting, where single-use agents are signed up online and offered money," Mr Lanchès said.
"Right now, there's limited evidence to tell us exactly what HAYI is and how it works, but we definitely need to take this seriously."

Why Has the United Kingdom Not Designated Iran's Revolutionary Guards as Terrorists?

Iran Recognizes the United Kingdom Is a Weak Link in Western Counter-Terrorism and Leverages That to Tehran's Advantage

Source: https://www.meforum.org/mef-observer/why-has-the-united-kingdom-not-designated-irans-revolutionary-guards-as-terrorists

June 02 – Every British opposition party has included the proscription of the Islamic Revolutionary Guard Corps in their party manifestos. However, once in government, none has moved forward with banning the organization. In the previous Conservative-led administration, the Foreign Office justification for inaction was the following: [Seventy] percent of Iran's economy is owned by the Islamic Revolutionary Guard Corps (IRGC) and all the diplomats are either IRGC or have been IRGC, so proscribing the IRGC would mean the United Kingdom could not do any trade or have diplomatic talks with Iran, and if the United Kingdom proscribes the IRGC, Europe won't, and therefore the United Kingdom will be left

alone in the cold and suffer in economic trade, while the European Union takes it all.

At the time, there was some justification to this argument. Josep Borrell, a Spanish socialist who was then-high representative of the European Union for Foreign Affairs and Security Policy, stated that such a designation would require prior legal determination. Borrell's remarks came after the European parliament's urged a ban of the Islamic Revolutionary Guard Corps. He argued that Europe could not make the decision on political grounds alone, but instead first needed a court ruling from a European Union member state. "You cannot say, 'I consider you a terrorist because I don't like you,'" he said.

Advocates argued that the British government might target individuals or entities without endangering trade and diplomatic relations.

Within the United Kingdom, there were suggestions that the British government, at a minimum, could proscribe the Qods Force. Advocates argued that the British government might target individuals or entities without endangering trade and diplomatic relations. This proposal also stalled.

At the time, some Iran-watchers found it frustrating when activists repeatedly cited examples of Islamic Revolutionary Guard Corps-linked terror as part of their campaign to force the British government to proscribe the Revolutionary Guard without engaging with the Foreign Office's reasoning, given that British diplomats were already aware of the Islamic Revolutionary Guard Corps' track record.

Cynicism was rife. While in opposition, the Labour Party insisted it would proscribe the Islamic Revolutionary Guard Corps if it came to power and criticized the Conservative government for not doing so. Yet almost two years after Keir Starmer won a landslide victory, his government has not acted on its pre-election promises.

The earlier justification that the European Union would not follow suit is now less relevant because the European Union finalized a decision to proscribe the Islamic Revolutionary Guard Corps on February 19, 2026. This designation brought the Guard under the European Union's counter-terrorism sanctions framework.

More recently, Europol-led enforcement action across 19 countries disrupted a coordinated Islamic Revolutionary Guard Corps propaganda and recruitment network. The operation reportedly led to the removal of more than 14,200 Revolutionary Guard-related accounts, posts, and links across social media platforms, streaming services, and blogs. The European Union designation provided the legal basis for coordinated action. Investigators also reported the use of artificial intelligence-generated content, religious and martyrdom narratives, multilingual messaging, and financial techniques such as cryptocurrency and international hosting services to sustain its online presence.

The United Kingdom, increasingly, is an Achilles' heel in any serious Western counter-terrorism strategy.

It is unclear why the United Kingdom has now fallen so far behind confronting Islamic Revolutionary Guard Corps activities in the West, despite several Revolutionary Guard-linked plots in the United Kingdom itself. One explanation is that the British legal framework differs from that of the European Union, though it is unclear what differences impact the lack of British action.

Former French military intelligence director and current member of the European Parliament Christophe Gomart has said that he views Qatar, Turkey, and London itself as major centers of Islamist extremist activity. Despite the gravity of his statement, it has received no coverage in mainstream British media.

The United Kingdom, increasingly, is an Achilles' heel in any serious Western counter-terrorism strategy. The Islamic Republic understands that the United Kingdom is a weak link and leverages that to Tehran's advantage. While British promises come easily in opposition, both U.S. and European officials must demand that the British government state why it continues to refuse to designate the Islamic Revolutionary Guard Corps. Allowing British silence is increasingly detrimental to Western security.

Potkin Azarmehr is a British investigative journalist and documentary filmmaker originally from Iran. He has contributed to various media outlets and think tanks, providing in-depth analysis of Middle Eastern affairs and Islamic extremism in the West.

ABSTRACT

Objectives The complex and dynamic care context of terror attacks must be better understood to reduce deaths. This study was designed to understand the tension between saving lives and maximising safety for emergency responders attending active terror incidents.

Design, setting and participants Qualitative study exploring the experience of survivors and emergency responders (armed and unarmed police, paramedics, doctors and fire officers) present in the hot (unsafe) zone of five major terror attacks in the UK since 2000. We used reflexive thematic data analysis to build qualitative case studies, comparing similarities and tensions between perspectives of different participant groups.

Results In our analysis of over 2000 min of interview data from 26 participants, we found a common view that the priority during a terror-related mass casualty event was to save lives. However, responder groups maintained distinct mental models that shaped their operational priorities regarding treatment for those injured within the hot zone. All responders expressed willingness to take self-assessed risks to save lives, but better interagency communication was noted to be required to achieve this safely. All responders felt it was vital to have experienced health professionals present to triage and facilitate urgent treatment and extraction decisions. Armed police commanders had dual responsibilities to achieve rapid care delivery while preventing further terrorist-inflicted injuries. Operationally, this was perceived as leading to a lack of shared mental models between responders regarding what is 'unsafe' due to zoning, rather than communication of risk, potentially delaying vital care delivery. There were mixed survivor perspectives regarding the risks that responders should be exposed to, but broad agreement that there was a notable absence of health professionals present in the hot zone during the immediate aftermath of attacks.

Conclusion There is strong professional and public support for improving care delivery, including potential hot zone working, to minimize the therapeutic vacuum in active terrorist attacks. Better risk communication and better shared mental models are necessary to balance responder risk with care delivery to maximize lives saved as safely as possible.

Between Tehran and Beirut: Iran's Growing Commitment to Hezbollah

By Raz Zimmt

Source: https://www.inss.org.il/publication/iran-hezbollah/

June 09 – Since the outbreak of Operation "Roaring Lion," and even more so against the backdrop of the escalation in Lebanon in recent weeks, the perception emphasizing Hezbollah's importance as a strategic component of Iran's security doctrine has grown stronger in Tehran. Hezbollah's decision to join the campaign alongside Iran was perceived in Tehran as an expression of its commitment to the pro-Iranian axis in the region and of the continued relevance of Iran's proxy strategy—which appeared to be eroding following the weakening of the Axis and the reluctance of Iran's allies, including Hezbollah, to join the campaign in June 2025. Iran's commitment to Hezbollah has been reflected in its insistence on binding any permanent ceasefire agreement with the United States to a ceasefire in Lebanon. This commitment reached its peak in Iran's strikes against Israel on June 7, following Israeli attacks in Beirut. Nevertheless, Iran continues to face significant challenges in implementing its proxy concept in the post-war period. These include the continuation of Israeli operations against Hezbollah; Israeli-Lebanese negotiations; growing criticism of Hezbollah and Iran within Lebanon; and worsening economic constraints inside Iran. Despite these challenges, it appears that, at this stage, the linkage between Iran and Hezbollah cannot be severed, partly due to the lack of any viable alternative to Iranian support for the organization. However, Israel can leverage the challenges and opportunities that have emerged in Lebanon to advance long-term processes that will help weaken the linkage between Iran and Lebanon.

The Importance of Hezbollah to Iran

An article published in early June 2026 by the online newspaper *Voice of Iran*, issued by the office of Iran's Supreme Leader, emphasized Hezbollah's significance to Iranian national security in the aftermath of Operation "Roaring Lion." Titled "The New Security Equation: From Hormuz to Beirut," the article argued that Iran would not return to the prewar period—not with regard to the Strait of Hormuz, the American military presence in the region, or the "Axis of Resistance." The war provided Iran with a strategic advantage, allowing it to advance a new regional order. Consequently, its relationship with the components of the pro-Iranian axis in the region, including Hezbollah, will no longer resemble what it was prior to the war, but will instead be determined by the reality that emerged in its wake. Iran's relationship with the "Resistance" in Lebanon is expected to grow even stronger, because Hezbollah's entry into the campaign not only reinforced its role as a central component of Iran's security doctrine, but also positioned it as part of the security balance of regional actors who refuse to submit to the United States and Israel. A second article, published in the same newspaper

on May 9, 2026, argued that Hezbollah is not merely a Lebanese actor but one of the pillars of the regional deterrence architecture. In the postwar reality, any threat to Hezbollah is viewed by Iran as a threat to the regional balance of power, making support for the organization a strategic necessity. The article maintained that Iranian support for Hezbollah must continue across political, media, and diplomatic spheres, and be defined as part of a broader conception of regional security, particularly in light of attempts to separate the various regional arenas from one another. Ultimately, the article claimed, developments in Lebanon are not just a local crisis but part of a broader struggle over the shaping of the future regional order in West Asia. Therefore, Iran's relations with the organization must be viewed as an enduring strategic alliance that will constitute one of the pillars of the regional balance of power in the years ahead.

These articles can be seen as an expression of the growing perception in Tehran that, in the wake of Operation "Roaring Lion," greater importance must be placed on preserving Iran's ties with the components of the "Axis of Resistance," foremost among them Hezbollah in Lebanon. Hezbollah is regarded as Iran's flagship regional proxy and a strategic asset that enables Tehran to attrit Israel and deter it from acting against Iran itself. It is also viewed as the organization most deeply committed to the Islamic Republic. The dynamic relations between Iran and the components of the "Axis of Resistance," including Hezbollah, as well as the constant tension between their ideological and political commitment to Tehran and their own distinct agendas and interests, have significantly shaped the character of Iran's proxy network. From the outset, this network—which also includes the pro-Shiite militias in Iraq and the Houthis in Yemen—did not operate as a hierarchical structure subject to direct Iranian command and control. Rather, it functioned as a loose network of actors bound together by a web of shared interests alongside a common ideological vision. In recent years, particularly following the assassination of Quds Force Commander Qasem Soleimani in January 2020, the network has undergone increasing decentralization. Soleimani's assassination posed a significant challenge to the proxy network, compelling Iran to manage it in a more decentralized manner than in the past. Iran continued to maintain considerable influence across the network, though not necessarily through full and permanent control over each of its components. At the same time, Hezbollah's former secretary-general, Hassan Nasrallah, assumed a more prominent role in managing the network's affairs, both by virtue of his experience and long-standing familiarity with Israel, and due to his pivotal status and influence in

Tehran, which grew stronger following Soleimani's assassination.

The Erosion of the Proxy Concept

Hezbollah's defeat by Israel in the summer of 2024 and the collapse of the Assad regime in Syria in December 2024 exacerbated the limitations of Iran's power in operating the regional network it had spent years cultivating. These limitations became particularly evident during Operation "Rising Lion," which further illustrated the erosion of the proxy concept. Iran's "Forward Defense" Doctrine, designed to intercept threats to its national security as far from its borders as possible through the use of proxy forces, ultimately failed to prevent Israel and the United States from launching direct attacks against it.

One of the primary objectives in constructing the "Axis of Resistance" was to deter Israel from striking Iran's nuclear facilities and to provide Tehran with an immediate retaliatory capability should such an attack occur. Yet, when put to the test, Iran's proxies did little to assist it during the war. The launch of Israel's military campaign against Iran in June 2025 caught the organizations of the pro-Iranian axis in deep crisis. Hezbollah, which had been intended to play a pivotal role in the Axis's "ring of fire" strategy and to assist Iran in the event of an Israeli attack, did not join the war because it was still unprepared to do so, limiting its involvement to declarations of support for Tehran.

As a result, the war intensified doubts that had already begun to emerge in Tehran regarding the effectiveness of Iran's proxy strategy. Nevertheless, it was clear that Iran had no intention of abandoning its allies in favor of a new regional strategy. Senior Iranian officials, led by Supreme Leader Ali Khamenei, continued to express support for the "Axis of Resistance" and confidence in its ability to confront Israel successfully. Amid growing pressure on Hezbollah to disarm, Iran stressed that the "Resistance" remains the only guarantee of Lebanon's security. Moreover, Iran renewed its weapons and funding supply routes to Hezbollah, including through Syrian territory. It also deepened its direct involvement in managing Hezbollah's affairs, as evidenced by the deployment of hundreds of officers from the Islamic Revolutionary Guard Corps who participated in Hezbollah's reconstruction and rearmament efforts.

Commitment to the Pro-Iranian Axis

Hezbollah's decision to join the campaign alongside Iran on March 2, 2026, following the assassination of Ali Khamenei at the outset of Operation "Roaring Lion" sparked a renewed debate over the effectiveness of the pro-Iranian regional Axis as a central component of Iran's deterrence strategy. Although it took Iran nearly two days to convince Hezbollah to enter the war, the death of the Supreme Leader ultimately persuaded the organization's secretary-general, Naim Qassem, to join the campaign in support of Iran. In Tehran, the decision by Iran's regional proxies to rally to its side was viewed as a demonstration of their commitment to the Axis. From Iran's perspective, this served to prove the enduring importance of this strategic concept. Senior Iranian officials emphasized the significance of the "Axis of Resistance" for Tehran, presenting it as a manifestation of its ability to maintain the concept of the "Unity of the Arenas" against Israel. For instance, in his first address to the Iranian people immediately following his election as Supreme Leader, Mojtaba Khamenei emphasized that Iran views the "Axis of Resistance" as an integral component of the values of the Islamic Revolution. Similarly, the Commander of the IRGC Quds Force, Esmail Qaani, underscored the importance of the Axis, declaring that it is now clear that "the 'Unity of the Arenas' constitutes a source of strength for the Islamic Nation and a nightmare for global arrogance [the West] and international Zionism."

Iran's commitment to Hezbollah was clearly evident in its insistence on linking any permanent ceasefire agreement between Iran and the United States to a ceasefire in Lebanon. Moreover, the renewed escalation in Lebanon in May 2026 provided Tehran with another opportunity to reinforce this linkage. Following the expansion of IDF operations in Lebanon, Iran intensified its threats against Israel. On June 1, Iranian Foreign Minister Abbas Araghchi warned that a violation of the ceasefire between Iran and the United States on any single front, including Lebanon, would be considered a violation of the agreement across all of them. On that same day, Iranian threats culminated in an announcement by the commander of Iran's emergency headquarters, Ali Abdollahi, stating that Iran would respond to an Israeli strike on the Dahiyeh district in southern Beirut by striking northern Israel.

In an interview with the Lebanese television network Al-Mayadeen on June 3, Araghchi warned that Iran would not tolerate an attack on Beirut, and that if Israel struck the Lebanese capital, Iran would respond by resuming the war. The pressure exerted by President Trump on Prime Minister Netanyahu to prevent Israel from carrying out its threats to strike Beirut was perceived in Tehran as further evidence of its success in enforcing the linkage it established between the Lebanese and Iranian arenas. From Iran's perspective, this achievement complements other gains from Operation "Roaring Lion," including the closure of the Strait of Hormuz and the damage inflicted on neighboring Arab Gulf states through missile and drone attacks. Together, these developments have further bolstered Tehran's sense of accomplishment and self-confidence in the wake of the recent war. Concurrently, coordination between senior Hezbollah and Amal officials and their Iranian counterparts continued throughout the war, with both sides taking care to give these interactions public

visibility. On June 2, the Speaker of the Iranian Parliament, Mohammad Bagher Ghalibaf, spoke with his Lebanese counterpart, Nabih Berri, emphasizing to him that if Israel continued its attacks in Lebanon, Iran will not only suspend negotiations with the United States but will also confront Israel directly. He stressed that Iran is determined to bring about a ceasefire across all of Lebanon, particularly in the country's south, and that if an agreement to end the war between Iran and the United States is reached, it will encompass the cessation of attacks in Lebanon as well. Prior to this, Mohammad Mokhber, advisor to the Supreme Leader of Iran, met in Tehran with Hezbollah's representative in the country, Abdullah Safi al-Din. He underscored the unity of the "Axis of Resistance" and noted that any ceasefire agreement with Iran that failed to include Lebanon would be meaningless.

On June 7, Iran acted on its threats and launched a direct attack against Israel, responding to the Israeli strike in Beirut's Dahiyeh district by firing several barrages of missiles at northern Israel. Tehran's decision to respond directly despite the limited nature of the Israeli strike reflects the Iranian leadership's willingness to risk renewed escalation with both Israel and the United States in order to uphold its commitment to Hezbollah. Iran's emphasis on support for Hezbollah and its efforts to link the Iranian and Lebanese arenas reflect not only a sense of obligation toward the organization but also a strategic approach that prioritizes its preservation and reinforcement. At the same time, they underscore the new Iranian leadership's continued adherence to the doctrine of "Resistance." This leadership, headed by Mojtaba Khamenei and the Revolutionary Guard Corps (IRGC), is hardline, unrestrained, deeply committed to Hezbollah and the "Resistance" doctrine, and self-confident. It is expected to maintain a rigid and defiant ideological posture, at least comparable to that which characterized the rule of Ali Khamenei. Statements by senior Iranian officials regarding the United States, Israel, and support for the "Axis of Resistance" leave no room for doubt regarding their refusal to retreat from the foundational tenets of the Islamic Republic. For instance, in a message published for Muslim pilgrims in May 2026, Mojtaba noted that the weapon of *"Allahu Akbar"* has strengthened the unity of the Islamic nation and young fighters of the "Axis of Resistance." He added that Iran's armed forces, alongside the fighters of the Resistance, especially in Lebanon, have achieved impressive victories against the Israeli and American militaries. Furthermore, Iran views the strengthening of the connection to the Lebanese issue as an additional means to leverage its achievements in the campaign, including its asymmetric military capabilities and its control over the Strait of Hormuz, with the ultimate goal of establishing a new regional order that recognizes its status and power. Tehran sees itself as being in a position to seize the initiative and impose new rules of the game on Israel and the United States that, in its view, reflect a balance of power tilted in its favor. This is particularly true given Tehran's assessment that President Donald Trump has no interest in renewing the war with Iran.

Challenges Facing the Axis and the Implications for Israel

Nevertheless, this does not mean that Iran is free of significant challenges in implementing its proxy strategy in the postwar period. These challenges include Israel's continued efforts to expand enforcement operations against Hezbollah's military buildup; the Israeli-Lebanese negotiations; the restrictions imposed by the Lebanese government on Iranian activity within its territory; the shared interest of the Lebanese leadership, Israel, and the United States to liberate Lebanon from Iranian influence; Hezbollah's relative weakness; the growing criticism against it within Lebanon—including among the Shiite public; and the Syrian regime's ongoing commitment to restrict the transfer of weapons from Iran to Lebanon through Syria. In addition, questions remain regarding Iran's ability to continue investing billions of dollars in rebuilding the capabilities of the "Axis of Resistance" and supporting its regional allies, given its fragile economic condition and its national priorities following the war. This is true even though Iran has repeatedly demonstrated a willingness to prioritize support for its proxies at the expense of the needs of the Iranian people. A further question concerns the viability of continuous investment in proxy forces compared to investing in Iran's other principal deterrence assets, foremost among them its missile program, its nuclear program, and its demonstrated ability to inflict severe damage on the global economy by closing the Strait of Hormuz. Moreover, Iran's efforts to prevent Israeli strikes on Beirut further exposed the limitations of the proxy concept: rather than the proxies defending Iran, Iran finds itself forced to protect Hezbollah. What is clear, however, is that the linkage between Iran and Hezbollah cannot be severed at this stage. This is not only because Iran is unwilling to do so, but also due to the absence of any viable alternative to Iranian assistance for Hezbollah, and through it, to the Shiite population in Lebanon. Furthermore, this linkage cannot be dismantled given the apparent recognition of its importance by the U.S. administration itself, as reflected in its efforts to maintain the ceasefire with Iran and advance a possible agreement with Tehran. Nevertheless, Israel can capitalize on the challenges facing Iran and Hezbollah, alongside the new opportunities that have emerged in Lebanon, to disrupt Iran's proxy strategy. By doing so, Israel can advance long-term processes aimed at strengthening the Lebanese state while weakening both the Islamic Republic and Hezbollah—efforts that could ultimately help weaken the linkage between Iran and Lebanon.

Dr. Raz Zimmt is the Director of the Iran and the Shiite Axis research program at the Institute for National Security Studies (INSS). He is also the co-editor of the institute's journal, Strategic Assessment. He holds a master's degree and a Ph.D. in Middle Eastern history from Tel Aviv University. His Ph.D. dissertation focused on Iranian policy towards Nasserism and Arab radicalism between 1954 and 1967.

'Horror' at north Belfast stabbing as MLA reacts to 'some of most depraved and barbaric violence I have ever seen'

Source: https://www.belfasttelegraph.co.uk/area/north-belfast-newtownabbey/north-belfast/horror-at-north-belfast-stabbing-as-mla-reacts-to-some-of-most-depraved-and-barbaric-violence-i-have-ever-seen/a/156285563.html

June 09 – A warning has been issued over social media footage circulating after a serious stabbing incident in north Belfast.

Police and paramedics were called to the incident in the Kinnaird Avenue area of the city at around 10:30pm.

Video posted to social media appears to show a Sudanese (?) man stabbing another man several times in the head with a knife.

The Belfast Telegraph understands police recovered a knife at the scene.

A large police presence remains in place with a large area of an apartment block cordoned off.

The "bravery" of an intervention has been praised after an eyewitness to the attack told the Belfast Telegraph "three men, one armed with a hurl, got the fella with the knife off the victim."

A spokesperson for the PSNI said: "Police in north Belfast are currently in attendance at Kinnaird Avenue following the report of a stabbing incident shortly after 10.30pm.

"A man has been arrested in relation to the incident and is in police custody while a second man has been taken to hospital with serious injuries."

Alliance North Belfast MLA Nuala McAllister has condemned the "depraved" attack overnight. "I am horrified by the footage emerging from North Belfast, depicting some of the most depraved and barbaric violence I have ever seen," she said.

"My thoughts are with the victim and all those who witnessed this deeply disturbing incident. This extreme brutality has no place whatsoever in our society."The investigation must be allowed to take its course. We must give the PSNI the space and support they need to establish the full facts and ensure that the individual responsible is held to account. Our focus must remain on securing justice and ensuring that those responsible face the full force of the law. "I'd appeal to anyone with any information that could help police to contact them urgently to help them with their investigation." SDLP north Belfast Councillor Carl Whyte asked social media users not to share footage of the incident out of respect for the family, and appealed for calm to "allow justice to take its course".

He said: "This was an appalling act of extreme violence. The victim of this attack has endured a terrifying ordeal and all our thoughts are with him and his family and we pray for his full recovery. The bravery of those who intervened saw the attacker stopped and arrested by the police and they must be commended for their actions.

"People who view this footage will feel fear, anger and shock. If you are sent this footage, I urge you not to view it nor share it further for the sake of the victim and his family. I have requested an update from the PSNI on this incident and there is a clear need to reassure the local community following this attack.

"I would also ask people not to engage with far-right elements who will use this incident in an attempt to sow division. It's important that people remain calm and allow justice to take its course." DUP Councillor Jordan Doran said he has been "left shocked and deeply concerned."

Taking to social media, he condemned the attack as "completely unacceptable, which understandably caused significant fear and anxiety amongst local residents. "The public will rightly expect a swift, thorough and robust investigation by the PSNI.

"Anyone found responsible for criminal acts of this nature must

face the full consequences of the law. "There can be no excuses and no tolerance for such brutality on our streets."
Sinn Féin MP John Finucane said the incident was "deeply shocking".
The north Belfast MP said: "I am aware of an appalling violent attack in Kinnaird Avenue of North Belfast last night.

"This is deeply shocking, there is no place for violence of any kind in our communities.
"My thoughts are with the victim and I hope they make a full recovery.
"I would urge anyone with information to come forward to the PSNI immediately so a full investigation can be carried out."

The day after in Belfast because patience is not endless!

EDITOR'S COMMENT: None of the mass media referred to him as a terrorist! In the days to follow, most probably we will read that this animal was known to authorities, that he was under psychiatric surveillance and medications, and all the usual stuff we are used to reading following similar incidents. Any action igniting terror is an act of terrorism! Just pray that this will not happen to you and your family!

In Germany, an Islamist was sentenced to 8.5 years in prison for planning a terrorist attack

Source: https://ua.news/en/world/u-nimechchini-islamista-zasudili-do-8-5-roku-viaznitsi-za-pidgotovku-teraktu

June 08 – The Regional Court in Bremen has sentenced a 35-year-old man found guilty of planning a terrorist attack. He was sentenced to eight and a half years in prison. According to the investigation, the defendant was involved in planning a terrorist attack and maintained ties to Islamist circles. The court found the evidence gathered to be sufficient to issue a guilty verdict.

The judges charged the defendant with conspiracy to commit murder, conspiracy to carry out an explosion, and financing terrorism. The court ruled that his mentally ill accomplice and nephew had limited capacity to control his actions. The 20-year-old man was acquitted but must be committed to a psychiatric hospital. The verdict is not yet legally binding.

The court was convinced that the two Germans had developed concrete plans for an attack last summer. **They intended to kill as many people as possible using firearms. Once emergency services arrived, the younger man was to detonate a homemade explosive vest. They considered a hospital, a large public event, or a synagogue in Bremerhaven as possible targets.**

The men planned to construct the explosive vest at the home of the 35-year-old defendant's mother, the court noted in its ruling. The woman ordered three different materials for testing in her kitchen. Ultimately, law enforcement thwarted their plans. During another investigation, they stumbled upon chats between the men and arrested them.

The trial also examined the backgrounds of both defendants. According to reports, the 35-year-old man converted to Islam several years ago and became radicalized. When his nephew was 14 years old, he allegedly showed him videos of executions carried out by the so-called "Islamic State" for the first time. These recordings are said to have intensified the teenager's obsessive thoughts and murderous fantasies.

The presiding judge is convinced that the 20-year-old defendant continues to pose a danger. Therefore, he ordered him to be placed in a psychiatric hospital. Otherwise, he might join the ranks of terrorists in search of social connections and recognition. His uncle, on the other hand, was found fully responsible for his actions and must serve eight and a half years in prison.

Hamas Launching "Strategic Shift" in Europe, Warns Greek Minister After Terror Arrest

Source: https://greekreporter.com/2026/06/09/hamas-strategic-shift-europe-warns-greek-minister/

June 09 – Greece's Minister for Citizen Protection, Michalis Chrysochoidis, has warned of a highly concerning "strategic shift" by Hamas, suggesting the organization may be expanding its operations into Europe following the arrest of a suspected operative on Crete.In an interview with radio station Parapolitika 90.1, Chrysochoidis pointed out that for the forty years since its founding, Hamas has traditionally restricted its violent activities to Israeli territory without causing external disruption. The potential establishment of European networks marks a dangerous departure from that history. "This is precisely what concerns us greatly—that it constitutes a strategic shift by Hamas," Chrysochoidis said, emphasizing the need for constant, continent-wide vigilance. "We need to see exactly what this means and understand the potential scope of such a danger, such a threat." The Minister also firmly rejected the idea that European security forces are dealing with isolated actors. When asked if recent threats could be classified as "lone wolf" actions, Chrysochoidis called the term unfortunate. "No one can carry out an action on their own; it requires extensive preparation, extensive training," he explained. "Let's abandon these images of the lone wolf and focus on efforts carried out by organizations or through coordinated campaigns aimed at striking specific targets."

Hamas suspect in Greece faces court deadline

The Minister's warnings come in the wake of a major counter-terrorism operation in Agios Nikolaos, Crete, where a 37-year-old Palestinian man was arrested for allegedly plotting terrorist attacks against Israeli interests using improvised explosive devices (IEDs). The alleged terrorist, who was detained in

Crete, had arrived in Greece approximately one year ago and held an active asylum application at the time of his arrest.
Among the items confiscated were chemical substances and laboratory measuring equipment, multiple mobile phones, laptops and USB storage drives, as well as bank cards and financial documents. No assembled explosive devices or firearms were recovered.
The suspect was escorted to court under heavy security measures to face both felony and misdemeanor charges. Appearing before the prosecutor and the examining magistrate without legal representation, he was granted a deadline until Thursday, June 11 to formalize his statement.

According to judicial authorities, the 37-year-old is being prosecuted for:

- Forming and joining a terrorist organization
- Receiving specialized training in the manufacturing and usage of explosives for the purpose of carrying out terrorist acts
- Traveling abroad to attend training related to committing terrorist acts
- Providing criminal support for terrorist purposes

Greek authorities are now working to determine the extent of the suspect's connections and whether he is tied to broader cells operating across other European countries.

The Terrorist Threat to the 2026 World Cup

Source: https://www.csis.org/analysis/terrorist-threat-2026-world-cup

May 27 – The 2026 World Cup will be the largest sporting event ever held—and a magnet for terrorists of all stripes. Major sporting events have long attracted a range of foreign terrorist groups and domestic extremists looking to bring their grievances to the fore or simply sow death and destruction. The most likely danger to the 2026 World Cup comes from a domestic lone actor or small group striking soft targets around the matches: fan zones, transit corridors, hotel and restaurant districts, and the queues outside stadium gates. The threats facing the tournament are real and diffuse, but so are the countermeasures arrayed against them.
In this summer's World Cup tournament, 48 teams will play 104 matches across 16 host cities over 39 days, with the United States hosting 78 games and Canada and Mexico 13 each. For millions of spectators attending the games and billions of fans watching around the world,

this is a nail-biting saga of triumph and loss playing out on a global stage.

That stage draws terrorists. Major sporting events have long attracted jihadists, ethnonationalist chauvinists, malign states, and a range of domestic extremists looking to exploit global attention to advance a cause, force their grievances onto the world's agenda, or simply sow death and destruction.

For counterterrorism officials with experience securing large-scale, single-day, and single-location events, protecting the World Cup poses a particularly difficult challenge. Protection for the World Cup must stretch out across the country—even the continent—and be sustained over many weeks. In addition, potential targets are numerous and varied. Although police and security officers can control access to key venues (e.g., searching match attendees before they enter the stadium), there will be crowds everywhere: gathering in front of the stadium to queue for security, riding in public transportation to and from the game, and coming together with their fellow fans in and around hotels, bars, and restaurants. Security everywhere is impossible, and that reality creates many potential soft targets.

Security officials are aware of these dangers and have been working aggressively to mitigate them. In the United States, attacks on sporting mega-events are exceedingly rare. Terrorist groups and radicalized individuals have many weaknesses and vulnerabilities that can—and have been—exploited by counterterrorism officials, and fans can attend the World Cup confident that those officials have worked hard to ensure their safety.

This brief examines the terrorism threat to the 2026 World Cup. It first details the range of potential attackers, examining both foreign-based and domestic threats. Next, it details the types of attacks that are most likely to occur based on trends in terrorism data and the current global security environment. It then examines the various counterterrorism mitigation efforts that are already well underway to prepare for the tournament and concludes with what is at stake for the World Cup and other major sporting events that will follow.

Foreign-Based Threats

The international terrorist threat picture is diffuse. In 2026, no one foreign organization presents the kind of singular, overriding threat that al Qaeda did after 9/11 or the Islamic State, also known as ISIS, did at the height of its external operations in the 2010s. Although this is a welcome development, several categories of foreign actors remain who could see attacking the World Cup as useful for different reasons: (1) jihadist groups seeking attention and casualties, (2) hostile states seeking disruption or retaliation, (3) militants tied to overseas conflicts seeking to internationalize their grievances, and (4) criminal organizations, especially those in Mexico, seeking leverage over or revenge against their own governments.

History offers many warnings. The 1972 Munich Summer Olympics attack, in which Palestinian terrorists killed nine Israeli athletes and a German policeman after a multiday hostage standoff, was perhaps the most famous terrorist operation in history until 9/11.[1] With every major media outlet already in Munich to cover the games, the hostage-taking seized global attention and put the Palestinian cause on the map. Abu Daoud, one of the planners, observed, "If we can, we have to squeeze our cause in 500 million houses all over the world."[2]

Sporting events have remained targets ever since. Algerian jihadists plotted to bomb matches at the 1998 World Cup in France.[3] ISIS attacked the Stade de France during a France-Germany soccer match in 2015 and later plotted against the 2024 Summer Olympics in Paris.[4] Kurdish militants struck a Turkish stadium in 2016.[5] Hostile states have joined in: Russian military intelligence has targeted every Olympics in the past decade with cyber operations—with the notable exception of the 2022 Winter Olympics in Beijing.[6] Russia is also suspected of plotting physical sabotage or an attack targeting the 2024 Summer Olympics in Paris; in July 2024 a Russian national with reported ties to Russia's Federal Security Service and Main Intelligence Directorate was arrested in Paris.[7]

Most of the ideologies behind past attacks continue to pose an active threat. The most active state sponsor of terrorism, Iran, may seek revenge for the U.S. and Israeli killing of more than 250 Iranian leaders. Iran could also strike to demonstrate that the United States, Israel, or their allies will pay a price for the war, thus trying to increase deterrence against future actions.[8] On May 15, the Department of Justice announced the arrest of Mohammad Baqer Saad Dawood al-Saadi, a senior member of Kataib Hezbollah, an Iraqi group with close ties to Iran. Saadi planned to target synagogues and Jewish centers in Arizona, Los Angeles, and New York.[9] It is easy to imagine similar attacks targeting the World Cup. The dispute over Iran's World Cup presence reflects this concern: The International Federation of Association Football (FIFA) insists Iran must participate, while the Trump administration has warned that trainers and journalists tied to the regime's security services will not be admitted.[10]

Iran is not the only state-level concern. Russia has orchestrated sabotage and arson operations across Europe in recent years, and an event on U.S. soil would offer similar opportunities to disrupt festivities and embarrass Washington.[11] Mexican cartels, newly designated as foreign terrorist organizations by the United States, have their own incentives after sustained U.S. and Mexican pressure on their leaderships. In February, for example, Mexican authorities killed Nemesio Rubén Oseguera Cervantes ("El Mencho"), the leader of the Jalisco New Generation Cartel, leading parts of

Mexico to erupt in retaliatory violence.[12] The World Cup's southern matches put fans and infrastructure within their easy operational reach.

The jihadist threat from foreign groups, though degraded in recent years, remains. Islamic State Khorasan Province (ISKP), the Islamic State's Afghanistan-based affiliate, remains the most externally focused branch, having attempted attacks in Europe as recently as 2024.[13] Al Qaeda in the Arabian Peninsula (AQAP) helped advise the attacker in the 2019 shooting at Naval Air Station Pensacola.[14] And the Somalia-based al Shabaab, the only African group known to have plotted a mass-casualty attack against the U.S. homeland, planned a 9/11-style plot disrupted in 2019.[15]

The international character of the tournament compounds the security problem. As the head of World Cup security put it, "The World Cup is the world stage, and it is a microcosm of everything that's happening in the world. . . . Those 48 teams don't check their politics at the door. They don't leave their issues at home, nor do their fans."[16] Colombia, Ecuador, Iraq, and other competing states face active violence or insurgencies at home, and those conflicts can travel with teams or surface within U.S.-based diasporas.

U.S. Domestic Threats

The lone actor—typically radicalized online, operating with little or no organizational direction and using readily accessible weapons against soft targets—has been the dominant domestic terrorism threat in the post-9/11 era in the United States.[17] Domestic terrorist movements in the United States lack the centralized leadership, training infrastructure, and funding networks that enable foreign groups to coordinate complex operations. As a result, within the United States, the threat from any given attack is shaped overwhelmingly by the intent and competence of the individual (or small group) involved, not by any organization's capability. The deadliest jihadist attack on U.S. soil since 2016, the Bourbon Street car-ramming on New Year's Day 2025—in which a U.S.-born Army veteran inspired by Islamic State propaganda killed 14 people—involved no foreign support.[18]

CSIS data on U.S. terrorist incidents over the past three decades reveals that the grievances motivating attackers are highly diverse, with the dominant ideologies varying over time.[19] For example, while antiabortion violence dominated U.S. terrorism in the 1990s, it has since receded. Jihadist attacks peaked in the 2010s, but have declined since the territorial defeat of the Islamic State in 2019, though such attacks remain disproportionately lethal when they do occur.[20] White supremacist violence has been a persistent feature for decades, producing some of the deadliest mass-casualty attacks of the past 10 years.[21] Anti-government and partisan extremism (violence against a person's political opponents, including high-profile figures) have surged more recently.[22] Other motivations, such as anti-LGBTQ+, anti-Muslim, and anti-Semitic violence, also appear with regularity. In addition, attackers are increasingly blending grievances that defy easy ideological categorization, further complicating analyses. For example, Patrick Crusius, who killed 23 at an El Paso Walmart in 2019, and Payton Gendron, who killed 10 at a Buffalo supermarket in 2022, each justified their attacks in manifestos fusing white supremacist replacement theory with arguments about immigration causing environmental degradation.[23]

Past attacks on sporting events and other large public gatherings in the United States have come from across the ideological spectrum, a diversity that is itself a warning: The next

threat could emerge from a broad range of causes. The cases below span both direct attacks on sporting events and attacks on events that had the kinds of crowds and festivities that the World Cup will draw across its host cities:

- In 1996, Eric Rudolph detonated a backpack pipe bomb in Atlanta's Centennial Olympic Park during the Summer Games, killing one and wounding more than 100. Rudolph was an antiabortion extremist seeking, in his words, "to confound, anger and embarrass the Washington government in the eyes of the word for its abominable sanctioning of abortion on demand."[24]
- In 2013, Tamerlan and Dzhokhar Tsarnaev—brothers self-radicalized in part through jihadist propaganda—detonated two pressure-cooker bombs near the finish line of the Boston Marathon, killing three and wounding more than 260. The plot was inspired, but not directed, by foreign terrorists.[25]
- In 2019, Santino Legan opened fire at the Gilroy Garlic Festival in California with a semiautomatic rifle, killing three before being shot by police. He had posted white supremacist content online days before the attack.[26]
- In 2023, Tibet Ergul and Chance Brannon were arrested for plotting a remotely detonated explosives attack at Dodger Stadium during an LGBTQ+ Pride Night.[27]
- In 2024, Marvin Jalo, a 17-year-old who claimed support from individuals he believed to be Islamic State sympathizers, was arrested for plotting to bomb the Phoenix Pride Festival with explosives strapped to drones.[28]
- Also in 2024, Mark Adams Prieto was arrested for plotting a mass shooting at a rap concert at Atlanta's State Farm Arena. He selected the venue specifically because, in his telling, the concert would draw many Black attendees, and the attack could help spark a race war.[29]

When Eric Rudolph bombed the 1996 Atlanta Olympics, antiabortion violence was the most common form of terrorism in the United States. In 2026, there are several widespread grievances which could prove relevant to the World Cup.

Anti-government violence surged in 2025, much of it tied to immigration enforcement by police and Immigration and Customs Enforcement officials—a grievance that the visible deployment of armed state, local, and federal personnel around tournament venues could easily channel toward World Cup targets.[30] Partisan extremism has climbed steadily since 2016 and shows no signs of abating.[31] The risk of political violence is compounded by FIFA's visible alignment with the Trump administration: FIFA's President Gianni Infantino's frequent White House appearances alongside the president and FIFA's creation of a "peace prize" awarded to Trump make it plausible that some attackers will perceive the tournament as a Trump-branded target.[32]

Conflicts in the Middle East involving the United States and Israel continue to spill into U.S.-based violence. Recent cases include the May 2025 shooting of two Israeli embassy staff in Washington by Elias Rodriguez who declared, "I did it for Palestine, I did it for Gaza" after his arrest; Mohamed Soliman's June 2025 firebombing of a Boulder march for Israeli hostages, which killed one and wounded seven; Cody Balmer's April 2025 arson at Pennsylvania Governor Josh Shapiro's residence, which Balmer told police was retaliation for Shapiro's stance on Gaza; Ndiaga Diagne's March 2026 mass shooting at an Austin bar, carried out the day after the United States and Israel killed Iranian Supreme Leader Ali Khamenei and committed by a gunman wearing Iranian-flag clothing and the words "Property of Allah"; and Ayman Ghazali's March 2026 car-ramming and shooting at a Detroit-area synagogue, executed a week after Ghazali lost relatives in an Israeli airstrike on Lebanon and framed by the attacker himself as vengeance.[33] The U.S. and Israeli war with Iran, with on-again, off-again hostilities continuing as the World Cup approaches, will only deepen the grievances driving this violence. Iran's qualification for the tournament gives those grievances a recurring focal point on U.S. soil.

White supremacists may also see opportunity in the tournament's demographic profile. Prieto, for example, selected an Atlanta concert specifically because he expected a large Black audience. White supremacists more broadly have repeatedly targeted venues that concentrate non-white crowds. A tournament drawing millions of fans from all over the world to 16 host cities offers that target environment at unprecedented scale.

Anti-LGBTQ+ extremists may also see the tournament as a target. Recent years have seen Pride events recurringly targeted, including the 2023 Dodger Stadium plot during Pride Night and the 2024 plot against the Phoenix Pride Festival. The 2026 World Cup schedule creates a particularly visible case in Seattle, where a game between Egypt and Iran is scheduled during the city's PrideFest weekend and has been dubbed by tournament organizers as the "Pride Match." National federations from both countries have formally protested, though Seattle's organizing committee has said the celebrations will go forward as planned.[34] A high-visibility Pride-themed match between two teams from countries that criminalize or prosecute homosexuality, along with the surrounding celebrations and gatherings, is the kind of event anti-LGBTQ+ extremists may seek to attack.

Types of Attacks and Target Vulnerabilities

The most likely terrorist threat to the World Cup is the kind that has dominated U.S. terrorism for the past decade: a lone actor or small

cell using firearms, vehicles, or improvised explosives against a soft target. Less likely is a sophisticated, foreign-conducted or foreign-directed operation of the kind ISIS executed on the Stade de France in 2015. The geographic, intelligence, and operational barriers that have prevented foreign groups from striking inside the United States in the decades since 9/11 remain intact. But vigilance remains necessary. A tournament drawing the world's attention for 39 days creates exactly the kind of high-payoff target that justifies the operational risk for groups such as AQAP, ISKP, and al Shabaab, or a hostile state such as Iran, to act. The likelihood of a foreign-directed attack remains low, but not low enough that security officials can write it off—indeed, it is their vigilance that makes such attacks less likely.

The tournament's structure shapes which targets are at greatest risk. Stadiums themselves will be among the hardest targets in North America during the matches. In the United States, the final at MetLife Stadium has been designated a National Special Security Event—the highest federal security tier, triggering a centralized Secret Service–led operation with hardened perimeters, magnetometer screening, FAA-enforced flight restrictions, counter-drone systems, and continuous counterterrorism monitoring across federal, state, and local agencies. The remaining 77 U.S. matches have been assigned Special Event Assessment Rating 1 or 2 designations, meaning they are treated as nationally significant security events requiring extensive intelligence support, protective planning, emergency preparedness, and security integration across federal, state, and local agencies.[35] Everything surrounding the stadium, however, is at greater risk: the crowds queuing for security, the fan zones and watch parties drawing spectators with fewer security measures, the transit corridors moving fans to and from venues, the hotel and bar districts where supporters cluster, and the high-profile individuals—players, coaches, dignitaries, and others—who move between them. Each presents a different kind of opportunity for a determined attacker.

Stadium Perimeters and Ingress Points: The points of greatest vulnerability at a stadium are the queues and chokepoints outside, not the fields or the seats inside. Crowds gathering to pass through magnetometers concentrate hundreds, even thousands, of people in unscreened space—a target location that has drawn attackers before. The 2015 Stade de France attack, in which ISIS bombers detonated suicide vests at stadium entrances during a France-Germany match, is the clearest analogue. The Boston Marathon bombing followed similar logic, with the attackers striking a soft point at an event with a large police presence. A vehicle ramming, an improvised explosive device (IED), and a firearms attack at a stadium ingress point are all among the most plausible high-casualty scenarios at the tournament.

Fan Zones and Watch Parties: FIFA's fan zones—large public viewing areas with food, entertainment, and screens—will draw crowds across host cities, often with looser security than the stadiums themselves. This kind of high-density, lightly secured event space could appeal to attackers. In addition, fan zones are likely to concentrate fans of particular teams in one location, increasing the risk of terrorism in the name of a grievance directed at that particular community. Some host cities have pulled back on these gatherings: San Francisco and New Jersey have canceled planned outdoor fan fests, reportedly in large part because of security costs.[36]

Transit, Hotels, and Gathering Areas: Crowds traveling to and from matches will fill metro lines, train stations, and downtown corridors. Hotels hosting teams or large fan contingents, and the bars and restaurants where supporters concentrate, present a wide array of targets with varying levels of security. The March 2026 pro-Iran Austin bar shooting illustrates the basic profile: a lone attacker, an easily accessible weapon, and an open location.[37] The geographic distribution of fan activity across each host city will create dozens of such locations during every matchday.

High-Profile Individual Targets: Players, coaches, FIFA officials, visiting heads of state, and other dignitaries present a separate threat profile. The multiple assassination attempts against President Trump and other leading U.S. officials, both Republican and Democrat, in recent years illustrate the risk of determined attackers striking at semipublic events, even with security measures. Still, the heavy protective details that surround many of these figures—close security personnel, advance work, hardened transit, and controlled access—make them among the least likely targets to be successfully struck during the tournament.

Across all of these varied target sets, a secondary risk compounds the first. Even an attack that kills no or few victims can trigger panic and a stampede in densely packed spaces, killing or injuring additional people. The 2017 Manchester Arena bombing illustrated this dynamic: The suicide bomb in the venue's foyer killed 22 directly, and witnesses described concertgoers being knocked down and trampled as the crowd fled the arena, though no fatalities from the crush itself were reported.[38] In Iraq in 2005, unfounded rumors of a suicide bomber on a crowded bridge prompted a stampede in which almost 1,000 people died.[39]

Firearms have caused the most fatalities in U.S. terrorism in the decades since 9/11 by far, vehicles are the second most popular mass-casualty tool against public crowds, and IEDs, while difficult to build and rarely used successfully in the United States, remain attractive to attackers seeking dramatic, visual destruction. Drones are increasingly a wild card. States such as Russia and Iran and sophisticated nonstate actors including Hezbollah, Kataib Hezbollah, and ISIS use them in their wars overseas. A handful of lone attackers in the United States in recent years from across the ideological spectrum have

attempted to use them to deliver explosives, though none have succeeded and the airspace in cities is increasingly secured against the drone threat.[40]

Mitigating Factors

Despite these risks, several factors lessen the danger of terrorism at the World Cup.

When it comes to foreign groups, the post-9/11 counterterrorism architecture has proven effective at reducing the danger. Global intelligence cooperation, military pressure on safe havens, financial disruption, and partnerships with foreign governments have weakened once-formidable groups, and, as a result, jihadist organizations are shadows of their former selves. Attacks conducted or directed by foreign groups on U.S. soil have been rare since 9/11, and when domestic actors have reached out to foreign operatives for guidance, those contacts have more often led to arrests than to attacks.

Foreign states must worry about escalation, making them more cautious about stirring up trouble in the United States. Although the U.S. and Israeli war with Iran poses an existential threat to the Iranian regime, the United States has only used part of its power so far. Notably, it has not put troops on the ground in Iran. In addition, domestic U.S. support for the war is low, and Iran is well aware of this.[41] A terrorist attack on U.S. soil might rally Americans and lead to escalation against Iran, making it harder for Iran to achieve a favorable war settlement. Finally, the devastation of Iran's leadership and the clear penetration by U.S. and Israeli intelligence probably have hindered Iran's ability to use terrorism abroad—which may be why Tehran has turned to Kataib Hezbollah, not its own operatives or its longstanding partner the Lebanese Hezbollah, to plot attacks. Russia faces a similar logic. Putin has already extracted much of what he wanted from the Trump administration related to the war in Ukraine, and an attack inside the United States risks pushing Washington back toward Kyiv. Though these factors do not eliminate the threat from state actors, they do narrow it.

Domestic terrorists, the most likely source of an attack, are constrained both by their own limited competence as well as broader counterterrorism measures. Radicalized individuals often post their intentions on social media, confide in unreliable acquaintances, or otherwise give themselves away. Many extremists also have regular encounters with law enforcement on unrelated grounds—narcotics, domestic abuse, firearms violations, and other offenses—and frequently trade information for leniency. If law enforcement maintains broad threat awareness, many plots can be disrupted before they mature. Social media and other technology companies can also play an important role, as many would-be terrorists boast about the operations they intend to conduct or otherwise use the internet for their plans. Equally important, most domestic attackers have little to no operational training. They are therefore more likely to make mistakes, get caught in the planning phase, or execute attacks that fail or kill fewer people than intended. Most of the deadliest terrorist attacks in modern history have been carried out by trained operatives—and the absence of that capability is a meaningful constraint on what most lone actors can achieve. The Bourbon Street attack is a reminder that the constraint is not absolute, but it remains a common limitation.

Most importantly, security officials in the United States, Canada, and Mexico are aware of the risks and are trying to guard against a wide array of threats. FIFA has stood up a dedicated trilateral planning structure, with a foundational "Safety and Security Concept" defining 18 common areas of focus and strategic objectives that every host city has agreed to deliver. Decisionmaking is dispersed to the venues, with the FIFA Tournament Operations Center reserving authority for issues that cross host cities. An International Police Cooperation Center outside Washington consolidates intelligence from the National Football Information Point officers of participating countries, channeling it through fusion centers, the FBI, the Department of Homeland Security (DHS), Royal Canadian Mounted Police Intelligence, and Mexico's Center for National Intelligence. Counter-drone capabilities—newly extended to state and local law enforcement under the 2025 Safer Skies Act—are being coordinated by a dedicated FIFA airspace security team across all three host nations.[42] FIFA has also committed $625 million to additional security funding for U.S. host cities, routed through FEMA.[43]

In April, the National Counterterrorism Center (NCTC), FBI, and DHS jointly published a series of unclassified guidance documents specifically about fan-zone security, hospitality and nightlife venue threats, rail infrastructure protection, and the safeguarding of high-profile figures at public events. The Office of the Director of National Intelligence has stood up an Intelligence and Threat Working Group with the FBI and DHS focused on the tournament, and NCTC will provide direct intelligence support to host cities before and during play.[44]

However, security preparation for the World Cup has also faced setbacks. The 76-day DHS funding shutdown in spring 2026 delayed host-city grant funding. The Cybersecurity and Infrastructure Security Agency—which coordinates protection of critical infrastructure including transit, communications, and event networks—lost roughly a third of its staff, and the Transportation Security Administration, slated to screen fans at stadium entrances in addition to its airport duties, lost nearly 8 percent of its workforce during the shutdown.[45]

The Paris Olympics in 2024 demonstrated what comprehensive prevention architecture can accomplish: French authorities disrupted three major terrorist plots before the games, conducted more than 900 administrative searches, placed

over 700 individuals under enhanced monitoring, and intercepted 90 unauthorized drones—and the games concluded without a major terrorist incident.[46] Across the World Cup's 16 host cities, similar mobilization is underway.

The Stakes

The measure of a successful World Cup, from a security standpoint, will be invisible: an absence of incidents and a tournament remembered for exciting games and stunning athleticism. The World Cup exists to bring billions of people together in a shared experience of sport and culture. Terrorism, whatever its underlying cause, depends on the opposite—on reshaping how people gather and what they feel safe doing. A tournament that feels celebratory rather than fearful is its own form of victory.

What is built in the next year will outlast the tournament itself. The 2028 Summer Olympics in Los Angeles and the 2034 Winter Games in Salt Lake City will face many of the same threats, and the architecture being stood up now will be the foundation for handling them. The threats facing the World Cup tournament are real and diffuse. But so are the countermeasures arrayed against them. If all goes as planned, the story of the summer of 2026 will be who lifts the trophy at the final match.

Daniel Byman is the director of the Warfare, Irregular Threats, and Terrorism (WITT) Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.
Riley McCabe is an associate fellow with the WITT Program at CSIS.

EDITOR'S COMMENT: Given the nexus between terrorism and organized crime, I wonder about the selection criteria for Mexico.

Over the last five years (approximately 2021–2026), organized crime in Mexico has remained heavily involved in drug trafficking while significantly expanding into a wide range of other criminal activities. Major criminal organizations, including the Sinaloa Cartel and the Jalisco New Generation Cartel, have evolved into diversified criminal enterprises that generate income from both traditional illicit markets and broader forms of organized crime.

Drug production and trafficking continue to be the primary source of revenue. Criminal groups manufacture and export fentanyl and methamphetamine, traffic cocaine and heroin, operate synthetic-drug laboratories, and manage international smuggling networks, particularly into the United States. During this period, there has been a notable shift from plant-based drugs toward synthetic drugs, especially fentanyl and methamphetamine.

At the same time, extortion has become one of the fastest-growing criminal activities. Organized crime groups demand "protection payments" from businesses, farmers, transport companies, market vendors, and restaurant owners, while also carrying out telephone and online extortion schemes. In many regions, these protection rackets directly affect local economies and daily life.

Kidnapping and forced disappearances remain significant concerns. Criminal organizations engage in ransom kidnappings, express kidnappings for quick payments, forced recruitment, and disappearances linked to territorial disputes and criminal operations. Human smuggling and human trafficking have also expanded, with criminal groups profiting from migrant flows by charging fees for passage through cartel-controlled territories and operating networks involved in labor and sexual exploitation.

Organized crime has increasingly diversified into economic crimes such as fuel theft, known locally as "huachicol." This involves illegally tapping pipelines, stealing fuel shipments, and selling stolen fuel through black-market networks. Criminal groups have also entered illegal mining, illegal logging, resource theft, and control of water resources, particularly in regions with limited government presence.

Another major trend has been the growing influence of organized crime over legal sectors of the economy. Criminal groups extort agricultural producers, especially those involved in high-value crops such as avocados and limes, control transportation routes and wholesale markets, and sometimes establish monopolistic control over local businesses and industries.

Political corruption and violence continue to play a central role in organized crime activities. Criminal organizations seek influence through bribery, intimidation of public officials, infiltration of local governments, manipulation of public contracts, and attacks on politicians, candidates, and community leaders. Research has documented a rise in political assassinations linked to organized crime efforts to influence local governments and secure control over territory and economic resources.

Violence associated with territorial disputes remains widespread. Criminal groups fight for control of drug-trafficking routes, border crossings, ports, highways, and strategic cities. These conflicts have contributed to exceptionally high levels of homicide and other violent crimes. Mexico recorded more than 30,000 intentional homicides in 2024 alone, equivalent to roughly 82 murders per day, and security analysts estimate that about two-thirds of homicides are linked to organized crime.

The human cost has been severe. More than 115,000 people were officially listed as missing by 2024, and the total number of recorded disappearances has since approached 130,000. Many of these cases are believed to be connected to criminal organizations, which frequently use forced disappearances as a tactic of intimidation, punishment, recruitment, or concealment of murders. Authorities and search groups have uncovered thousands of clandestine graves across the country.
Overall, the most significant development in Mexico's organized crime landscape during the last five years has been the diversification of criminal activities. While drug trafficking remains the foundation of cartel revenues, organized crime groups increasingly rely on extortion, fuel theft, migrant smuggling, human trafficking, illegal resource extraction, agricultural rackets, corruption, and territorial control. During this period, organized-crime-related violence has contributed to well over 150,000 homicides nationwide, tens of thousands of kidnappings and disappearances, and widespread economic and social disruption across many regions of the country.
June 11: Five police officers were killed, and an equal number of their colleagues were injured in an armed attack in the state of Michoacan, in western Mexico, an area ravaged by drug cartels, local authorities announced, while the World Cup is expected to start in the country tonight.

Thai court sentences two men to death over 2015 Bangkok shrine bombing

Source: https://www.bbc.com/news/articles/ckg8v51g9lno

June 11 – A court in Thailand has found two men guilty of carrying out the country's worst-ever terrorist attack and sentenced them to death. The two men, both from China's Uyghur minority, were convicted of planning and detonating a powerful bomb on the evening of 17 August 2015, next to a shrine in central Bangkok that is popular with foreign tourists. Twenty people were killed and more than 120 were injured.
However, flaws in the police investigation, and in the ten year-long trial of the two men, who both pleaded not guilty, have left questions hanging over this verdict. The bomb exploded a short distance from the BBC bureau in Bangkok, and I was there within a couple of minutes. The blast had ripped through people praying at the Erawan shrine, and knocked over motorbike riders waiting at the nearby intersection, setting some of them on fire. Paramedics and ambulances were quickly on the scene and began treating the injured, or laying sheets over the

dead. I watched them helping a man, whose wife lay lifeless next to him. His injuries were not life-threatening, so they gently asked him to wait, getting him to hold his wife's hand, while they tended to other casualties.

It was loud, chaotic, and profoundly shocking. I had seen plenty of political violence in Bangkok, but a bomb attack of this size was unprecedented. Who could have carried it out, and why? From the start the official investigation was less than reassuring. Worried about the impact on the all-important tourist industry, the government ordered the scene of the attack to be cleaned up as quickly as possible. The shrine was reopened two days later, the crater left by the bomb cemented over. Many of the security cameras in the area were found to be not working, but some grainy video did show a man with long hair and thick glasses leaving a backpack under a bench and walking quickly away. His trail was lost, but the police showed video of another man in a different location kicking what turned out to be a second bomb into a canal, where it exploded harmlessly. They said they were looking for several suspects, but insisted the bomb was not an act of terrorism.

Within two weeks of the attack they had arrested the two men who have now been convicted.

Bilal Mohammad was found hiding in a house on the outskirts of Bangkok where the authorities also discovered chemicals suitable for making bombs. He had a forged Turkish passport, under the name Adem Karadag. Yusufu Mierali was apprehended in Cambodia, and handed over to Thailand.

Both men were identified as Uyghurs, but initially the Thai police said neither was the person who planted the bomb. Later they charged Bilal Mohammad with the crime, although he bore little resemblance to the man in the video. Arrest warrants were also issued for 13 other people, some of whom had already left the country.

Unsurprisingly, people began to link the bomb to the controversial Thai decision the month before to forcibly repatriate 109 Uyghur men to China, which provoked angry protests by Uyghur sympathisers in countries like Turkey. The shrine was well known as especially popular with Chinese visitors. It looked like an act of retribution.

But the military government refused to accept this possibility. At one point they suggested it might be disgruntled opponents of the military junta which had seized power the year before. Later they insisted that it was just human traffickers angry at the government's efforts to shut down their activities.

In a bizarre twist the police offered a reward of $80,000 to anyone who led them to the culprits – then awarded it to themselves once they had their first two suspects in custody, despite acknowledging that many more suspects were still at large. Case closed, they said. Both suspects were kept in military custody, and complained that they had been tortured into making confessions. They withdrew these once the trial, in a military court, began.

Bilal Mohammad appeared to be extremely distressed, shouting that he was being mistreated. He testified that he had been waiting at the house where he was apprehended for a smuggler to move him to Malaysia, from where he wanted to fly to Turkey, a well-established route used by Uyghur asylum-seekers.

Then the delays began. Usually, it was because the Thai authorities said they could not find a Uyghur-speaking translator. The defendants rejected those offered by the Chinese embassy. The delays went on and on, for more than ten years.

The International Commission of Jurists is one of several human rights groups that have criticised the procedures and extraordinary duration of the trial, arguing that it was so problematic the two suspects should have been released.

"The investigation, prosecution, and trial of Bilal Mohammed and Yusufu Mieraili have been rife with human rights violations and have exposed some of the systemic deficiencies of Thailand's criminal justice system."

However the judges ruled that there was sufficient evidence to justify convicting them, in particular, records of phone calls submitted by the police that show both men near the scene of the crime at the time of the bombing, and communicating with each other.

The lawyer for the two men has said they will appeal against the verdict.

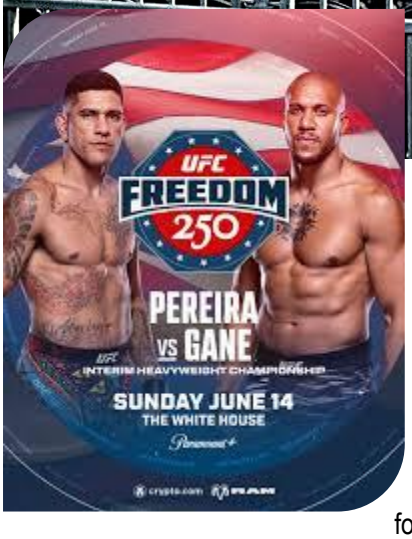
FBI says it foiled terrorist attack on White House during UFC Freedom 250

By Mark Puleo | Senior Editor on the Daily Desk at The Athletic
Source: https://www.nytimes.com/athletic/7365717/2026/06/16/ufc-white-house-terrorist-attack-foiled-fbi-secret-service/

June 16 – FBI director Kash Patel said Tuesday his agency disrupted an alleged terrorist attack threatening Sunday night's UFC America 250 event at the White House.

"On June 10, FBI and our law enforcement partners became aware of a potential threat to the UFC America 250 event in Washington, D.C. involving individuals outside of the National Capital Region — and thanks to the rapid action of this FBI, our partners, and the Department of Justice in a multi-state operation, multiple individuals are now in custody and allegedly

planned attacks were stopped cold," Patel said in a Tuesday post on X. News of the FBI foiling the attack plot was first reported by Fox News, which also reported that five individuals were in custody as of Monday and 23 people were identified by investigators to be part of the planning. Patel told Fox that the alleged group planned to use drones to hit buildings surrounding the South Lawn with explosives and then target attendees as they fled while another group of attackers stormed the White House. The Associated Press also reported five men were arrested. Charges are expected to be unsealed later Tuesday.



The FBI said it does not have any additional information to share beyond Patel's statement and did not respond to a request for confirmation of the details Fox reported.

The UFC did not respond to a request for comment and its CEO, Dana White, never mentioned the alleged plot in front of media during the lead-up to Sunday's event.

Secret Service Director Sean Curran addressed the situation Tuesday, saying the Secret Service worked closely with the FBI.

"In the days leading up to this weekend, our special agents, mission support personnel, and technical security teams worked around the clock to identify those responsible and hold them accountable," Curran said. "Equally important to our protective mission is ensuring accountability through the justice system." The Secret Service did not respond to a request for comment or a clarification on how many days in advance their agency was aware of the plot.

Federal court filings indicated UFC was prepared for a crowd of up to 120,000 to attend its events around Washington leading up to Sunday's fights and, during the broadcast, Paramount + reported that about 85,000 were watching the fights from the Ellipse.

For media, security for entry to the Ellipse consisted of walking through a metal detector and scanning belongings through an X-ray machine, and later having their credentials scanned at another entry point.

Earlier in the week, media was given a tour of the octagon setup at the White House. Prior to entering the White House grounds, media was held outside the Eisenhower Executive Office Building while Secret Service members searched their bags. During the tour, a Secret Service officer told a reporter to stop looking over a barricade at the surrounding construction, saying, "That's not what we're here for."

Fox reported that some of the alleged attackers planned to travel to Fredericksburg, Va., on June 12 or 13 to prepare for the attack. The news conference for Freedom 250 was held June 12 outside the Lincoln Memorial, and on June 13, a fan fest was held at the Ellipse preceding the weigh-ins.
Vice President J.D. Vance appeared on "Fox & Friends" shortly after Patel's post and said, "We got to tell everybody to tone it down."

John Kassimatis, the Greek-American Hero of September 11, Dies at 73

By Tasos Kokkinidis
Source: https://greekreporter.com/2026/06/16/ohn-kassimatis-greek-american-hero-september-11-dies/

Kassimatis dragged an unconscious, bleeding woman to an ambulance just moments before the North Tower collapsed. Public Domain and New York Port Authority

June 16 – John V. Kassimatis, a Greek-American icon of bravery and dedication during the September 11 terrorist attacks, has died at the age of 73. A veteran of the Port Authority Police Department of New York and New Jersey, Kassimatis rose to the rank of Inspector over his decades-long career. He was also a prominent figure in the Greek Orthodox community, serving as an Archon Deputatos of the Ecumenical Patriarchate.
On 9/11, while stationed at the Manhattan Bus Terminal, Kassimatis rushed to the World Trade Center immediately after the attacks began. En route, he witnessed the second plane strike the South Tower, arriving to a scene of catastrophic destruction.

Kassimatis saves injured, escapes death on 9/11

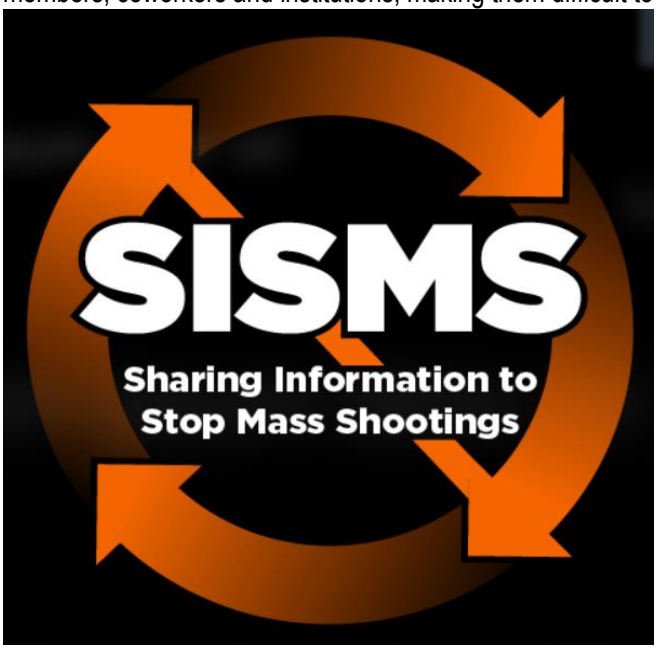
Inside the North Tower's Galleria level, he and fellow officers managed a chaotic evacuation, guiding terrified, bottlenecked crowds to safety. When the South Tower collapsed, the impact threw Kassimatis and buried him in pitch darkness. Believing he wouldn't survive, he joined hands with other officers and Secret Service agents to form a human chain, eventually escaping to West Street using a flashlight. Once outside, despite his own leg and shoulder injuries, Kassimatis dragged an unconscious, bleeding woman to an ambulance just moments before the North

Tower collapsed. He and other rescuers survived the second collapse by sheltering within an NYPD vehicle.
Kassimatis continued working through the day to set up an emergency command post, later dedicating his official report to the 37 Port Authority colleagues who perished.
In the tragedy's aftermath, he collaborated with chaplain Fr. Alex Karloutsos to bring former Archbishop Demetrios back to New York for spiritual guidance, and he actively assisted in retrieving sacred relics from the ruined St. Nicholas Greek Orthodox Church.
Visitation will take place on Wednesday, June 17, from 4:00 p.m. to 8:00 p.m. at St. Paul's Cathedral in Hempstead, NY. The funeral service will be held on Friday, June 19, at 9:30 a.m. in the same cathedral.
John Kassimatis is survived by his wife, Sandy, his children Maria and Vasilios, his grandchildren, and many relatives, friends, and colleagues who knew him as both a hero of September 11 and a man who dedicated his life to serving others.

Most Mass Shooters Show Warning Signs Before Attacks: Study

By Amanda Watford
Source: https://www.homelandsecuritynewswire.com/dr20260616-most-mass-shooters-show-warning-signs-before-attacks-study

June 16 – People who carry out mass public shootings often display observable warning signs long before an attack, but those signals are frequently fragmented across friends, family members, coworkers and institutions, making them difficult to



piece together, according to a new study (SISMS) from the Regional Gun Violence Research Consortium at the Rockefeller Institute of Government, a nonpartisan public policy think tank.
The report, which analyzed a sample of **171 mass public shootings in the United States between 1999 and 2024**, such as those at workplaces, schools or shopping malls, found that these attacks are rarely sudden or unpredictable. Instead, researchers describe them as the result of cumulative stressors, concerning behaviors and communications of intent that, if connected, could offer opportunities for earlier intervention.
An overwhelming majority of perpetrators, nearly 86%, communicated violent thoughts or intentions to at least one other person before carrying out an attack, a pattern researchers refer to as "leakage." These disclosures most often occurred through in-person conversations or text messages and were typically made to people within the perpetrator's immediate social circle, including friends, family members and coworkers.
On average, warning signs were spread across more than two different groups of observers, meaning no single person had a complete view of the escalating threat, according to the report.
The researchers also found that perpetrators tended to experience multiple overlapping stressors rather than a single triggering event. On average, people had five distinct stressors prior to an attack, including mental health challenges, job-related difficulties and family problems. Researchers also identified an average of 6.6 concerning behaviors per perpetrator, including suicidal ideation and other forms of emotional distress or aggression.
Planning often unfolded over an extended period. The report's authors found that perpetrators spent an average of nearly 10 months preparing for attacks, including researching locations and studying prior mass shootings.
Firearms were most often obtained through legal channels, with nearly 60% purchased from federally licensed dealers. About one-third of perpetrators had at least one factor that would have legally prohibited them from possessing a firearm, according to the report.
Researchers also found that nearly two-thirds of perpetrators had prior contact with law enforcement, underscoring what they describe as missed opportunities for intervention when warning signs appeared across different systems but were not fully connected.
"Warning signs are regularly present, observable, and known to people in the perpetrator's social network long before the first shot is fired," Jaclyn Schildkraut, the executive director of the consortium and lead author of the report, said in a news release. "By understanding how these indicators cluster and by building

robust pathways for everyday bystanders to report what they see, we can connect the dots and intervene before a crisis turns into a tragedy."

The report argues that improving communication between schools, law enforcement, mental health providers and community members could strengthen efforts to identify and respond to potential threats. It also highlights the need for clearer pathways for reporting concerning behavior and better systems for assessing risk when multiple warning signs emerge across different settings.

Alongside the findings, the consortium is developing an open-source database and training tools aimed at helping threat assessment professionals and community members recognize pre-attack behaviors and communication patterns.

Amanda Watford (formerly Hernández) covers criminal justice for Stateline (part of States Newsroom, the nation's largest state-focused nonprofit news organization, with reporting from every capital).

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

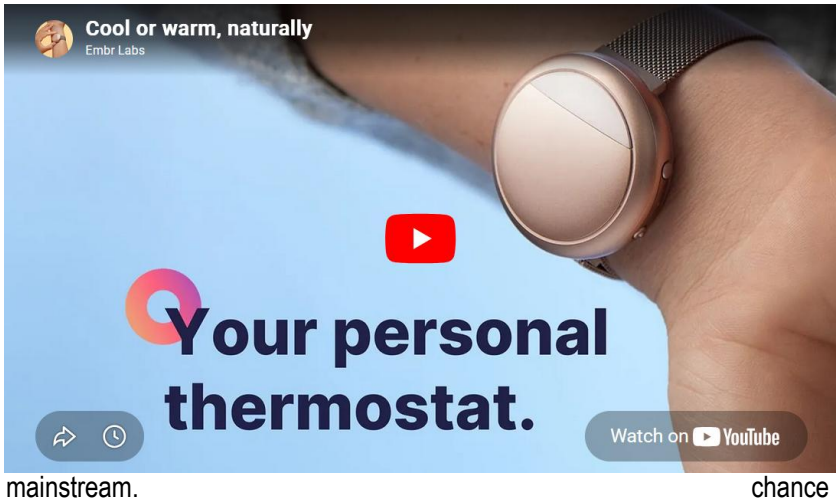
C²BRNE DIARY

CHEM NEWS

Sony's wearable 'air conditioner' gets an upgrade for a better fit and stronger cooling

Source: https://newatlas.com/wearables/sony-reon-pocket-pro-plus-wearable-air-conditioner-upgrade/

May 24 – Don't sweat it if you didn't know there's such a thing as a wearable air conditioner. It's not a miniature version of the real thing in your home, and only a couple of brands make this sort of thing, so they haven't yet gone properly mainstream.



One of those brands, though, is Sony. It launched the first of these Reon Pocket devices back in 2019, and it's now launched an updated version that's better in practically every way – except the name. The Reon Pocket Pro Plus applies the Peltier effect, in which cooling caused by an electric current flowing across the junction of two different conductors can cause heating or cooling. It's worn around your neck and sits between your shoulders; when placed against your skin where it can impact your circulatory system, this device can lower or raise your skin temperature by several degrees. It won't affect your core temperature.

The idea is it'll make things a bit more comfortable if you often face a crowded commute, an overly chilly AC in the office, or sultry weather while working outdoors. If you're prone to hot flashes, this might be worth a try too.

The first model was said to cool you down by as much as 23 °F (13 °C), or raise the temperature by 14 °F (8 °C). This new one's said to be far more effective, beating the last model from 2025 with an additional 3.6 °F (2 °C) cooling capability. It also features a revamped neckband that allows for a more secure fit for a stronger cooling effect, and the airflow exhaust that faces upwards is now easy to adjust behind high collars for optimal performance.

The Pro Plus manages 5.5 hours of cooling on its highest setting from a full two-hour charge; turning it down all the way allows it to run for a maximum of 34 hours. It also comes with an ambient temperature and humidity sensing tag that can go on your bag and inform the Pro Plus' automatic adjustments. You can control the device using buttons on it, or via a companion mobile app.

While it certainly sounds cool, I'd recommend trying this out for yourself before placing an order for one, as your perception of the effect may differ from the numbers you're reading. Back in 2018, I had a chance to try out the first Embr Wave wrist-worn personal climate control device developed by a team including MIT graduates, and it was underwhelming to say the least. Your mileage may vary, and it's possible Sony has made more headway in delivering on the promise of this type of gadget. The Reon Pocket Pro Plus is on sale in

some Asian markets including Singapore, where it's listed at S$349 (US$273). It's set to go on sale in the UK and Europe through Sony's online store and via other retailers – but it likely won't arrive stateside, so you'll need to get your hands on it some other way.

There's also a more recent version of the Embr Wave, which now features a smartwatch-like design and can be purchased outright or as a $20 monthly rental in the US. That might be more accessible for some, if you want to see what all the personal-cooling fuss is about.

Check out Sony's Reon Pocket Pro Plus on the company's Singapore site.

EDITOR'S COMMENT: Interesting! It might be useful to be tried while donning a Level-A PPE.

OPCW: Chemical materials and munitions linked to the ousted regime found in Syria

Source: https://sana.sy/en/politics/2319576/

May 26 – The Organisation for the Prohibition of Chemical Weapons (OPCW) announced on Tuesday that dozens of munitions, chemical materials and related equipment linked to the deposed regime had been found at several sites in Syria, as part of ongoing verification efforts conducted in coordination with the Syrian authorities.

Agence France-Presse quoted the organization as saying in a report that an OPCW team deployed earlier this month to verify the accuracy and completeness of declarations related to the ousted regime's chemical weapons stockpiles. The organization said search and assessment operations covered a number of priority sites in the northern coastal and central regions, with full support and facilitation from the relevant Syrian authorities.

The findings included aerial bombs, missiles, chemical materials and equipment linked to the deposed regime, in addition to thousands of pages of documents related to its chemical program. The materials are currently undergoing detailed technical analysis by OPCW experts, with a comprehensive report on the

findings to be issued once examination and assessment procedures are completed, according to the report.
Earlier on Tuesday, the Permanent Mission of the Syrian Arab Republic to the OPCW said that search and investigation operations carried out by Syria had identified sites linked to the chemical program of the ousted regime era. It added that aerial and surface-to-surface munitions similar to those used in attacks carried out by the deposed regime in 2013 and 2017 had been found, along with materials used in the production of sarin gas, mixing and storage equipment, and quantities of other substances that remain under analysis.

North Korea: New report sheds light on chemical weapons

By Julian Ryall
Source: https://www.dw.com/en/north-korea-new-report-sheds-light-on-chemical-weapons/a-77329770

May 28 – A new study shows the North Korean regime is investing heavily in chemical weapons capacity, with analysts warning they could be deployed by the regime if it faces an existential threat.

Kim Jong Un seen at a chemical research facility in 2017
Image: AP Photo/picture alliance

A new report released last week has revealed clues on North Korea's chemical weapons program by combining information on more than 30,000 patents and journal articles.
The report published on the 38 North website was based on research carried out under "Project Anthracite," a multi-year effort led by the Royal United Services Institute (RUSI) security think tank in London to use open source materials to produce a "networked overview" of North Korea's chemical weapons potential. The report points out that industrial facilities, universities and government-run research institutions have the equipment and access to adequate feedstocks to produce a number of chemical weapons agents. Although the report emphasizes that it does not prove production of chemical weapons in North Korea, it does add to the existing intelligence by "providing a feasibility baseline and identifies indicators worth monitoring."
"Taken together, the most striking insight from this analysis is not the presence of any single 'smoking gun,' but the convergence of multiple, discrete indicators that point towards embedded industrial capability," the report says.

'Little known' about North Korea's chemical weapons

That the assessment tallies convincingly with other reports and is a cause for concern among experts, especially as Pyongyang has already demonstrated a clear willingness to use a chemical

weapon. In 2017, agents assassinated Kim Jong Nam, the brother of North Korean dictator Kim Jong Un, with the VX nerve agent at Kuala Lumpur airport.

"It is absolutely clear that North Korea can and has made chemical weapons, with the use of VX in 2017 confirming that," said Margaret Kosal, director of graduate studies at Georgia Institute of Technology.

"Compared to other former and suspected current offensive chemical warfare programs, we don't know a lot about the DPRK's program," Kosal told DW, pointing out that similarly little is known about the regime's biological warfare and nuclear capabilities.

"But based on what can be inferred they have capabilities to produce large amounts of sulfur mustard — often incorrectly described as 'mustard gas' — and some amount of nerve agents," said Kosal, who advised the US administrations of presidents George W. Bush and Barack Obama on the threats posed by chemical weapons.

"They can probably produce large amounts of nerve agents like sarin. And some amount of VX."

"Most likely is to be used operationally to hinder South Korean soldiers, including along the North-South border," she said. "In the event of conflict, use against civilian centers like Seoul is likely planned."

As much as 5,000 tons of chemical weapons

North Korea is believed to have **stockpiles of between 2,500 and 5,000 tons of chemical weapons**. Dan Pinkston, a professor of international relations at the Seoul campus of Troy University, told DW the regime would have little compunction in using the weapons if it assessed its imminent collapse. "There is paranoia within the regime and the rationale there is that any kind of lethal capacity is for its own safety," said Pinkston, who authored a report for the International Crisis Group on the North's chemical and biological weapons programs in 2009.

Despite the horrors associated with chemical weapons, Pinkston believes that should conflict break out on the peninsula, chemical weapons would be used before a nuclear attack.

South Korean students seen during a gas mask drill Image: Ahn Young-joon/AP Photo/picture alliance

It was previously believed that the program was designed to be a "poor man's nuclear weapon" to serve as a deterrent before the North had truly developed an atomic capability, but there appear to be multiple reasons why the North continues to invest in chemical weapons, shesaid.

"A nuclear attack by the North would be met by overwhelming retaliation that would end the regime there," he said. "But if a conflict was going against the North, and South Korean troops were advancing on Pyongyang, then the North could use chemical weapons to degrade or delay that operation."

On the battlefield, the consequences could be appalling, particularly among civilians caught

up in any fighting and not equipped with protective equipment.
"It would be awful," Pinkston said. "We have plenty of examples, unfortunately, such as Iraq using chemical weapons against Iranian forces in the 1980s, Syria doing the same against rebels and civilian populations, and there are also reports of Russia using them in Ukraine.
"Some say that chemical weapons are a taboo because what they do to the human body is so horrific and so indiscriminate, but North Korea is not a signatory to the Chemical Weapons Convention and there are examples of them using this stuff, so I see no signs that they will give them up."

Alarm at additional data

Ryo Hinata-Yamaguchi, an associate professor specializing in military issues at Tokyo International University, is equally alarmed at the latest data emerging from North Korea.
"This builds on information from other sources, including high-ranking defectors, so we have to take this very seriously," he said. "Having said that, and while we know that the regime is ruthless and cruel, we do not know how effective these will be as weapons, including the systems that they need to deliver them to the battlefield."
But he agrees that the regime would not hesitate to at least attempt to use them to stave off final collapse.
"They have shown that they had no concerns about using VX in a public space in 2017, the North regularly defies international law and I believe they see chemical weapons as having a useful psychological impact," he said.
"I feel they would use anything they could to level the playing field against a technologically superior opponent, so, worryingly, the likelihood of the North using chemical weapons in wartime conditions is quite high."

EDITOR'S COMMENT: A sudden large-scale North Korean chemical attack on the western United States using missiles and drone swarms would almost certainly become one of the most catastrophic military events in modern history, but the outcome would depend heavily on delivery effectiveness rather than just the size of the stockpile. Having thousands of tons of sarin or VX does not automatically translate into the ability to successfully disperse those agents across major American population centers. The first reality is geography. North Korea is extremely far from the continental US. To hit the West Coast directly, it would need intercontinental ballistic missiles or covert delivery systems. Chemical weapons are difficult to deliver effectively via ICBMs because the heat and stress of atmospheric reentry can destroy or degrade the agent unless the warhead is specially engineered. VX is more stable than sarin, but both still face major technical challenges during long-range missile delivery. That means North Korea would likely rely on a mix of methods: some ballistic missiles aimed at ports or military facilities, drones launched from ships or containers closer to the US coast, cyberattacks to disrupt response systems, and possibly sabotage teams. The United States would probably detect preparations before the attack actually landed. North American Aerospace Defense Command, United States Strategic Command, naval radar networks, satellites, and Pacific missile defense systems are designed specifically to watch for launches from North Korea. Some incoming missiles would likely be intercepted by systems such as Missile Defense Agency assets, including ground-based interceptors in Alaska and California, Aegis destroyers, and THAAD batteries. If even a fraction penetrated defenses and dispersed chemical agents over urban areas like Los Angeles, San Francisco, Seattle, or military/naval facilities, the immediate impact would be mass panic, overwhelmed hospitals, transportation shutdowns, and potentially tens of thousands of casualties in the first hours depending on weather conditions and concentration. VX is especially terrifying because tiny amounts can kill, and contamination can persist longer than sarin. Sarin disperses more quickly but can still produce devastating casualties in enclosed or dense urban environments. Drone swarms would add another layer of difficulty. Hundreds of small drones flying low could potentially evade some radar systems, especially if launched from offshore merchant vessels or disguised platforms. However, chemical dispersal from small drones is less efficient than people often imagine. Wind, sunlight, humidity, and urban airflow dramatically reduce concentration levels outdoors. Chemical weapons are most lethal in enclosed spaces, subway systems, tunnels, or indoor ventilation environments. The broader consequences would likely be even larger than the direct deaths. The US government would probably immediately declare a national emergency, suspend portions of civilian air traffic on the West Coast, mobilize the military domestically, and activate continuity-of-government plans. Financial markets could temporarily halt. Ports in California and Washington might close completely. There would likely be evacuations, quarantine zones, and widespread fear of secondary attacks. Militarily, the US response would almost certainly be overwhelming and immediate. North Korea's leadership knows this, which is one reason analysts generally believe these weapons are primarily deterrents rather than practical first-strike tools. A confirmed chemical attack on the American homeland would likely trigger massive conventional retaliation against North Korean military infrastructure and potentially leadership targets. The risk of escalation into nuclear conflict would become extremely high within hours. Another important point is that casualty estimates in chemical warfare are often exaggerated

in the public imagination because movies depict gases spreading endlessly through cities. In reality, outdoor chemical attacks are highly dependent on wind patterns, atmospheric stability, terrain, and dispersal quality. Even large stockpiles can produce limited strategic effects if delivery systems fail or weather conditions shift unexpectedly. Biological weapons generally pose a greater mass-casualty threat over long distances than chemical weapons do. The most plausible "worst case" would not be destruction of the western US, but rather a combination of several successful strikes causing severe local casualties, economic paralysis, psychological shock, and rapid military escalation. The geopolitical consequences could reshape global security for decades.

Hard to Find, Hard to Kill: Foundational Protection in a Transparent Battlefield

By Chief Warrant Officer Two Joshua LaPlant

Source: https://home.army.mil/wood/contact/publications/cr_mag-2/Hard-to-Find-Hard-to-Kill-Foundational-Protection-in-a-Transparent-Battlefield

May 29 – The modern battlefield is transparent. The rapid introduction of small unmanned aerial systems (sUAS) has altered the operational environment and makes widespread sensing a combat reality.[1] A recent course provided firsthand experience and revelations that highlight necessary evolutions within the Protection Warfighting Function to support movement and maneuver. While high tech solutions are critical, my experience evading sUAS in the woods of North Carolina proved that low-tech fieldcraft remains effective against high-tech platforms. To ensure future force readiness, the Maneuver Support Center of Excellence (MSCoE) and U.S. Army Chemical, Biological, Radiological, and Nuclear School (USACBRNS) must continue to improve and formalize unique sUAS tactics, techniques, and procedures (TTPs) while reinforcing the foundational principles of protection found in ADP 3-37.[6]

Protection in the Transparent Age

Persistent surveillance by stabilized platforms means that being hard to find is a prerequisite to being hard to kill. This aligns with the discussion in the Breaking Doctrine podcast, "Episode 66 Protection in Operations," which emphasizes that protection is not just a staff function but a foundational task for every Soldier.[1] Success in a sUAS saturated environment relies on a cultural mindset where minimizing signatures is a deliberate and constant discipline.[10] In modern peer and adversary tactics, stabilized sUAS generally act as the intelligence, surveillance, and reconnaissance (ISR) hunters. These platforms prioritize sensor stability over speed, utilizing high-fidelity thermal cameras and laser range finders to fix positions for indirect fire or to employ in first person view (FPV) killers. These FPV sUAS are purpose-built lethal effects platforms, often carrying specialized munitions or improvised payloads. Purpose-built FPV racing sUAS are capable of speeds exceeding 90 mph. When carrying lethal armament payloads, they function as high-speed, low-cost precision munitions in the hands of skilled pilots. With sUAS missions being highly tailorable and ranging from non-lethal electronic warfare to kinetic suicide strikes, Soldiers must be able to categorize the threat instantly to determine the correct survival response. Precise recognition is crucial because stabilized platforms possess the payload capacity to carry heavy armament which blurs the line between hunter and killer. This wide range of capabilities reinforces the urgent need for visual and acoustic identification as a foundational survival skill.

Firsthand experience in the field demonstrated that detecting the threat often begins with the basics, such as acoustic recognition. Unlike electronic detection systems that might miss smaller platforms, the distinct audible signature of a quadcopter can provide immediate warning. We currently test Soldiers on their ability to visually identify enemy vehicles, so we must now apply that same rigor and accuracy to the acoustic and visual recognition of different types of sUAS and their capabilities. Training Soldiers to recognize these signatures must become as fundamental as gunnery skills tests (GST). This will enable them to rapidly identify the platform, assess its payload, and execute Battle Drill 10 (React to Aircraft while dismounted) immediately.[3]

Standardizing Reporting Procedures

Detection is useless without dissemination. Once a threat is identified, the reporting format must be standardized across the force to ensure rapid engagement or avoidance. Current doctrine, specifically ATP 3-01.81 Counter-Unmanned Aircraft Systems Techniques,[7] recommends the use of a modified SALUTE report tailored for the sUAS fight. It requires specific details that change the commander's response. Formalizing and tailoring this reporting standard in the USACBRNS ensure that future leaders can feed the common operational picture (COP) accurately and transform individual Soldier observations into actionable intelligence.

Fieldcraft

Once detected, surviving relies on signature management. During daylight, stillness discipline and the use of thick, layered canopy were effective means of confusing thermal sensors by breaking up the human silhouette against the ambient heat of foliage. Movement was consistently the most reliable signature for detection. Successful countermeasures required absolute stillness and matching camouflage to the specific background environment. At night, however, thermal detection proved significantly easier for the sUAS operators. It is important to use 360-degree camouflage, masking presence, use deception, and unground fighting positions. This reinforces that basic Soldier discipline, which is the deliberate reduction of one's own thermal and visual signature, remains the baseline layer of protection.[3]

Discipline and TTPs

Operating in this environment requires disciplined emission control and deceptive flight maneuvers. We found that the common practice of relying on a sUAS's default return to home (RTH) setting, which would automatically engage when signal is lost, compromised the operator's location by tracing a predictable path back to the launch point. To mitigate this, we employed deception tactics like dogleg maneuvers, which is the technique of using not direct launch and recovery paths that deliberately masked the true location of the control base.[2] Furthermore, recovery teams had to treat retrieval operations as tactical patrols by utilizing bounding overwatch and SLLS (stop, look, listen, smell) to detect adversary reconnaissance platforms attempting to backtrack our position.[8] This same technique proved useful in any movement, keeping Soldiers alert and aware of possible threats around, above, and below.

The CBRN Paradox and sUAS Integration

A critical foundational paradox emerged during training where the terrain features that offer the best concealment from sUAS often present the highest contamination risks. Low draws, dense vegetation, and thick brush are excellent for masking thermal signatures from aerial observation, but they are naturally areas where chemical agents settle and accumulate. This forces leaders to face a complex dilemma. They must choose sUAS concealment and risk chemical exposure, or they must avoid contamination and risk aerial detection. This requires a deeper level of planning to predict how an enemy might synchronize these threats. CBRN planners must aid commanders in determining if the enemy is using CBRN to dislodge our forces out of cover for sUAS annihilation or using sUAS to fix our forces in place for a CBRN attrition strike. To resolve this, the USACBRNS must develop specific planning for hazard understanding and awareness that prioritizes remote sensing with sUAS assist units with risk management in these paradox zones.

Airspace Deconfliction and Planning

Integrating friendly sUAS to solve this paradox introduces a risk of accidental collisions or engagement by friendly forces. In an sUAS-saturated airspace, deciphering friendly from enemy platforms proved exceptionally difficult. When multiple friendly sUAS were employed for reconnaissance, airspace deconfliction became critical to prevent mid-air collisions and friendly fire incidents.[4] This requires strict adherence to airspace control measures and a heavy reliance on the COP and grid reference graphics (GRGs) to track friendly sUAS positions in real-time.[4,9] These coordinating measures added unforeseen complexities that the USACBRNS must address in detailed planning curriculums to ensure mission success.

Recommendations for Implementation

In summary, the way ahead is to transform these lessons into institutional readiness, and the USACBRNS should implement the following across all Programs of Instruction (POIs):

- **Institutionalize GST Identification:** Integrate visual and acoustic sUAS recognition into Gunnery Skills Tests to ensure Soldiers can distinguish sUAS across their varied capabilities.
- **Reinforce the Foundational Basics:** Adopt training standards for the deception maneuvers, mandate the use of 360-degree camouflage and defilade fighting positions to emission signatures, and aid in the defeat of thermal and visual sensors.
- **Standardize Reporting:** Mandate the use of the *ATP 3-01.81* modified SALUTE report for all sUAS sightings to ensure accurate data flows to the COP.
- **Plan for the Paradox:** Train leaders to plan and employ remote sensing via sUAS for reconnaissance to assist in risk-based decision making in support of operations.
- **Visual Feedback Training:** Utilize aerial thermal imagery captured during field exercises to provide students with immediate, undeniable evidence of their signature management successes and failures.

While these are not new recommendations, there is a difference between reading observations from sources such as the Center for Army Lessons Learned (CALL) and experiencing those lessons firsthand. These simple and effective observations will propel the USACBRNS and MSCoE forward and produce a significantly more prepared and lethal fighting force ready for the successful implementation and employment of robotics and unmanned systems by our future students.

Endnotes:

[1]Combined Arms Center. (2023). *Breaking Doctrine Episode 66: Protection in Operations* (Audio podcast).

[2]Department of the Army. (2022). *Aviation Urban Operations (ATP 3-06.1)*, https://www.alssa.mil/Portals/9/Documents/mttps/auo_2022.pdf
[3]Department of the Army. (2023). *Battle Drill 10: React to Aircraft While Dismounted – Platoon (07-PLT-D8015)*, https://rdl.train.army.mil/catalog-ws/view/100.ATSC/C17A21F3-CAFB-4591-BCC6-E2543F2CFE59-1688735194590/report.pdf
[4]Department of the Army. (2024). *Fire Support and Field Artillery Operations (FM 3-09)*, https://rdl.train.army.mil/catalog-ws/view/100.ATSC/9B9879F3-F213-4CD7-9D20-8D4520E8D38E-1397219978180/fm3_09.pdf
[5]Department of the Army. (2024). *Infantry Rifle Platoon and Squad (ATP 3-21.8)*, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN44065-ATP_3-21.8-001-WEB-3.pdf
[6]Department of the Army. (2024). *Protection* (ADP 3-37), https://rdl.train.army.mil/catalog-ws/view/100.ATSC/AEB2A8F7-017C-44B0-864C-0E7C2D039A6B-1346422199893/adp3_37.pdf
[7]Department of the Army. (2025). *Counter-Unmanned Aircraft Systems Techniques (ATP 3-01.81)*, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN43877-ATP_3-01.81-000-WEB-1.pdf
[8]Department of the Army. (2025). *Ranger Handbook (TC 3-21.76)*, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN45113-TC_3-21.76-000-WEB-2.pdf
[9]Joint Chiefs of Staff. (2021). *Close Air Support (JP 3-09.3)*, https://jdeis.js.mil/jdeis/new_pubs/jp3_09_3.pdf
[10]National Training Center. (2025). *Counter-Unmanned Aerial Systems (C-UAS) Training and Implementation at the National Training Center (25-1093)*, https://armyeitaas-my.sharepoint-mil.us/personal/joshua_e_laplant_mil_army_mil/Documents/Documents/390a/DOCTRINE and PRODUCT/25-1093, Counter-Unmanned Aerial Systems (C-UAS) Training and Implementation at the National Training Center (Aug 25).

Chief LaPlant currently serves as the CBRN Warrant Officer Instructor at Fort Leonard Wood, Missouri. He holds a bachelor's degree in computer animation from the International Academy of Design and Technology in Tampa, FL.

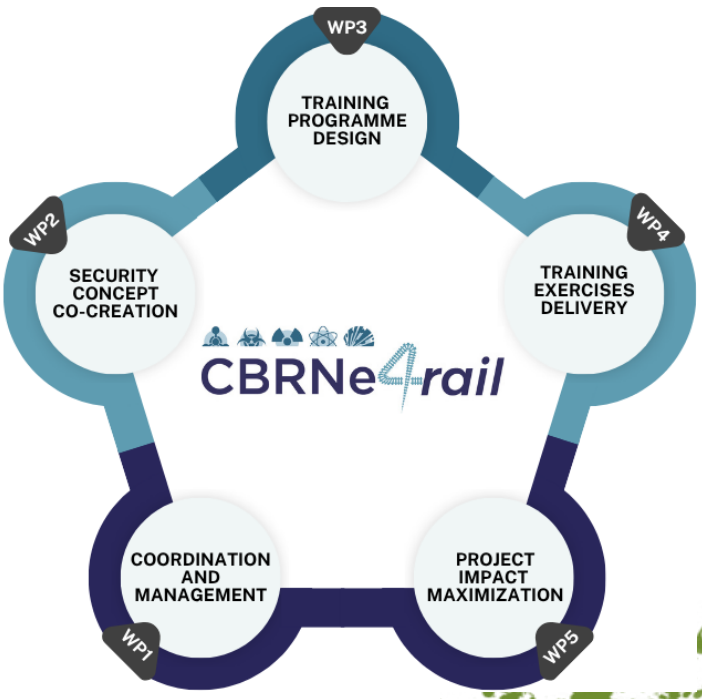
Source: https://www.cbrne4rail.eu/

This project aims to enhance awareness and capabilities of railway stakeholders to effectively respond to Chemical, Biological, Radiological, Nuclear and explosive (CBRNe) emergencies at railway stations by improving their security plans and training railway staff.
It tackles the whole CBRNe threat spectrum, including explosives as a means of delivery for CBRN agents. It focuses on railway stations as both a critical element of railway infrastructure and a key vulnerability element of public spaces. The public space inside stations and the adjacent public space in the vicinity of stations are considered.
Objectives
Co-create a railway CBRNe security concept with the inclusion of security-by-design recommendations
Develop a harmonised CBRNe training program for the railway sector for better cooperation with First Responders
Implement test and evaluate the training program by railway end-users in an operational environment
Provide a 'CBRNe Label' certified training and training kits to railway stakeholders for a long-term impact

EXPECTED RESULTS & ADDED VALUE

The project will adapt key results of recent EU- and NATO-funded CBRNe projects to the specific constraints of railway infrastructure and the needs of railway sector. It will develop a set of key exploitable results (KERs) which will enhance the preparedness and protection capabilities of the railway sector against CBRNe threats:

- Surveys, on-site expert field visits and workshops will be used to co-create and validate an effective railway CBRNe security concept. This will result in **an actionable guideline for railway end-users**, infographics and recommendations on how to adjust security plans.
- **An integrated, agile and scalable curriculum for the railway sector** and for better cooperation with the involved specialised First Responders will be developed, tested and updated.
- **A certified CBRNe training program** will be available at the end of the project for the rail community.



ORGANISATION OF THE WORK

The core technical work will be divided into three work streams. The first workstream will co-create a railway CBRNe security concept by: (1) assessing rail CBRNe threats, current security plans, existing security dedicated hardware and cooperation protocols; (2) creating operational scenarios revealing how terrorist attacks could be conducted and what impact it could bring upon the public; and (3) providing a guideline with recommendations to increase the CBRNe security level.

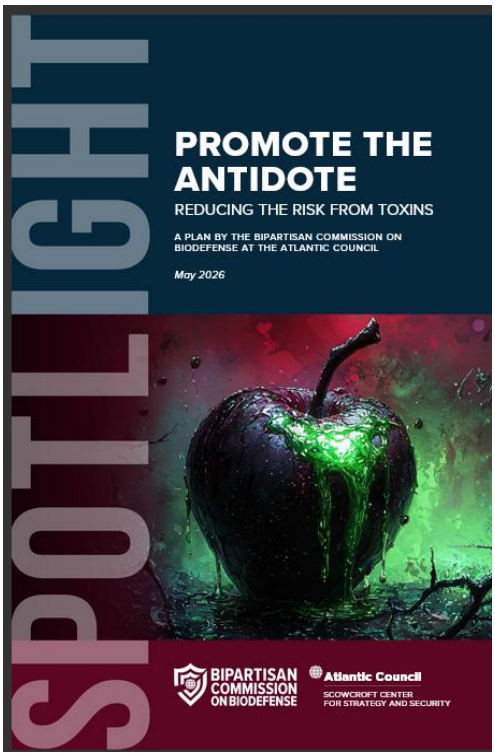
The second workstream will develop a harmonised CBRNe training programme for the railway sector and for better cooperation with the involved First Responders. The CBRNe4rail harmonised training programme will draw from past projects and will result in an integrated, agile and scalable curriculum for the CBRNe rail training program. The training will

be delivered to railway staff coming from at least 4 different EU Member States.
The third workstream will consist of the actual implementation and evaluation of the training program by railway end-users in an operational environment to apply the staff's newly gained knowledge and skills in simulated incidents at actual railway stations. At least 4 in-situ training exercises will be organised and will involve railway staff along with First Responders and LEAs (Law Enforcement Agencies). Based on the evaluation results, the training programme and materials will be fine-tuned and updated.
The impact of the technical activities and expected outcomes will be maximised as part of the "Communication, Dissemination & Exploitation" set of activities. Exploitation will include the certification of the training programme to ensure sustainability and pave the way for enlarging the number of railway companies receiving the certified training.

Consortium

Promote the antidote: Reducing the risk from toxins

By the Bipartisan Commission on Biodefense at Atlantic Council
Source: https://www.atlanticcouncil.org/in-depth-research-reports/report/promote-the-antidote-reducing-the-risk-of-toxins/



Toxins pose a persistent and evolving threat to national security

May 28 – While toxins occur naturally, contaminating food and feed with sometimes deadly consequences, malevolent actors have weaponized toxins for assassination and mass-casualty terror. Nation-states, terrorists, and lone actors continue to produce and weaponize these agents. The February 2026 confirmation by European governments that Russian opposition leader Alexei Navalny was assassinated using epibatidine (a lethal neurotoxin derived from a South American poison dart frog) underscores the twenty-first century reality of state-sponsored toxin warfare. Yet, national and international defenses remain fractionated. Efforts to address toxin threats span the agriculture, defense, law enforcement, and public health sectors, which often operate in silos.
The policymaking community is not fully aware of the expansion of the threat from toxins, instead focusing on contagious biological threats arising from viruses and bacteria. Significant and systemic governmental policy gaps persist despite a clear history of accidental contamination, criminal use, and the continued development of toxins in foreign offensive biological weapons programs. The United States cannot afford to ignore these vulnerabilities. It must identify and bridge these policy gaps immediately, as any biological event involving toxins will have profound implications for national and global security.

World's new tallest building races toward completion in Saudi Arabia

Source: https://newatlas.com/architecture/jec-tower-june-2026-update/

June 04 – The future world's tallest building has passed a major construction milestone. Saudi Arabia's JEC Tower has now reached 102 floors and is rapidly progressing toward its planned height of more than 1 km (0.62 miles).

Back in November of last year, we reported on the JEC Tower rising to 69 floors. With progress now moving at extremely rapid pace, it surpassed 100 floors in recent weeks, becoming one of only around 25 buildings worldwide to do so.

Architects Adrian Smith + Gordon Gill (AS+GG) recently confirmed it will consist of at least 157 floors. It will also be significantly taller than the current world's tallest building, the 828-m (2,717-ft) Burj Khalifa and almost twice the height of the USA's tallest skyscraper, the 541-m (1,776-ft) One World Trade Center. This kind of immense height requires a carefully considered structural system.

"Concrete is king in the Middle East," says engineering firm Thornton Tomasetti, which is helping realize the project. "So why not take advantage of Saudi Arabia's local techniques to construct Jeddah Tower? We did just that, with an efficient concrete-based system that employs construction practices and concrete strengths common in the region.

"The structural system is simplicity itself – without columns, outriggers, floor beams, spandrel beams, and vertical transfers. Specifically designed to be built quickly and efficiently, all walls are interconnected, and each structural element resists both wind and gravity loads. Below, a massive concrete foundation system

supports the weight of all that height – with a 5-meter [16.4-ft]-thick raft foundation supported on 270 bored piles, each 1.8 meters [5.10 ft] in diameter, that go to depths up to 105 meters [344 ft]."
Previously referred to as both the Kingdom Tower and Jeddah Tower, the JEC Tower is at the center of a new urban development in the bustling port city of Jeddah. Its interior will boast the world's highest observation point, plus a luxury hotel, office space, and palatial apartments.
The megatall skyscraper is just one of several "gigaprojects" announced for Saudi Arabia as it aims to transform into a major tourism destination. However, while others like the Line and Mukaab have seen their ambitions reduced or been cancelled altogether, JEC Tower is now firmly on track after years of delays, and Saudi authorities seem intent on realizing the project's ambitious vision.

EDITOR'S COMMENT: You are already aware of my intense addiction to super tall or long constructions when it comes to CBRNe defense. Same for this giga structure that will erupt without a specific plan for asymmetric threats (as always). To this, add drone and fire defense (see the new firefighting Chinese heavy drone for tall buildings since internal systems usually are not sufficient enough). Hope that the old perception "it will not happen to us" belongs to the past.

CBRNe Research and Innovation 2026: European Sovereignty Takes Center Stage at Arcachon Conference

By Marie-Andrée Karras Bianchini
For C²BRNE Diary

The **CBRNe Research and Innovation 2026** conference convened in Arcachon, France, from May 19–21, bringing together **680 participants representing over 40 nationalities**. The event featured **more than 100 scientific presentations**, **220 posters**, **15 thematic workshops**, **5 dynamic demonstrations**, and **35 international exhibitors**—marking one of the largest gatherings of its kind in Europe.
Organized with precision and efficiency, the congress provided a comprehensive platform for specialists from diverse backgrounds—civilian, military, academic, and industrial—to exchange knowledge on evolving CBRNe threats and preparedness strategies.

Strategic themes
European strategic autonomy
A dominant message throughout the inaugural session, delivered by **Mrs. Isabelle Rebattu** (Deputy Director of French State Protection and Security, SGDSN), emphasized the imperative for European

sovereignty in security and medical countermeasures. As highlighted in the French National Strategic Review 2025, Europeans must now take control of their own destiny, overcome fragmentation, and develop the depth, mass, and scale needed to address emerging hybrid threats.

"That era is over. The time has come for Europeans to take control of their own destiny." — French President Mr. Emmanuel Macron.

Seven thematic pillars

The conference was structured around seven core areas:

1. **Medical countermeasures** – advancing causal therapies and regenerative approaches
2. **Detection technologies** – AI-enhanced platforms and unified multi-modal systems
3. **Integrated risk & crisis management** – cyber-CBRNe nexus and systemic resilience
4. **Protection & decontamination** – active materials and thermal regulation
5. **Forensics & attribution** – building unbreakable chains of evidence
6. **Education & training** – immersive technologies and inter-agency collaboration
7. **Depollution & environmental restoration** – sustainable remediation strategies

Key Highlights: strategic shifts and operational innovations

The scientific program at Arcachon 2026 reflected a decisive pivot from reactive measures to proactive, integrated resilience. Three major trajectories emerged across the seven thematic pillars:

1. Medical countermeasures: from supportive care to regenerative sovereignty

A dominant theme was the urgent push for **European strategic autonomy** in Medical Countermeasures (MCMs). Rather than relying solely on global supply chains, the community is prioritizing the development and manufacturing of critical therapies within the EU.

- **Field-readiness:** Significant progress was highlighted in moving away from complex intravenous administration toward **non-invasive delivery routes** (such as intranasal or inhalation). This shift is designed to facilitate mass casualty management where traditional medical infrastructure may be compromised.
- **Causal Therapies:** The focus is expanding beyond merely sustaining life to actively repairing biological damage. Emerging research discussed **regenerative approaches** and host-directed strategies that aim to neutralize threats at the cellular level, reducing the severity of long-term sequelae for survivors.
- **Broad-spectrum innovation:** Discussions centered on next-generation vaccines and antivirals capable of addressing both known high-threat agents and rapidly evolving pathogens, emphasizing rapid response capabilities over static stockpiling.

2. Detection technologies: the rise of unified, AI-driven platforms

The era of single-purpose detection alarms is giving way to **intelligent, multi-modal systems**.

- **Convergence of threat classes:** New platforms are being designed to detect Chemical, Biological, and Radiological threats simultaneously. This reduces the logistical burden on first responders, who can now rely on a single, autonomous device rather than multiple specialized instruments.
- **AI as a force multiplier:** Artificial Intelligence is no longer optional but essential for interpreting complex spectral data in real-time. These systems can distinguish between genuine threats and background interference, handle "masking" scenarios (where threats are hidden), and provide immediate characterization rather than simple alerts.
- **Remote sensing & stand-off capabilities:** To enhance force protection, there is a marked trend toward using drones and remote sensors to characterize threats from a safe distance. This allows for the identification of hazardous materials in inaccessible or highly contaminated zones without exposing personnel to risk.

3. Integrated risk management: bridging the cyber-physical gap

The conference reinforced that modern CBRNe crises are rarely isolated physical events; they are **hybrid incidents** where digital vulnerabilities amplify physical dangers.

- **The cyber-CBRNe nexus:** expert sessions emphasized the need for interdisciplinary crisis units that integrate cybersecurity experts alongside traditional CBRNe specialists. Scenarios discussed included cyber-attacks triggering chemical releases or disinformation campaigns exacerbating radiological emergencies.
- **Strategic communication:** a new pillar of crisis containment was identified as **strategic communication**. In an age of cognitive warfare, managing the information environment and countering disinformation is as critical as physical decontamination for preventing panic and ensuring public compliance with safety measures.
- **Systemic resilience:** moving beyond siloed drills, training initiatives are adopting holistic frameworks that simulate complex, multi-domain disruptions, preparing organizations to adapt to the unpredictable nature of hyperconnected threats.

4. Protection and decontamination: active defense and human-centric design

Personal Protective Equipment (PPE) is undergoing a transformation from passive barriers to **active, adaptive systems**.

- **Active degradation:** Research showcased materials capable of not just trapping threats but actively neutralizing them at the molecular level. This innovation significantly reduces the risk of secondary exposure during doffing and minimizes environmental persistence.
- **Thermal regulation:** Recognizing heat stress as the primary limiter of operational endurance, new designs are prioritizing moisture management and thermal regulation. The goal is to extend safe working times in extreme environments without compromising wearer safety.
- **Realistic validation:** A critical takeaway was the move away from static laboratory testing toward **dynamic validation**. Simulations using animated mannequins and realistic field conditions are revealing that proper sealing of equipment interfaces is often more effective than fabric impermeability alone.

5. Forensics and attribution: building unbreakable chains of evidence

The scope of forensics has expanded from simple identification to **attribution and accountability**.

- **Source tracing:** Advanced analytical methods are now capable of linking specific agents to their production batches or synthetic pathways, providing the scientific basis needed for international judicial proceedings.
- **Post-conflict monitoring:** There is a growing emphasis on the long-term chemical legacy of conflict. Integrating environmental forensics with human biomonitoring is essential for protecting civilians in repopulated zones and assessing the full impact of past incidents.

6. Education & training: from standardized drills to immersive adaptability

The training paradigm presented at Arcachon signaled a decisive move away from rigid, siloed exercises toward **adaptive, immersive, and collaborative learning environments**. As threats become more hybrid and complex, the workforce must be trained not just to follow procedures, but to think critically under pressure.

- **Immersive technologies (XR & AI):** A major highlight was the mainstream adoption of **Extended Reality (XR)** and **Artificial Intelligence** in training scenarios. These technologies allow responders to practice high-risk missions—such as detecting invisible agents or managing mass casualty incidents—in fully virtual, safe environments. This approach eliminates environmental hazards, reduces costs, and enables the repeated rehearsal of rare but critical events that are difficult to simulate with live agents.
- **Inter-agency collaboration:** Recognizing that modern crises transcend organizational boundaries, training programs are increasingly designed to foster **cross-sector cooperation**. New frameworks bring together firefighters, medical teams, police, and cyber experts to solve shared problems, ensuring that communication barriers do not hinder response efforts during actual emergencies.
- **Safe, high-fidelity simulants:** The development of innovative, non-toxic simulants that mimic the physical behavior of hazardous agents allows for realistic victim decontamination drills without safety risks. This ensures that first responders can master the nuances of protective gear donning/doffing and decontamination protocols with a level of realism previously impossible to achieve safely.
- **Global standards, local realities:** While international bodies like the OPCW provide essential global frameworks, the conference emphasized the need for **local adaptation**. Training must be tailored to specific regional resources, cultural contexts, and infrastructure realities to ensure true operational readiness everywhere, from urban centers to remote Arctic regions.

7. Depollution & environmental restoration: rapid neutralization and long-term stewardship

The approach to decontamination has evolved from simple physical removal to **targeted molecular neutralization** and sustainable environmental recovery. The focus is now on restoring functionality to contaminated sites as quickly as possible while understanding the long-term ecological impact.

- **Speed and sustainability:** Traditional decontamination methods, which often generate large volumes of chemical waste, are being replaced by **rapid, low-waste technologies**. Innovations such as nanometric fog systems were highlighted for their ability to disinfect air and surfaces in minutes, allowing for a faster return to normal operations without leaving harmful residues behind.
- **Active vs. passive cleansing:** Similar to protection strategies, decontamination is shifting toward **catalytic destruction**. New materials are being developed that actively break down toxic agents into harmless byproducts rather than merely absorbing or trapping them. This significantly reduces the risk of secondary exposure and simplifies the disposal of contaminated waste.
- **Physics of cleaning:** Research presented underscored the importance of understanding the **physics of porous surfaces**. Effective cleaning requires tailoring protocols to the specific material (e.g., concrete vs. fabric) and initial moisture conditions to prevent the redistribution of contaminants deeper into structures.
- **Environmental fate and bioaccumulation:** beyond immediate cleanup, the conference stressed the necessity of **long-term environmental monitoring**. Studies on how radionuclides and toxins accumulate in marine ecosystems (such as bioaccumulation in shellfish) provide critical data for post-accident risk assessment. This mechanistic understanding is vital for developing effective remediation strategies and protecting food chains years after an incident.

Personal reflections

Having attended numerous CBRNe conferences globally, several aspects stood out:

Strengths:

- Exceptional organization with practical mobile applications for real-time program navigation
- High-quality presentations with meaningful opportunities for post-session discussions
- Valuable diversity of international perspectives enriching the discourse
- Strong presence of young researchers ensuring continuity in specialized research

Key takeaways:

1. **Relay generation:** The significant number of early-career researchers provides optimism for sustained advancement in this highly specialized field.
2. **European cooperation:** Particularly among smaller nations, there is a genuine appetite for shared knowledge and resources—though larger states face greater regulatory complexities.
3. **Balanced autonomy:** Effective crisis response requires both national operational autonomy and robust international cooperation—a dual approach acknowledging different countries' capacities while promoting standardized exchanges of knowledge and equipment.
4. **Agility advantage:** In my assessment, small agile structures with streamlined decision chains adapt better during crises than heavily regulated large bureaucracies.
5. **Public awareness:** There remains an urgent need to develop a broader culture of risk management among civilian populations, who will inevitably be the first responders in major incidents.

Regrets & future directions

Like many attendees, I regretted being unable to attend all sessions of interest due to scheduling conflicts—a testament to the breadth and quality of content presented. Looking ahead, the CBRNe community would benefit from:

- Extended networking periods between formal sessions
- Dedicated forums for North-South knowledge exchange
- Continued emphasis on translating laboratory innovations into field-ready solutions

Conclusion

Arcachon 2026 demonstrated that European CBRNe resilience depends on **smart, integrated approaches** combining scientific innovation with operational realities. The convergence of advanced technologies, collaborative networks, and human-centered design principles represents the path forward against increasingly complex hybrid threats.

As the conference concluded, the consensus was clear: **strategic sovereignty is not merely political ambition — it is a medical necessity.** The development of robust, sovereign medical countermeasures and detection capabilities forms the cornerstone of future resilience against evolving CBRNe threat landscapes.

Marie-Andrée Karras Bianchini is a PharmD – International Consultant specializing in medical management of Chemical, Biological, Radiological, and Nuclear risks, with a particular focus on European cooperation frameworks and crisis preparedness. Contact: makarras@cbrnerisk.com

CBRN Threat Preparedness Amid Rising Global Tensions

Source: https://fast-act.com/cbrn-threat-preparedness-amid-rising-global-tensions/

Recent military exchanges involving Iran, Israel, and the United States — including missile strikes and retaliatory actions — have increased instability across parts of the Middle East. Public reporting from NBC News and the BBC describes expanding cross-border activity and heightened military alert levels. As tensions rise, defense sectors reinforce preparedness across the full Chemical – Biological – Radiological – Nuclear (CBRN) spectrum to ensure readiness against both conventional and unconventional threats.
For defense sectors, readiness planning must account not only for conventional force engagement, but also for potential chemical exposure risks — whether from intentional use, damaged industrial infrastructure, radiological release, or secondary hazardous material events.
In environments where military tensions rise, preparedness planning remains a constant. For defense, military, civil protection organizations, and emergency responders, CBRN readiness is part of standard operational responsibility in complex and evolving security landscapes.

Why Escalation Increases CBRN Risk Awareness

Periods of instability elevate awareness across the full CBRNE spectrum. While media coverage often focuses on conventional military activity, defense planners evaluate broader exposure pathways involving chemical warfare agents, toxic industrial materials, radiological materials, and potential biological events.
CBRN risks may emerge through:

- Intentional deployment of nerve agents or other chemical warfare agents
- Damage to chemical storage sites or facilities near nuclear reactors
- Infrastructure disruption causing environmental contamination
- Accidental radiological release following strikes on industrial assets
- Secondary contamination during recovery or stabilization missions

It is important to recognize that CBRN risk does not rely solely on deliberate Chemical/Biological Terrorism Incidents. Industrial facilities and dual-use materials present in conflict zones can create serious exposure hazards if damaged. In such environments, threat detection, CBRN monitor teams, and rapid decontamination procedures become essential components of operational continuity. For defense organizations, CBRN threat preparedness requires planning for both deliberate and incidental exposure scenarios.

Chemical Threats Within the CBRN Defense Framework

Within the broader CBRN defense landscape, chemical threats demand particular attention due to their potential for rapid onset and vapor hazard exposure. Unlike some biological events that may present delayed symptoms, exposure to certain chemical warfare agents can produce immediate operational consequences.
Chemical hazards can impact:

- Force readiness and mission continuity
- Personal Protective Equipment integrity
- Vehicles, aircraft, and operational infrastructure
- Environmental stability within contested zones

Effective CBRN defense planning incorporates layered mitigation strategies. These typically include:

- Personal Protective Equipment readiness and disposal protocols
- Threat Detection systems and monitoring equipment
- Rapid-response decontamination procedures
- Structured CBRN defense training
- Readiness reporting and compliance with established CBRNE policies

CBRN Risk Mitigation and Security Governance Units within defense structures often oversee policy awareness, training levels, and readiness verification to ensure operational standards

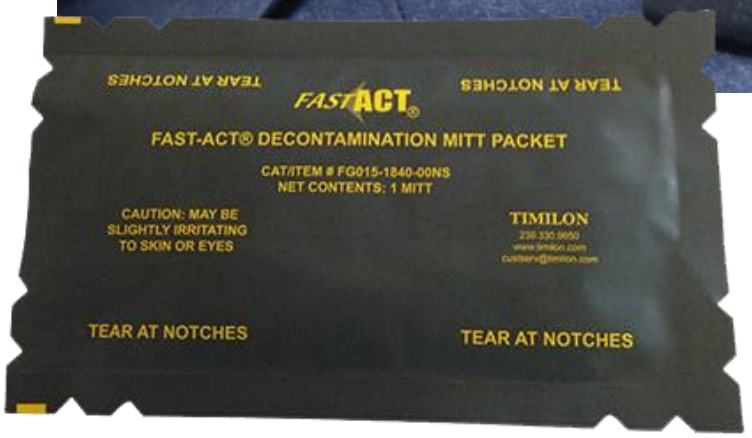
are maintained. Preparedness must be deployable under operational conditions — not limited to fixed installations or controlled environments.

The Role of Training and Simulation in CBRN Preparedness

CBRN threat preparedness is not solely equipment driven. It depends heavily on training programs and practical rehearsal.
Defense sectors frequently evaluate training gaps through simulation exercise and simulation-based training environments. These exercises help assess:

- Proper execution of decontamination procedures
- RED ZONE, YELLOW ZONE, and GREEN ZONE control integrity
- Coordination between emergency medical services and military units
- First responders' integration into disaster management protocols

Training levels must align with operational demands. Without regular CBRN defense training, policy awareness may exist on paper but fail under real-world pressure. Structured simulation-based training strengthens response speed, reduces hesitation, and reinforces discipline in high-risk environments.



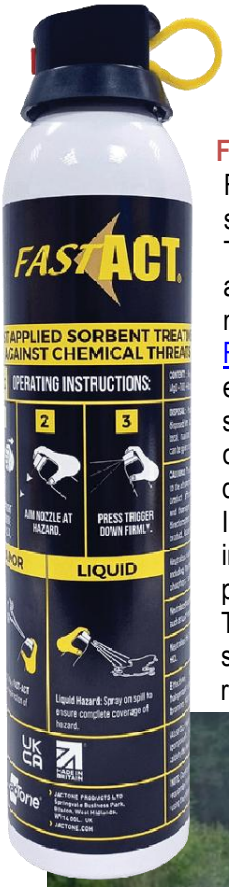
Scalable Chemical Mitigation in Dynamic Environments

Large-scale decontamination systems remain foundational in CBRN defense. However, early-stage mitigation tools are equally critical, particularly when infrastructure is compromised or mobility is required.
Organizations operating in unstable environments must be capable of:

- Containing hazardous vapors rapidly
- Reducing contamination spread across equipment and surfaces

environmental

- Supporting personnel protection before full decontamination lines are established
- Preserving force readiness during exposure assessment



Scalable chemical mitigation tools function as a bridge between initial exposure and comprehensive decontamination operations. In conflict or disaster management environments, rapid intervention capability strengthens resilience and reduces operational disruption.

FAST-ACT's Role in Chemical Risk Mitigation

FAST-ACT specializes in chemical neutralization technologies designed to support military, defense, civil protection sectors, and industrial response environments.

The FAST-ACT Pressurized Cylinder provides rapid adsorption and neutralization of hazardous chemical vapors and liquids. Its controlled discharge and portability support deployment in dynamic environments where immediate mitigation is required.

FAST-ACT Decontamination Mitts enable targeted neutralization on skin and surfaces, assisting personnel and equipment protection within operational zones. *CE classified as a class I medical device for use on skin and surfaces in the EU. FAST-ACT Decontamination Wipes support removal of trace contaminants, including hazardous chemicals and radiological materials, helping reduce secondary contamination. *CE classified as a class I medical device for use on skin and surfaces in the EU.

In addition to individual response tools, FAST-ACT offers scalable dry decontamination kits that integrate these applications into ready-to-deploy configurations. These kits support structured CBRN response planning and can be incorporated into broader CBRN defense training and operational readiness frameworks.

These solutions complement broader medical countermeasures and CBRN defense systems. They are designed to support early-stage chemical risk mitigation, enhancing layered preparedness rather than replacing established response frameworks.

Maintaining Preparedness in a Developing Situation

The situation involving Iran, Israel, the United States, and regional actors remains fluid and evolving. As information continues to emerge, defense organizations must focus on maintaining a disciplined CBRN threat preparedness plan.

CBRN readiness strengthens emergency responders' operational confidence and reinforces structured disaster management capabilities across sectors — including military units, first responders, and healthcare professionals operating within broader response frameworks.

Preparedness in the CBRN domain is not reactive. It reflects ongoing professional responsibility in uncertain environments. This remains a developing situation, and as conditions evolve, disciplined CBRN preparedness ensures organizations remain positioned to respond to potential risks.

Decontamination in Extreme Cold Weather:

By 1LT Jackson Riley

Source: https://home.army.mil/wood/contact/publications/cr_mag-2/Decontamination-in-Extreme-Cold-Weather-Operational-Viability-of-HEPA-Vacuum-Systems-for-CBRN-Response

CBRN Recon Platoon skijoring to a simulated production site. | Photo by PFC Ortiz, Victor

As Army operations expand into Arctic and sub-Arctic environments, the limitations of traditional chemical, biological, radiological and nuclear (CBRN) decontamination methods are increasingly evident. Current dry and liquid-based systems, though effective in temperate climates, are impractical in extreme cold weather. Freezing temperatures compromise equipment, delay response times, and endanger personnel. Recent field evaluations published by the U.S. Army Engineer Research and Development Center (ERDC) Cold Regions Research and Engineering Laboratory (CRREL) demonstrate that dry decontamination using high-efficiency particulate air (HEPA) vacuum decontamination systems offers a cheap, effective, and viable alternative for cold-weather operations.[i]

Environmental and Operational Challenges in Arctic CBRN Response

Arctic and extreme cold-weather conditions present severe operational challenges to CBRN protection. Sustained subzero temperatures freeze decontamination liquids on contact, damage sensitive equipment, and significantly increase the risk of hypothermia in contaminated casualties and CBRN response personnel. Moreover, reduced infrastructure and austere conditions limit the availability of generators, heating elements, and liquid storage systems required to run traditional decontamination stations. As a result, the environmental burden of liquid-based systems becomes a liability in cold-weather environments.

Patient decontamination in -20 degrees F. | Photo by PFC Ortiz, Victor

Most significantly, there is currently no effective way to remove radioactive-particle contamination or dusty-chemical agents in extreme cold-weather conditions. Using brushes is insufficient and cannot realistically be scaled to larger contaminated areas, elements, or equipment. Further, chemical agents behave differently in cold weather. While volatility of some liquid agents may decrease, thereby decreasing the vapor threat, their persistence on surfaces increases dramatically. In the case of sulfur mustard (HD), the physical state of the agent changes from a liquid to a solid in colder weather. Chemical dust is particularly difficult to remove without adequate heat or surfactants and cannot be removed or denatured with M291 or M100 kits. NATO's Science and Technology Organization noted in its technical report on sensitive-equipment decontamination that the need for dry, non-damaging removal methods is extremely relevant when dealing with electronics and other sensitive systems in extreme climates.[ii]

In joint-training exercises hosted by the 1st Brigade, 11th Airborne Division (ARCTIC) CBRN Reconnaissance Platoon, decontaminating personnel exiting contaminated areas proved a significant challenge. With temperatures sitting at an average of -15°F, M291-sorbent decontamination kits were the only option available without risking frostbite. The decontamination process not only took a significant amount of time, which increased the risk of cold-weather injury, but also failed to fully eliminate contamination. To make matters worse, in an Arctic-CBRN environment, supply lines can end up contaminated for months at a time given that normal weathering does not eliminate chemical hazards. This means that the availability of M291 kits can quickly diminish without resupply, which can be costly, hazardous, and nearly impossible in the worst conditions.

Laboratory and Field Validation of HEPA-Based Dry Decontamination

Decon team member skiing to establish EPDS. | Photo by PFC Ortiz, Victor

To address this capability gap, CRREL conducted laboratory assessments of four dry-decontamination technologies under a range of temperature and contamination conditions. These included the M2DCON wipe, FiberTect wipe, SX34 spray-and-vacuum system, and a commercial HEPA vacuum manufactured by NIKRO Industries. Simulated radiological particles were applied to pig skin, a common substitute for human skin, and contaminant removal was measured using X-ray fluorescence analysis.

The HEPA vacuum outperformed all other systems except FiberTect wipes, and even then, it showed superior results in several categories. At all three tested temperatures—64°F, 35°F, and 5°F—the vacuum maintained removal rates as high as 96 percent with no statistically significant performance loss at the lowest temperature.[iii]

To validate performance in a realistic operational setting, CRREL and AFRRI field tested the HEPA vacuum and FiberTect wipes during Exercise Arctic Eagle/Patriot 22 in Anchorage, Alaska. Participating units included the U.S. Marine Corps Chemical Biological Incident Response Force (CBIRF), National Guard CERF-P elements, and the 95th Chemical Company. Role players were subjected to both ambulatory and nonambulatory decontamination procedures using colored simulants to visually assess efficacy. Both technologies achieved complete contaminant removal from easily accessible areas, such as forearms and hands. However, the HEPA vacuum proved more effective in hard-to-reach areas,

such as behind the ears. Role-player surveys found no difference in perceived effectiveness but did reveal a higher rate of physical discomfort from the HEPA vacuum's brush, suggesting a need for ergonomic improvement.[iv]

1/11 CBRN Platoon conducting troop decon. | Photo by PFC Ortiz, Victor

Process throughput favored the HEPA vacuum, with an average of 45 ambulatory casualties processed per hour compared to 29 with FiberTect wipes. Combining both methods, using wipes for gross contamination followed by HEPA vacuum for detail cleaning, produced the highest efficiency at 48 individuals per hour. These results support dual-use integration of dry technologies into doctrine.

Doctrine and Fielding Implications

The performance of HEPA vacuums under extreme cold-weather conditions justifies their inclusion in CBRN doctrine for cold-weather operations. Additionally, pairing vacuums with powder-based decon systems offers a redundant, scalable solution that remains effective even when power sources fail. Given the flexible application, ease of use, and performance under temperature stress, HEPA-based dry decontamination should be considered a doctrinally valid alternative to water-based systems in both extreme-cold and temperate environments.

Should vacuum-based decontamination kits be fielded, certain issues still need to be solved, primarily power supply and waste disposal. Once vacuums are full, opening units in the cold risks seal failure due to material embrittlement. A working solution is to seal the entire unit in a vapor-resistant bag for disposal with pre-staged clean replacements swapped in to maintain tempo. Powering the devices comes with potential problems as well. Battery-powered devices of all types face significant performance loss below 20°C, and charging batteries in the cold can cause permanent damage. This can be mitigated by keeping storage and charging stations heated, protecting batteries with insulated covers or warmers, maintaining a rotation schedule for charged spares, and placing uninterruptible power supply (UPS) systems for essential equipment in temperature-regulated spaces.

This dry approach also aligns with larger Department of Defense efforts to modernize field CBRN response capabilities. As demonstrated by AE/P-22, integrating HEPA vacuums into Arctic operations increases operational speed, reduces logistical burden, and improves casualty throughput.[v]

Conclusion

The U.S. Army must prepare for sustained operations in Arctic and extreme cold-weather environments where traditional wet decontamination is not only untenable but can be outright lethal. Current dry-decontamination methods prove insufficient and logistically burdensome. Laboratory and field evidence demonstrates that HEPA vacuum systems offer a cold-capable, logistically lean, and effective alternative. Integrating alternate dry-decontamination methods into doctrine, training, and procurement will ensure that CBRN units remain capable and resilient, even in the world's toughest climates.

Acknowledgement:
My sincere thanks to Dr. Joseph Corriveau of the Cold Regions Research and Engineering Laboratory whose careful review and supportive guidance helped me refine this article and approach it with greater clarity.

1LT Jackson P. Riley is a U.S. Army CBRN Officer currently attending CBRN CCC at Fort Leonard Wood, Missouri. He has served in operational and planning roles in 1st Brigade 11th Airborne Division at Fort Wainwright, Alaska, with experience in dismounted CBRN reconnaissance, decontamination, and training development in extreme cold-weather conditions.

EDITOR'S COMMENT: This article reminded me our training in the ABC Zentrum, Swiss Army, for the 2004 Olympic Games in Athens. Such a pleasant training with below zero temperatures!

OPCW examines how drone technology changes global chemical security landscape

Source: https://www.opcw.org/media-centre/news/2026/06/opcw-examines-how-drone-technology-changes-global-chemical-security

June 10 — Emerging technologies are reshaping the chemical security landscape, and uncrewed aerial vehicle (UAV) technologies, commonly referred to as drones, are among the most prominent examples. Drones are widely used in many areas of security, including border surveillance, critical infrastructure monitoring, disaster response, and law enforcement operations, but also in other areas of life, such as agriculture, industry, logistics, and tourism.

As these systems become cheaper, more capable and more widely available, they create new challenges for preventing the misuse of toxic chemicals. At the same time, they offer opportunities to support verification and capacity-building activities carried out by the Organisation for the Prohibition of Chemical Weapons (OPCW).

Seventeen experts from various organisations had the opportunity to explore how this technology could impact the implementation of the Chemical Weapons Convention (CWC) at an OPCW technical workshop from 22 to 23 April 2026 at the Organisation's Centre for Chemistry and Technology (ChemTech Centre). The workshop was organised with financial support from the European Union.

Rapidly evolving technology in a dynamic security landscape

"UAVs are not inherently problematic," said OPCW Deputy Director-General, Ambassador Odette Melono, at the opening of the event. "On the contrary, they offer significant benefits across civilian, industrial, and humanitarian domains. However, they also exemplify the challenge of dual-use technologies that could threaten the object and purpose of the Convention."

Under the CWC, chemical weapons include any munitions and devices designed to inflict harm or cause death through the release of toxic chemicals. Experts warned that non-State actors have demonstrated capabilities in both chemical weapons and drone weaponisation. The possible convergence of these threats raises concerns and should be closely monitored.

Experts at the workshop underlined that drone technology is evolving faster than the ability to control it. Criminal actors are quick to test and adapt emerging technologies, and keeping up to date with technological developments is no longer optional.

From threat to tool: Drone technology in support of OPCW's mandate

The dual-use nature of UAV technology cuts both ways. The same advances that give rise to concern also open new possibilities. Participants in the workshop examined how drone technology could support the OPCW's non-routine field operations — activities carried out in complex, often dangerous environments such as active conflict zones, contaminated or damaged sites, or areas where access is restricted.

Working through a series of realistic field scenarios, a consistent theme emerged: in the context of OPCW field work, experts suggested that drones could be a valuable reconnaissance and safety tool. By

surveying a site before any team enters, a UAV can fundamentally alter the risk calculus of a mission, prioritising the safety of those involved.

Keeping pace

The workshop reflected OPCW's broader commitment to monitor scientific and technological developments that may affect the Convention's implementation. As UAV technology continues to evolve, the OPCW remains vigilant about the challenges new capabilities may present.

By bringing together experts from across disciplines, the OPCW is helping ensure that the CWC remains effective in a rapidly changing technological environment, while ensuring the Organisation and its Member States are able to acknowledge and address emerging chemical security challenges.

Background

How drone technology could impact the CWC has been a topic of discussion closely examined by the OPCW Scientific Advisory Board and the Open-ended Working Group on Terrorism.

The OPCW's Open-Ended Working Group on Terrorism, the primary platform through which States Parties address the challenge of chemical terrorism, has dedicated successive sessions to the issue, hearing from the United Nations Office of Counter-Terrorism in July 2025, an academic expert on UAV attack scenarios and emerging trends in October 2025, and, most recently, an Interpol expert in March 2026.

The Organisation's Scientific Advisory Board has been equally active, flagging risks posed by commercially available agricultural spraying platforms, the implications of AI integration, and the role of additive manufacturing in enabling bespoke dispersal devices.

As the implementing body for the Chemical Weapons Convention, the OPCW, with its 193 Member States, oversees the global endeavour to permanently eliminate chemical weapons. Since the Convention's entry into force in 1997, it is the most successful disarmament treaty eliminating an entire class of weapons of mass destruction.

In 2023, the OPCW verified that all chemical weapons stockpiles declared by the 193 States Parties to the Chemical Weapons Convention since 1997 — totalling 72,304 metric tonnes of chemical agents — have been irreversibly destroyed under the OPCW's strict verification regime.

For its extensive efforts in eliminating chemical weapons, the OPCW received the 2013 Nobel Peace Prize.

Did you knew?

Cantharidin, from the Greek *kantharis*, for beetle, is an odorless, colorless natural product with solubility in various organic solvents, but only slight solubility in water. The level of cantharidin in blister beetles can be quite variable. Among blister beetles of the genus *E picauta* in Colorado, *E. pennsylvanica* contains about 0.2 mg, *E. maculata* contains 0.7 mg, and *E. immaculata* contains 4.8 mg per beetle; males also contain higher levels than females. Males of *Berberomeloe majalis* have higher level of cantharidin per beetle: 64.22 ± 51.28 mg/g (dry weight) and 9.10 ± 12.64 mg/g (d. w.). Cantharidin content in haemolymph is also higher in males (80.9 ± 106.5 µg/g) than in females (20.0 ± 41.5 µg/g). Topical cantharidin is absorbed by the lipid membranes of epidermal cells, causing the release of serine proteases, enzymes that break the peptide bonds in proteins. This causes the disintegration of desmosomal plaques, cellular structures involved in cell-to-cell adhesion, leading to detachment of the tonofilaments that hold cells together. The process leads to the loss of cellular connections (acantholysis), and ultimately results in blistering of the skin. Lesions heal without scarring.

Cantharidin poisoning and acute radiation syndrome are fundamentally different conditions with different underlying mechanisms. However, severe cantharidin toxicity can produce some symptoms that overlap with those seen after significant **radiation** exposure and could, at least initially, suggest a similar diagnosis.

Both conditions may cause nausea, vomiting, diarrhea, abdominal pain, mucosal injury, skin blistering, shock, and, in very severe cases, multi-organ dysfunction. Cutaneous exposure to cantharidin is particularly known for causing vesicles and bullae, while high-dose radiation exposure can also lead to blistering, ulceration, and tissue necrosis.

Despite these similarities, important differences usually allow the two conditions to be distinguished. Acute radiation syndrome typically follows a characteristic sequence of prodromal symptoms, a latent phase, and then a manifest illness phase. It commonly causes bone marrow suppression, resulting in decreased white blood cells and platelets, increased susceptibility to infection, bleeding tendencies, and sometimes anemia. Delayed hair loss is another classic feature.

Cantharidin poisoning, in contrast, acts primarily as a vesicant and a toxin affecting the gastrointestinal and urinary tracts. Severe cases are more likely to present with blistering, intense gastrointestinal irritation,

blood in the urine, painful urination, kidney injury, electrolyte disturbances, and occasionally neurological symptoms. Bone marrow failure and the characteristic hematologic abnormalities of acute radiation syndrome are not typical features.
In summary, cantharidin exposure can mimic certain aspects of radiation injury, particularly severe skin and gastrointestinal manifestations, but it does not usually produce the full clinical picture of acute radiation syndrome, especially the hallmark bone marrow suppression and characteristic temporal progression.

Dismantling Syria's chemical-weapons stocks and legacy

By Annemiek Dols
Source: https://www.iiss.org/online-analysis/online-analysis/2026/06/dismantling-syrias-chemical-weapons-stocks-and-legacy/

June 12 – In March 2026, Syria's transitional government unveiled a plan to track and destroy the former Assad regime's remaining chemical weapons (CW) and facilities, including setting up an international task force in cooperation with the Organisation for the Prohibition of Chemical Weapons (OPCW). In addition to the inherently hazardous process of dismantling CWs, exacerbated by the presence of landmines and other unexploded ordnance around CW sites, Syrian authorities must deal with legal questions as to how to treat victims and perpetrators, as well as how to prevent chemical terrorism and CW non-proliferation to non-state armed groups. With documents and buried barrels of suspected chemical-warfare agents resurfacing, Syria faces major challenges in destroying the former CW programme, likely for years to come.

Tracing Syria's CW past

Following the chemical attack in Ghouta in August 2013 and the United States' and Russia's subsequent diplomatic campaign, in October 2013, Syria acceded to the 1993 Chemical Weapons Convention. Its initial declaration to the OPCW listed 12 production facilities, 1,300 tonnes of CW or precursors and a number of CW storage facilities. A joint United Nations–OPCW mission executed the removal and destruction of those CW-capabilities, verifying the destruction of 1,330 tonnes of CW in 2014. However, both the OPCW and the international community had suspicions that Syria's inventory had been far from completely listed, particularly as the Assad regime continued to conduct chemical attacks after 2014. Since the fall of the Assad regime in December 2024, more information about Syria's remaining CW has surfaced. There may be 100 additional facilities related to the former CW programme, accounting for various gaps in the previous declaration, such as mustard gas, methylphosphonyl difluoride (DF) and precursors to sarin. The full size of the programme is still unclear. Compared to the declared

programme of the former Soviet Union – 40,000 tonnes – the scale of the declared Syrian programme appears to be small, but it is larger than Libya's limited CW inventory of 23 tonnes of mustard agent in 2004.

A challenging task and environment

ue to the covert conduct and lack of transparency under the Assad government, the OPCW has been unable to verify the completeness of Syria's 2013 CW declaration. According to the OPCW Technical Secretariat, 19 issues remain unresolved, including the disappearance of 75 undeclared cylinders from a location previously reported to the OPCW. The armed conflict and the fall of the Bashar al-Assad government have resulted in the dispersal of knowledge, expertise and know-how about the former CW sites, and with that, a potential loss of evidence. Another concern is the potential acquisition of CW by non-state armed groups.

Moreover, the chemical-disarmament operations will require an investment of at least €12.5 million in 2027. For war-torn Syria, such a financial burden is difficult to carry, especially following the second Trump [US] administration's budget cuts to USAID programmes, which supported groups working on chemical disarmament. Syrian chemical-disarmament challenges do not end there. Firstly, the presence of unexploded ordnance around CW sites is an obstacle for OPCW inspectors. Clearing these bomb-damaged sites of explosives requires armoured mechanical assets. Secondly, ongoing domestic unrest in Syria, particularly in the coastal areas where most of the chemical arsenal and facilities are likely located, creates hazardous conditions and obstacles, compounded by a lack of guards to protect the facilities. For instance, the Islamic State (IS) remains active in Syria and has a track record of using CWs. Finally, the regional conflict creates unfavourable conditions for the chemical-disarmament process, such as preventing OPCW inspectors from entering the region.

The long tail of Syria's CW

Undoing the legacy of a CW programme is an arduous and technically challenging undertaking anywhere in the world. In Syria, it will likely take several years to inspect, destroy and verify 100 undeclared sites that might be linked to Syria's former CW programme. Its plan to eliminate the CW includes an international task force, consisting of Canada, France, Germany, Qatar, Türkiye, the United Kingdom, the US and the OPCW Technical Secretariat, to coordinate support for Syria in the form of training and equipment for the containment, storage, transfer and destruction of CW and residues.

Since November 2025, the OPCW Technical Secretariat has re-established its office in Syria, and visited more than 20 sites – including previously unexamined facilities in Barzeh and Jamraya – conducting interviews, preparing inventories and collecting samples and documents. At least four of these sites could be declarable to the OPCW and traces of a chemical-warfare agent were found at one site. The Syrian authorities also handed over 37 sealed cardboard boxes containing over 60,000 pages of documents. Thus, further investigation is required to determine the full scope of Syria's CW.

However, because of continuous civil unrest in Syria, OPCW personnel left the country in March 2026 and field visits were suspended until May 2026. A team has since been redeployed to Syria and has found 'dozens of undeclared chemicals munitions such as aerial bombs and rockets, as well as separately found chemicals and related equipment' – including rockets of the same type that were used in the Ghouta attacks – at undeclared locations in northwestern coastal and central regions. Previously, civil war meant that to safely dispose of its declared arsenal, Syria's CW were destroyed aboard the *Cape Ray*, a cargo ship. To dispose of the remaining stocks, the OPCW has called for an expedited on-site destruction process that preserves the evidence of CW use in Syria.

A final challenge is related to criminal justice for survivors and surviving relatives of chemical attacks. At least 18 people were recently arrested for their alleged involvement in the Ghouta attacks. In June 2026, the OPCW plans to conduct interviews into allegations of the use of CW and will provide information to the International, Impartial and Independent Mechanism to investigate perpetrators, which was established in 2016 to collect information and prepare criminal proceedings. Winning the race to secure evidence will be critical for Syria's road towards judicial accountability for the use of CWs.

For these reasons, dismantling and dealing with the legacy of the Assad regime's CW programme will likely take years to complete

.

Annemiek Dols is Programme Administrator for Strategy, Technology and Arms Control. Based in the IISS–Europe office in Berlin, Annemiek's duties include assisting the Strategy, Technology and Arms Control (STAC) team in the management and coordination the programme (such as publishing the Arms Control Primer podcast, event planning, and reporting), providing research support and background briefings, and writing articles on topics related to strategy, technology and arms control. Languages: English, Dutch, French, German.

Mind the Chemical Gap

By Sajad Shiri | CBRN Data Analyst | The Hague, South Holland, Netherlands
Source: https://www.linkedin.com/pulse/mind-chemical-gap-sajad-shiri-kgi6e/

June 13 – In March 2026 the body that polices the global ban on chemical weapons said something quietly alarming about artificial intelligence. The Organisation for the Prohibition of Chemical Weapons, the OPCW, the outfit that has verifiably destroyed every declared chemical-weapons stockpile on Earth; released the final report of its Scientific Advisory Board's working group on AI. The report's headline was optimistic: AI can help with verification, with sifting declarations, with corroborating reports of attacks (**1).** Buried in the framing was the uncomfortable part. The way the AI-safety world currently measures danger does not really see chemistry. It sees biology, and assumes chemistry is close enough.

It is not close enough. And the gap between how well we measure biological risk in frontier models and how poorly we measure chemical risk is now wide enough, and well-enough documented, to name plainly.

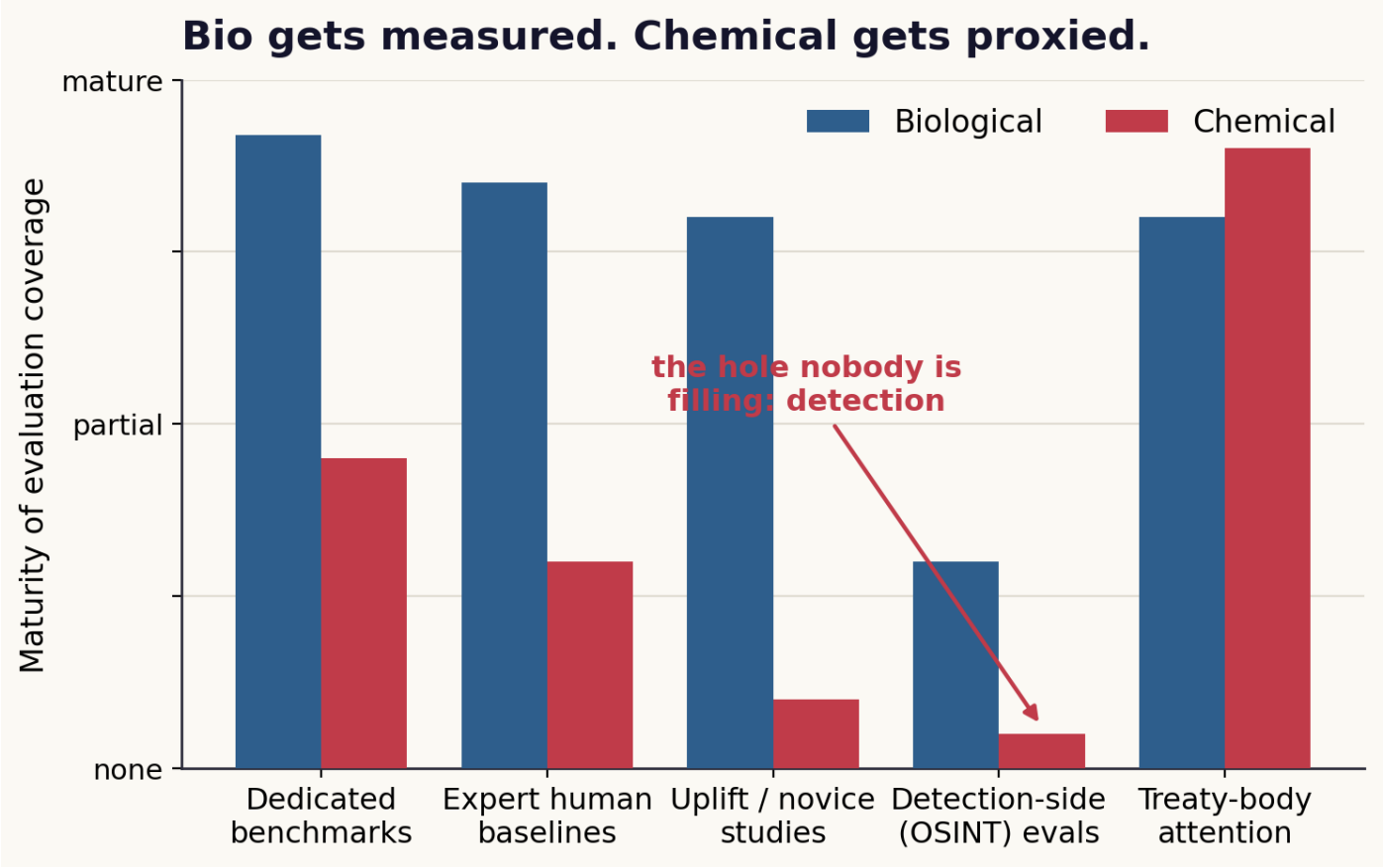


Figure 1. The asymmetry in one chart. Across the dimensions that make a risk legible; dedicated benchmarks, expert baselines, uplift studies, and detection-side evaluations; chemical-weapons coverage trails biological coverage on everything except treaty-body concern. Charted from the public benchmark and policy record; maturity is the author's coding, not a metric.

1.The proxy habit

Here is how the asymmetry got built, and it wasn't through negligence. When the major labs and evaluators sat down to measure whether a model could meaningfully help someone build a weapon of mass destruction, biology was the louder fire. The reasoning was defensible: a capable bioweapon can self-replicate and spread, the potential casualty ceiling is higher, and so biology became the canary. OpenAI's own preparedness work treats biological and chemical capability as a *combined* category and uses biological evaluations as the indicator for the high-risk thresholds (**2).** RAND's May-2025 benchmarking exercise (twenty-seven frontier models across eight knowledge benchmarks) is, by its own title, about the *biological* knowledge of frontier models; chemistry rides along (**3).**

The trouble with a proxy is that it works right up until the two things it bundles drift apart. Chemical-weapons risk is not a dimmer version of biological risk. The precursors are different, the production signatures are

different, the supply chains are different, and (crucially for anyone trying to *catch* a program rather than model one) the open-source footprint is completely different. A combined alarm line calibrated on the biological number can sit comfortably above the rising chemical one, and nobody notices the chemical curve climbing underneath it.

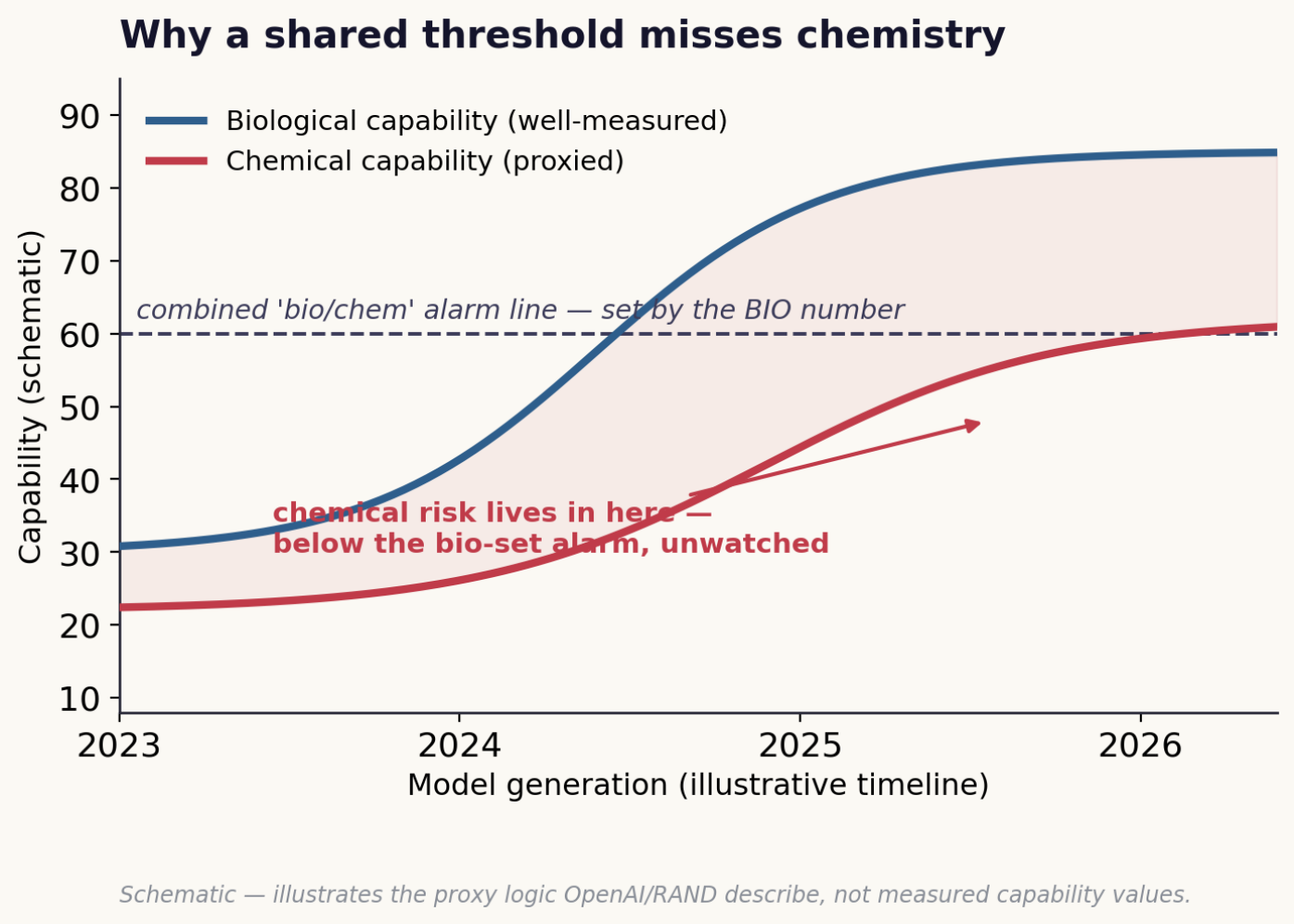


Figure 2. The proxy trap, schematically. When a single bio/chem threshold is set by the biological capability number, chemical capability can rise through the shaded band (real, growing, and below the alarm line) without ever tripping it. Schematic of the proxy logic described by OpenAI and RAND, not measured values.

The OPCW report is the first treaty-level acknowledgement that this bundling has a cost. Independent commentary on the report put it bluntly: the bio-as-proxy approach leaves chemical-specific risks *undertested* (**1).** When the organisation responsible for the Chemical Weapons Convention says the measurement instruments don't quite fit its weapon, that is not a footnote. That is the story. The AI-safety field measures whether a model knows dangerous chemistry. The OPCW needs to know whether AI can help it see a chemical programme in the open-source noise. Those are not the same test.

2.What the chemical tests actually test

There are chemical evaluations. The point is not that the cupboard is bare; it's that everything in it is pointed the same direction. WMDP includes a chemistry set; ChemBench probes chemical reasoning; ChemSafetyBench, published in early 2026, runs tens of thousands of prompts across chemical-property queries, legality, and synthesis-style requests; SoSBench covers chemistry among six high-risk scientific domains (**4,5,6).** The 2025 Frontier-Risk threshold work even sets a separate "chemical hazardous-knowledge" line, anchored on the WMDP-Chemistry expert baseline (**7).**

Line them up against the tasks a model could be asked to do, though, and a column goes empty.

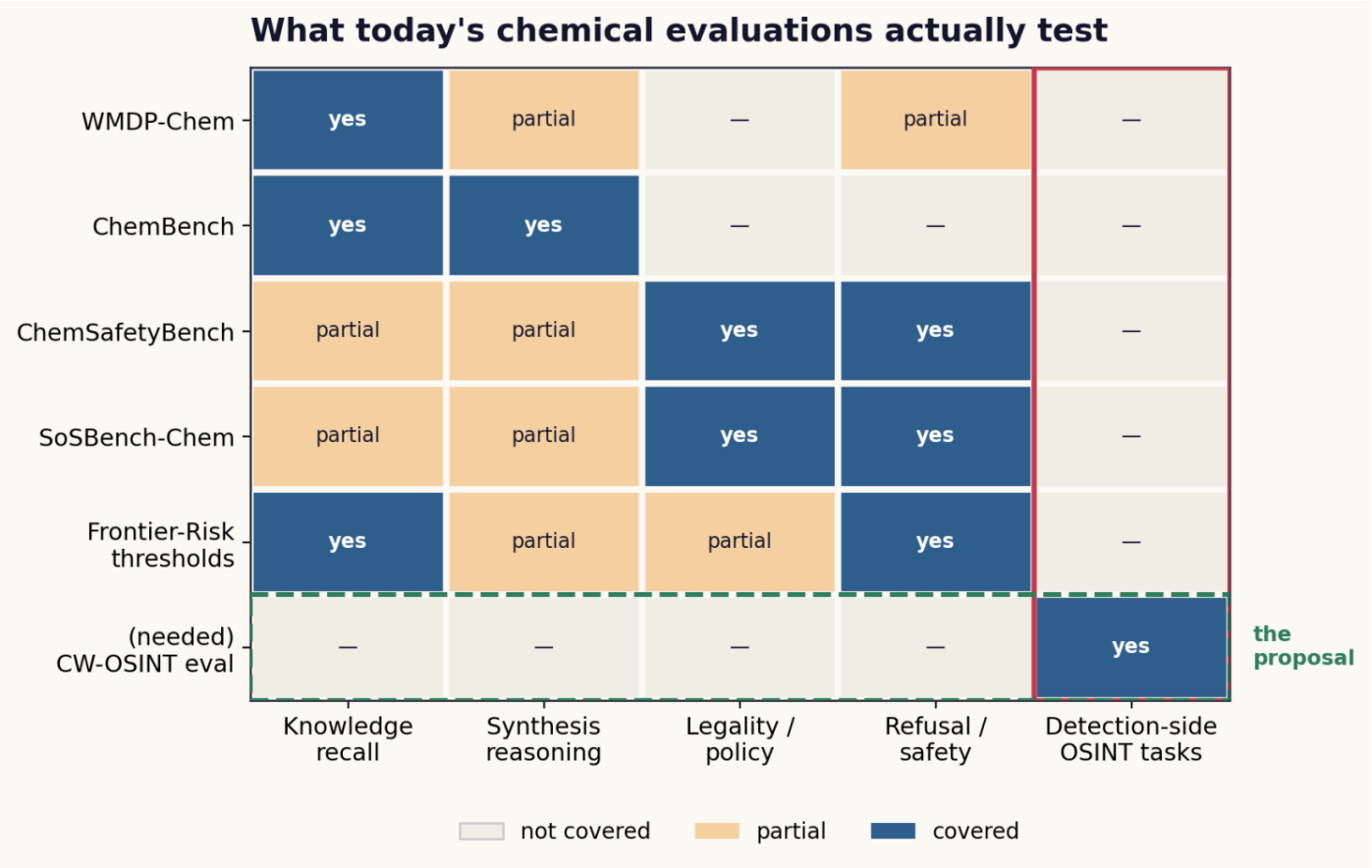


Figure 3. A coverage matrix of today's chemical evaluations against the task types that matter. Knowledge recall, synthesis reasoning, legality, and refusal are reasonably covered. The detection column; tasks an analyst would actually use AI for; is empty across every existing benchmark. The dashed row is the artifact this essay argues for.

Every existing chemical benchmark asks a variant of the same question: *does the model know, or reason about, or refuse, dangerous chemistry?* Knowledge in, knowledge out. None of them asks the defender's question: *given a pile of open-source material (customs records, satellite imagery, procurement filings, social media) can the model help an analyst find the signal that a program exists?* That is detection, and detection is not on the menu.

3.Recall is not detection

This distinction is the whole argument, so it's worth slowing down on. A recall benchmark is a closed-book exam: the dangerous fact either is or isn't in the model's head, and we test whether it comes out. A detection task is open-world and adversarial: the relevant facts are scattered across messy public data, half of it is noise, some of it is deliberately staged, and the job is to assemble fragments into a calibrated judgement that a programme is or isn't there.

Why does the defender side go unmeasured? Partly because it's harder to benchmark; you need labelled real-world cases, and confirmed chemical-weapons cases are mercifully rare and politically radioactive. Partly because the AI-safety community grew up worried about *uplift* (does the model make a bad actor more capable?) rather than *augmentation* (does the model make a defender more capable?). Both matter. Only one gets tested.

4.What to build instead

The fix is not to stop running recall benchmarks. They catch a real risk; that a model hands a novice the knowledge they couldn't otherwise get; and the uplift studies emerging on the biological side show that risk is no longer hypothetical (**3).** The fix is to build the missing column: a *defender-oriented, detection-grounded* evaluation for chemical-threat OSINT.

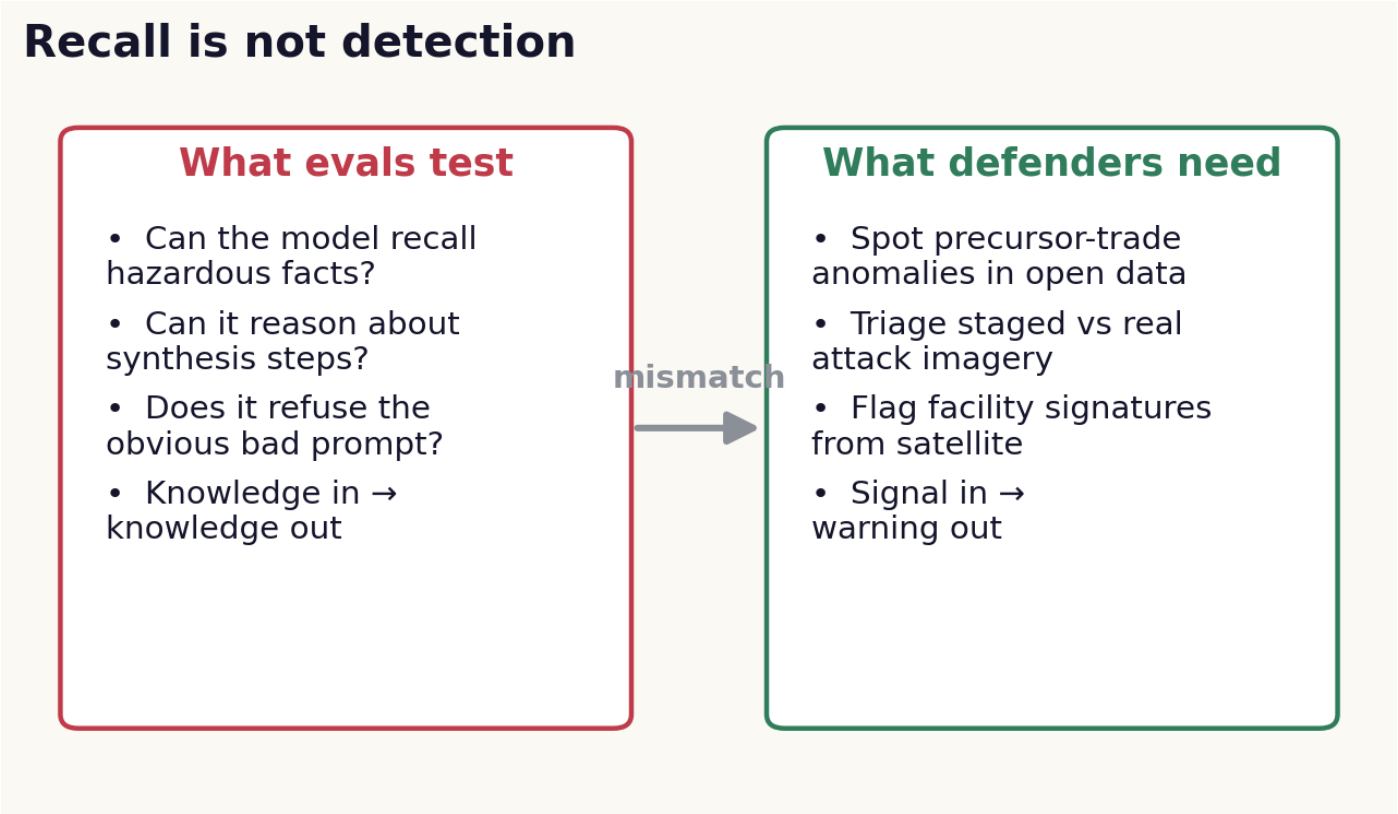


Figure 4. The mismatch in plain terms. The left column is what chemical evaluations measure. The right is what a chemical-threat OSINT analyst actually needs a model to do. The arrow between them is the gap. *Author's synthesis.*

A specification, in four parts

1. **Detection tasks, not recall items.** Give the model realistic open-source fragments (a customs anomaly, a facility image, a procurement chain) and score whether it surfaces the right signal, not whether it recites a fact.
2. **Labelled on public cases.** Anchor ground truth in already-documented, already-public events and matched dual-use controls, so the benchmark teaches discrimination, not memorisation - and adds zero hazardous content.
3. **Scored on the defender's metrics.** Precision and recall against the controls, false-alarm rate, and calibration - the numbers an analyst lives and dies by - rather than a single accuracy figure.
4. **Released open, for replicate-and-compare.** The thing that turns a one-off paper into a standard is a versioned, citable benchmark others must report against.

None of this requires touching dangerous detail. A detection benchmark scores whether a model can help *find* a programme in public data; it contains no synthesis routes, no acquisition tradecraft, no weaponization parameters. That's not a compliance afterthought; it's the reason the defender side is the publishable, fundable, citable side of this work.

5.Why this matters now

Timing is the argument's sharpest edge. The OPCW is not theorising about AI-assisted open-source corroboration; it is building toward it, and it has said so in a formal report and at an Executive Council side event.**1** National analysts are doing the same. If those tools get hardened into operational use without a defender-side evaluation to tell anyone how well they actually detect (their false-alarm rates, their blind spots, their calibration) then the chemical domain will have skipped the one step that would let it trust its own instruments.

The biological side spent the last three years learning to measure itself, sometimes uncomfortably, often in public. The chemical side has the same opportunity and a narrower window. The first move is cheap and entirely open-source: map what the existing chemical evaluations cover, name the detection column they all leave empty, and write the specification for filling it.

That map is a paper anyone in this field will have to cite, because it draws the boundary everyone downstream has to work inside.

Sources

1. OPCW. *OPCW releases landmark report on AI and the Chemical Weapons Convention.* 11 March 2026; and Scientific Advisory Board Temporary Working Group on AI, Final Report (SAB), released 3 March 2026. opcw.org. Independent commentary on the chemical-evaluation gap: *Biosecurity Handbook*, AI biosecurity notes, Nov 2025.
2. OpenAI. *Preparedness Framework* (biological and chemical capability treated as a combined category; biological evaluations as indicators for High/Critical thresholds). See also OpenAI, *Estimating Worst-Case Frontier Risks of Open-Weight LLMs*, arXiv:2508.03153, 2025. arxiv.org/abs/2508.03153.
3. Dev S, Teague C, Ellison G, et al. *Toward Comprehensive Benchmarking of the Biological Knowledge of Frontier Large Language Models.* RAND Corporation, RR-A3797-1, 2025. rand.org. On novice uplift: Zhang CBC, Knight CQ, et al. *LLM Novice Uplift on Dual-Use, In Silico Biology Tasks*, arXiv:2602.23329, 2026.
4. Li N, et al. *The WMDP Benchmark: Measuring and Reducing Malicious Use With Unlearning.* arXiv:2403.03218, 2024. arxiv.org/abs/2403.03218.
5. Zhao H, Tang X, Yang Z, et al. *ChemSafetyBench: Benchmarking LLM Safety in Chemistry.* 2026 (30,000+ samples across property, legality, and synthesis-style tasks). Project documentation, 2026.
6. *SoSBench: Benchmarking Safety Alignment on Six Scientific Domains.* arXiv:2505.21605, 2025 (chemistry among six high-risk domains; 3,000 regulation-grounded prompts). arxiv.org/abs/2505.21605.
7. *Frontier AI Risk Management Framework in Practice: A Risk Analysis Technical Report.* arXiv:2507.16534, 2025 (chemical hazardous-knowledge threshold anchored on WMDP-Chemistry expert baseline, 43.3%). arxiv.org/abs/2507.16534.
8. Quantifying CBRN Risk in Frontier Models. arXiv:2510.21133, 2025 (three-tier attack methodology; chemical/CBRN prompt set). arxiv.org/abs/2510.21133.

Toxins

By the Editor

A toxin is generally defined as a poisonous substance produced by a living organism. Toxins may originate from bacteria, fungi, algae, plants, animals, or marine organisms and can cause injury, disease, or death through biochemical interactions with cells and tissues. Contemporary toxicology distinguishes toxins from synthetic toxicants, although both may produce similar physiological effects. Natural toxins include bacterial neurotoxins, snake venoms, marine biotoxins, fungal mycotoxins, and plant-derived poisons. According to the Encyclopaedia Britannica definition of toxin, the term encompasses poisonous substances generated by organisms ranging from microorganisms and fungi to higher plants and animals.

Sources and Classification of Toxins

Plant toxins include ricin from castor beans, aconitine from monkshood, and cardiac glycosides from foxglove. Animal toxins include snake venoms, scorpion venoms, cone snail toxins, and pufferfish tetrodotoxin. Fish and marine organisms accumulate or produce toxins such as ciguatoxins and saxitoxins. Fungal toxins include aflatoxins and ochratoxins, whereas bacterial toxins include botulinum toxin, tetanus toxin, diphtheria toxin, and cholera toxin. The World Health Organization recognizes numerous naturally occurring toxins in food and aquatic environments, including algal toxins, shellfish toxins, and fish-associated toxins (i.e., Silver-cheeked toadfish | *Lagocephalus sceleratus* | tetrodotoxin), that may cause severe neurological and gastrointestinal disease.
Although fossils themselves do not produce toxins, paleontological specimens may preserve evidence of ancient venom systems or toxin-delivery structures, enabling reconstruction of toxin evolution. Consequently, fossils contribute indirectly to toxin research rather than serving as toxin sources.

Availability of Toxin Records and Databases

A substantial toxin record infrastructure already exists. The Toxin and Toxin Target Database (T3DB), available through T3DB (Toxin and Toxin Target Database), contains thousands of toxin records linked to molecular targets, toxicological properties, mechanisms of action, exposure data, and treatment information. Current versions include more than 3,600 toxins and over 2,000 toxin-target records.
Additional specialized repositories such as BioTD, accessible through BioTD (Biotoxins Database), catalog thousands of venom-derived and biologically active toxins relevant to drug discovery and biomedical research.

Beneficial Uses of Toxins

Despite their toxicity, many toxins have become valuable therapeutic agents. Botulinum toxin, one of the most potent biological substances known, is widely used in neurology, ophthalmology, dermatology, and pain medicine. Venom-derived compounds have produced drugs such as captopril, which originated from studies of Brazilian pit viper venom. Other toxin-derived compounds are being investigated for cancer treatment, targeted drug delivery, antimicrobial therapy, and chronic pain management.

Modern pharmacology increasingly views toxins as biologically precise molecules capable of targeting specific receptors, ion channels, and signaling pathways. This precision has transformed several toxins from feared poisons into important medicines.

Malicious Uses of Toxins

Toxins have also been employed in warfare, terrorism, criminal poisoning, and assassination. Their high potency, difficulty of detection, and often delayed clinical presentation make some toxins attractive agents for covert attacks. Historical interest in toxic substances spans ancient civilizations, medieval courts, intelligence services, and contemporary criminal investigations.

Notable Assassinations and Suspected Assassinations Involving Rare Toxins

One of the most famous toxin-related assassinations occurred in 1978 when Bulgarian dissident Georgi Markov was killed in London after exposure to ricin delivered through a modified umbrella device. Ricin, a ribosome-inactivating protein derived from castor beans, remains one of the most studied plant toxins in forensic toxicology.

Several historical poisonings involving aconitine, derived from monkshood plants, have also been documented in criminal and suspected assassination contexts because of the toxin's potent cardiotoxic and neurotoxic properties.

While confirmed assassinations involving tetrodotoxin, saxitoxin, or botulinum toxin are comparatively rare, these substances have periodically appeared in intelligence assessments, criminal investigations, and bioweapon discussions because of their extraordinary potency.

Artificial Intelligence and Toxins

Artificial intelligence is rapidly transforming toxin research. Machine-learning systems are used to predict toxin structure, receptor binding, toxicity, environmental persistence, and therapeutic potential. AI-assisted screening platforms can identify novel antidote candidates, optimize vaccine design, and accelerate toxicological risk assessments.

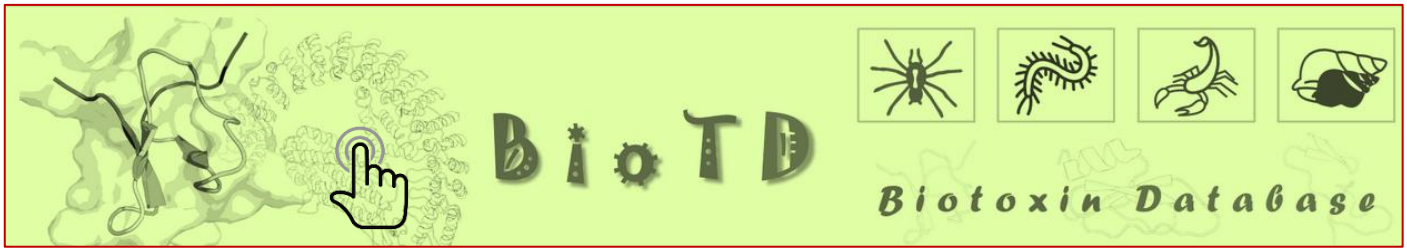
At the same time, AI raises dual-use concerns. Computational models capable of predicting biological activity could theoretically facilitate the design of more potent toxic molecules. Consequently, governments, research institutions, and technology developers increasingly emphasize biosecurity safeguards, controlled access, and responsible AI governance in toxin-related research.

Management and Clinical Treatment

Management of toxin exposure depends on rapid identification, supportive care, decontamination, and toxin-specific interventions. Activated charcoal, mechanical ventilation, intensive care support, and targeted antidotes remain central to treatment strategies.

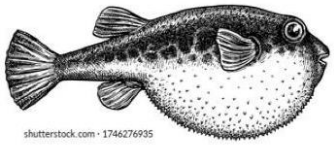
Several antidotes are already available. Botulism can be treated with antitoxin preparations that neutralize circulating toxin before irreversible neuronal binding occurs. Early administration significantly improves outcomes.

Antivenoms are available for many medically important snake, spider, and scorpion envenomations. Digoxin-specific antibody fragments are used for cardiac glycoside poisoning. Chelation therapies may be employed for certain metal-associated toxic exposures.



Vaccines Available Against Toxin-Mediated Diseases

Toxin	Vaccine Available?
Tetanus toxin	Yes (tetanus toxoid vaccine)
Diphtheria toxin	Yes (diphtheria toxoid vaccine)
Anthrax toxins	Yes (for selected risk groups)
Botulinum toxin	Experimental and limited-use candidates only
Ricin	Experimental vaccines under development
Saxitoxin	No approved vaccine
Tetrodotoxin	No approved vaccine



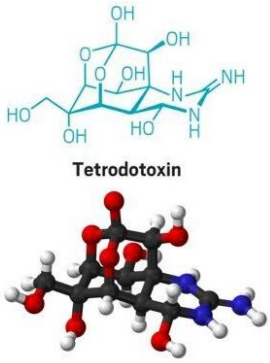


Table of major toxins and currently available antidotes, antitoxins, antivenoms, or specific treatments. Not every toxin has a true antidote; in many cases treatment is primarily supportive.

Toxin	Source	Main Clinical Effects	Specific Antidote / Treatment Available?	Notes
Botulinum toxin	*Clostridium botulinum*	Flaccid paralysis, respiratory failure	Botulinum antitoxin	Most effective when given early
Tetanus toxin	*Clostridium tetani*	Muscle rigidity, spasms	Human tetanus immune globulin (TIG)	Prevention by tetanus toxoid vaccine
Diphtheria toxin	*Corynebacterium diphtheriae*	Airway obstruction, myocarditis	Diphtheria antitoxin	Usually combined with antibiotics
Ricin	Castor bean (*Ricinus communis*)	Multi-organ toxicity	No approved antidote	Supportive care only; vaccines under development
Tetrodotoxin	Pufferfish (lagokefalos, pufferfish)	Rapid paralysis, respiratory failure	No approved antidote	Intensive supportive care and ventilation
Saxitoxin	Marine dinoflagellates, shellfish	Paralytic shellfish poisoning	No approved antidote	Respiratory support may be required
Aflatoxins	*Aspergillus* fungi	Liver injury, liver cancer	No specific antidote	Exposure prevention is critical
Amanitin	Death cap mushroom (*Amanita phalloides*)	Severe liver failure	Silibinin (available in many countries), supportive therapy	Liver transplantation may be necessary
Muscarine	Certain mushrooms	Cholinergic toxicity	Atropine	Highly effective antidotal therapy

Toxin	Source	Main Clinical Effects	Specific Antidote / Treatment Available?	Notes
Cyanogenic glycosides (cyanide release)	Cassava, bitter almonds, some plants	Cellular hypoxia	Hydroxocobalamin, sodium nitrite/sodium thiosulfate	Established antidote regimens
Cardiac glycosides (digoxin, oleander toxins)	Foxglove, oleander	Cardiac arrhythmias	Digoxin immune Fab	Effective against several related toxins
Snake venoms	Venomous snakes	Neurotoxic, hemotoxic, cytotoxic effects	Species-specific antivenoms	Mainstay of treatment worldwide
Scorpion toxins	Scorpions	Neurological and cardiovascular toxicity	Antivenom available for some species	Availability varies by region
Spider toxins	Certain spiders	Pain, muscle spasms, necrosis	Antivenom available for selected species	Depends on species
Cone snail toxins	Cone snails	Neuromuscular paralysis	No approved antidote	Supportive care
Ciguatoxins	Reef fish	Gastrointestinal and neurological symptoms	No approved antidote	Symptomatic treatment
Cholera toxin	*Vibrio cholerae*	Severe diarrhea and dehydration	Oral/IV rehydration	No toxin-specific antidote
Staphylococcal enterotoxins	*Staphylococcus aureus*	Food poisoning	Supportive care	Usually self-limited
Shiga toxin	*Shigella* spp., STEC	Hemolytic uremic syndrome	Supportive care	No approved toxin-specific antidote
Anthrax toxins	*Bacillus anthracis*	Shock, organ failure	Anthrax antitoxin (raxibacumab, obiltoxaximab)	Combined with antibiotics
Marine brevetoxins	Harmful algal blooms	Neurotoxic shellfish poisoning	No approved antidote	Symptomatic treatment

Vaccines and Emerging Countermeasures

Vaccines have successfully reduced disease caused by toxin-producing organisms. Tetanus toxoid vaccination is among the most effective examples of toxin-directed prophylaxis and has dramatically reduced mortality from tetanus worldwide.

Research is ongoing into next-generation vaccines against botulinum neurotoxins, ricin, staphylococcal enterotoxins, and other high-consequence biological threats. Advances in mRNA technology, structural biology, and AI-assisted antigen design may accelerate the development of new toxin countermeasures during the coming decade.

Prophylaxis

Prevention remains the most effective defense against toxin-related disease. Food safety programs, environmental monitoring, seafood surveillance, vaccination campaigns, occupational protections, and public-health education substantially reduce toxin exposure risks. Laboratory biosafety measures and international controls on biological agents further limit opportunities for malicious use.

Future prophylactic strategies may include personalized risk prediction, AI-assisted exposure monitoring, wearable biosensors, and broadly protective toxin-neutralizing antibodies.

Conclusion

Toxins occupy a unique position at the intersection of biology, medicine, toxicology, security, and biotechnology. Produced naturally by organisms ranging from bacteria and fungi to plants and animals, these substances can cause devastating disease while simultaneously providing powerful tools for therapeutic innovation. Comprehensive toxin databases now allow systematic study of thousands of toxins and their molecular

targets. Although toxins have occasionally been used in assassinations and other malicious acts, advances in antidotes, vaccines, surveillance systems, and AI-assisted research are expanding humanity's capacity to detect, prevent, and treat toxin-related threats. Continued investment in toxicology, biosecurity, and responsible AI governance will be essential to maximizing the benefits of toxin science while minimizing its risks.

What Operation Red Card Revealed About CBRNE Preparedness for the 2026 FIFA World Cup

Source: https://www.hstoday.us/subject-matter-areas/emergency-preparedness/what-operation-red-card-revealed-about-cbrne-preparedness-for-the-2026-fifa-world-cup/

June 16 – A recent George Washington University (GWU) Chemical, Biological, Radiological, Nuclear, and Explosive - Weapons of Mass Destruction (CBRNE-WMD) Capstone exercise, named Operation Red Card, examined how the United States can prepare for high-consequence, low-probability CBRNE incidents during major events such as the 2026 FIFA World Cup. The exercise brought together emergency management, public health, law enforcement, fire service, military, intelligence, and homeland security professionals to test response capabilities against complex, multi-domain threats involving chemical releases, biological incidents, radiological attacks, cyber disruptions, and cascading infrastructure failures.

The Challenge: From Awareness to Preparedness

More than two decades after September 11, the homeland security community has developed extensive awareness of CBRNE threats. The challenge is no longer identifying potential hazards but ensuring that organizations are adequately prepared to respond.

Despite numerous plans, exercises, and assessments, significant gaps remain between strategic threat assessments and operational readiness. The exercise found that preparedness often remains fragmented across jurisdictions and disciplines, limiting the ability to

respond effectively to complex incidents.

Three Scenarios, One Common Lesson
Students in the GWU CBRNE-WMD microcredential series explored three scenarios at World Cup sites in the US: a Chemical Attack and Infrastructure Failure in Los Angeles, a Biological Incident in Kansas City, and a Radiological Dispersal Device in New Jersey. Targets included infrastructure, event participants, and response capabilities. Challenges included multiple simultaneous attacks, presence of soft targets surrounding the game sites, loss of public confidence, and decontamination needs.

Key Lessons for Homeland Security

Intelligence and Fusion Must Be Operational
Fusion centres and intelligence-sharing mechanisms must be fully integrated into planning, prevention, response, and recovery activities rather than activated only during crises.

Capabilities Matter More Than Scenarios
Preparedness should focus on building flexible capabilities that can address a range of hazards rather than preparing for a single predicted event.

Cyber and Physical Security Are Inseparable
Infrastructure failures can significantly degrade emergency response capabilities. Planning must account for simultaneous attacks on both physical and digital systems.

Governance Influences Response
Legal authorities, mutual-aid agreements, and decision-making structures directly affect operational effectiveness during complex incidents.

Medical Countermeasures Remain Essential
Rapid decontamination, casualty management, prophylaxis programs, and long-term health monitoring remain critical components of any CBRNE response strategy.

Recovery Begins on Day One
Long-term recovery planning—including public information, behavioral health support, infrastructure restoration, and economic recovery—must be incorporated into preparedness efforts before an incident occurs.

Looking Ahead
The 2026 FIFA World Cup represents one of the most complex security environments ever faced by North American emergency management and homeland security agencies. The lessons identified during Operation Red Card extend well beyond sporting events and are applicable to any large-scale gathering or critical infrastructure target.
The exercise demonstrated that successful CBRNE preparedness is not simply a function of resources. It depends upon effective coordination, integrated planning, intelligence sharing, governance flexibility, and the ability to adapt to rapidly evolving threats.

Homeland Security Today Takeaway
The greatest challenge facing homeland security is not identifying potential threats—it is ensuring that communities, agencies, and governments are prepared to respond when those threats become reality.

Authors
Jennifer D. Osetek, PhD, MHS, CEM
Chuck Lineback, MS, NRP, NHDP-BC
Paul Biddle, CEM-ME
Victoria P. Simmons, MPS
Jason Kephart, MSC
Lamar González Medlock, MBA, CBRNE-WMD-C

Advisors
Bobby Baker
Elaine Lammert

2026 C²BRNE TERRORISM CONFERENCES

The NCT event series, organized by the CBRNe Society, offers regional editions in Europe, the United States, South America, the Middle East, and Asia. These events are characterized by conference streams, workshops, industry exhibitions, capability demonstrations, and training sessions. The events typically host 250-500 participants over 2-3 days and provide access to conference sessions led by first responders, technology exhibitions, and live CBRNE capability demonstrations. **The CBRNe Society** also conducts NCT PRO Trainings, which involve military and civil first responder teams from various regions. These teams are trained to operate in mock CBRNE, C-IED, and EOD scenarios, preceded by product training provided by industry sponsors. **NCT PRO** events focus on multinational and multidisciplinary training, offering participants an opportunity to work with cutting-edge equipment in a coordinated and efficient manner. The trainings consist of product training sessions and training missions tailored to the participants' needs and sponsored equipment.

DISASTER MEDICINE

Summer School

3-5 JULY, 2026

San Marino, Italy

Bright minds deserve a chance to shine — and we're here to help make it happen!

The Disaster Medicine Summer School aims to bring together motivated students and early-career professionals for an immersive educational experience in disaster and emergency medicine.

- Lectures
- Simulations
- Master classes
- Excursions
- Tabletop exercises
- Panels

Organised by:

European Centre for Disaster Medicine

EUROPA

World Association for Disaster and Emergency Medicine

CTM-E

Register your interest now

More info:students@wadem.org


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
BIO NEWS

Are there proven treatments for Ebola?

Source: https://www.nationalacademies.org/news/are-there-proven-treatments-for-ebola

May 22 – Yes. Scientists have developed treatments that improve survival for Ebola virus disease caused by Zaire ebolavirus, especially when patients receive care early. But treatments that work for one species of Ebola virus may not work against all Ebola viruses.

Supportive medical care remains the foundation of Ebola treatment.

Ebola virus disease can cause fever, vomiting, diarrhea, bleeding, dehydration, and kidney and liver failure. Patients often become severely ill because they lose large amounts of fluids and their organs may begin to fail.

Doctors treat Ebola patients with supportive care such as:

- Oral or intravenous fluids
- Oxygen support
- Blood pressure management
- Treatment for secondary infections
- Pain and fever control

Research during past Ebola outbreaks showed that high-quality supportive care can significantly improve survival, especially when patients receive care early and have access to well-equipped medical facilities.

Some Ebola treatments have been proven effective through clinical trials.

During the 2014–2016 Ebola outbreak in West Africa, researchers and public health officials worked to test experimental treatments during the emergency response. Clinical trials later identified antibody-based therapies that improved survival for patients infected with Zaire ebolavirus, the species responsible for several major Ebola outbreaks.

In 2020, the U.S. Food and Drug Administration approved two treatments for Zaire ebolavirus infection:

- Inmazeb
- Ebanga

These medicines use laboratory-made antibodies that help the immune system target the virus.

Research conducted during Ebola outbreaks helped scientists determine which treatments worked and which did not. Experts have emphasized that careful clinical research during epidemics is essential for identifying safe and effective therapies.

Existing Ebola treatments may not work for every Ebola virus.

"Ebola virus" actually refers to several related viruses. The two FDA-approved Ebola treatments were developed and approved for infections caused by Zaire ebolavirus and should not be assumed to be effective against other species of the virus.

The current outbreak in Uganda and the Democratic Republic of the Congo involves Bundibugyo virus, a different species of Ebola virus. Scientists are still studying whether existing treatments will work well against it.

This can create confusion because news reports may refer broadly to "Ebola treatments" or "Ebola vaccines," even though some products were designed for specific Ebola viruses.

Unproven remedies can delay lifesaving care.

Past Ebola outbreaks generated false claims about cures involving saltwater, high-dose vitamins, herbal remedies, colloidal silver, and other untested products. Public health experts warned that these claims could cause people to delay medical treatment or avoid trusted healthcare providers.

Researchers determine whether treatments work by conducting clinical trials that are designed to show whether those treatments are safe and effective. Anecdotes, social media posts, and individual testimonials cannot prove whether a treatment is safe or effective.

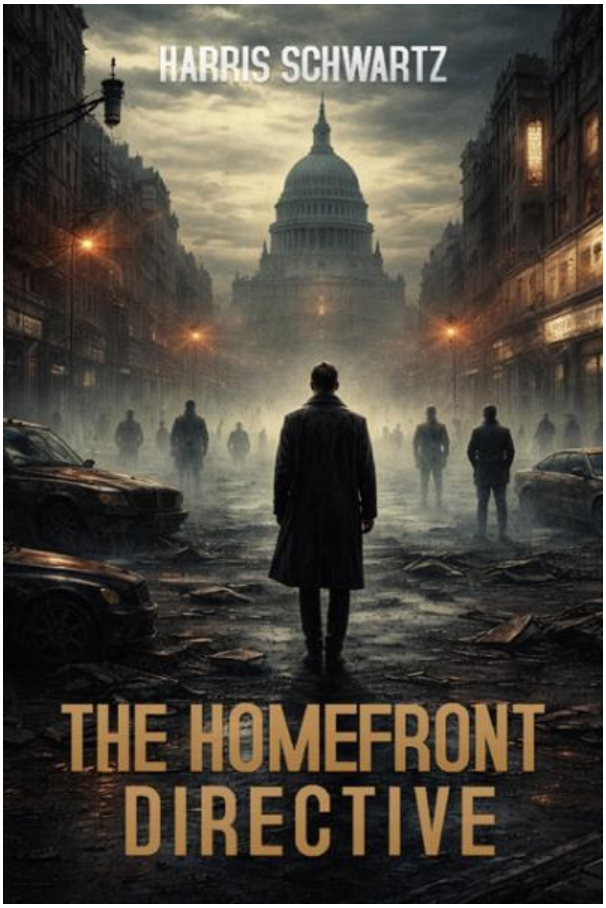
Health officials continue to monitor potential new treatments during outbreaks, but therapies should be evaluated through rigorous scientific testing before they are widely used.

Early treatment and trusted information are critical.

People who may have been exposed to Ebola should follow guidance from public health authorities and seek medical care promptly. Early diagnosis, supportive medical care, and evidence-based treatments can improve survival.

Harris Schwartz Debuts Political Thriller Exploring Bioterrorism, Broken Institutions, and the Fine Line Between Whistleblowing and War

Source: https://www.scottcoop.com/markets/stocks.php?article=globeprwire-2026-5-28-henderson-author-harris-schwartz-debuts-political-thriller-exploring-bioterrorism-broken-institutions-and-the-fine-line-between-whistleblowing-and-war



May 28 - Harris Schwartz's debut novel, The Homefront Directive, published by Writers of the West, opens in the early hours of a Denver morning with a rooftop, three people in respirators, and canisters of engineered microorganisms being released into the city's air supply. Nobody dies. The sensors go haywire and then go quiet. By noon, the mayor's office calls it an equipment glitch. The cover-up is so seamless it barely qualifies as one.

That is where the book begins, and it only gets more unsettling from there.

About the Book

The man behind the Denver operation is Dr. Erik Vance, a former corporate scientist who discovered that the research division he worked in had been quietly repurposed into something designed to harm people at scale. He did everything right. He documented the evidence, reported through official channels, and waited for the system to correct itself. What happened instead cost him his career, his clearance, and his faith in institutions entirely.

By the time the novel opens, Vance has spent years building a movement from the wreckage of that experience. Not a terrorist cell, exactly, but something harder to categorize: a distributed network of scientists, engineers, and bureaucrats who were each betrayed by the same institutions in their own way, now coordinated around a single purpose. They are not trying to kill anyone. They are trying to make the failure visible.

Chasing him is Jack Rence, a burned-out National Counter-Threat Agency analyst who has spent six months watching a threat pattern that the rest of his agency has written off as noise. When Denver breaks, Rence and his partner Maya Torres are the only people in the building who understand what they are actually looking at. Getting anyone else to believe them is a different problem altogether.

The novel moves fast and wide, from Washington to Denver to Iceland to the Norwegian Arctic, across fifty-three days of escalating crisis and one covert operation that asks its protagonist to disappear entirely into the world he is trying to dismantle. Schwartz has a sharp eye for the small institutional moments that determine whether crises get handled or get buried: the jurisdictional argument that burns three hours, the press statement drafted before anyone knows what happened, the analyst whose tracking log gets wiped overnight.

The result is a thriller that takes its time being right about things. Vance's diagnosis of institutional failure is not wrong. His methods are. Schwartz earns the ambiguity rather than selling it as a trick, and the book's final pages carry the kind of weight that lingers.

From the Author

"I kept thinking about the gap between how oversight is supposed to work and how it actually works when there is something powerful on the other side of it," Schwartz said. "Vance is not crazy. He is someone who tried to use the system and watched it turn on him. What I wanted to explore is what happens to a person after that, and what happens to the people who still believe the system can be made to work. Both of those stories feel true to me. The tension between them is the book."

Harris D. Schwartz is a global security executive and tenacious investigator with over 30 years of industry experience. Specializing in counterintelligence operations and domestic terrorism investigations, he has built a career pursuing complex threat actors and mitigating risks posed by domestic terrorist groups

targeting various industry-sector companies. His operational expertise includes safeguarding high-profile international events, such as the Super Bowl, and protecting Fortune 100 and Fortune 250 clients across the pharmaceutical, biotech, and financial services industries. By establishing robust business risk intelligence programs and leading complex investigations, Schwartz has consistently operated on the front lines of corporate defense, preventing domestic terrorism and financial fraud before they strike.

Scientists Discover New Giant Virus That Replicates in a Totally Unique Way

Source: https://www.sciencealert.com/scientists-discover-new-giant-virus-that-replicates-in-a-totally-unique-way

Giant viruses are so named because of the size of their genome. (Tumeggy/Science Photo Library/Getty Images)

May 28 – Researchers have discovered a new type of giant virus, which replicates in a way we've never seen before.

Stranger still, this entity could give us clues to the very origins of complex life. Viruses sit outside the standard tree of life, as they're made of segments of genetic material rather than cells. That makes it challenging to figure out how they originally evolved, and how they relate to living organisms.

Giant viruses – so called for their huge and complex genomes, compared to that of standard viruses – could help unravel that mystery. In this new research, microbiologists from the Tokyo University of Science (TUS) discovered the new giant virus, furtivovirus, in the Inasegawa River in Kamakura City, Japan. Its name comes from the Latin word *furtivus*, which means 'hidden' or 'stealthy', because of the initial difficulty the team had in picking it out from their sample.

This follows on from the recent identification of other giant viruses, including the discovery of ushikuvirus earlier this year by some of the same researchers.

While these giants all follow the standard virus practice of hijacking host cells to spread, there are some crucial variations too.

"Although these viruses belong to the same group, they use the cell nucleus in different ways," says Masaharu Takemura, a virologist at TUS.

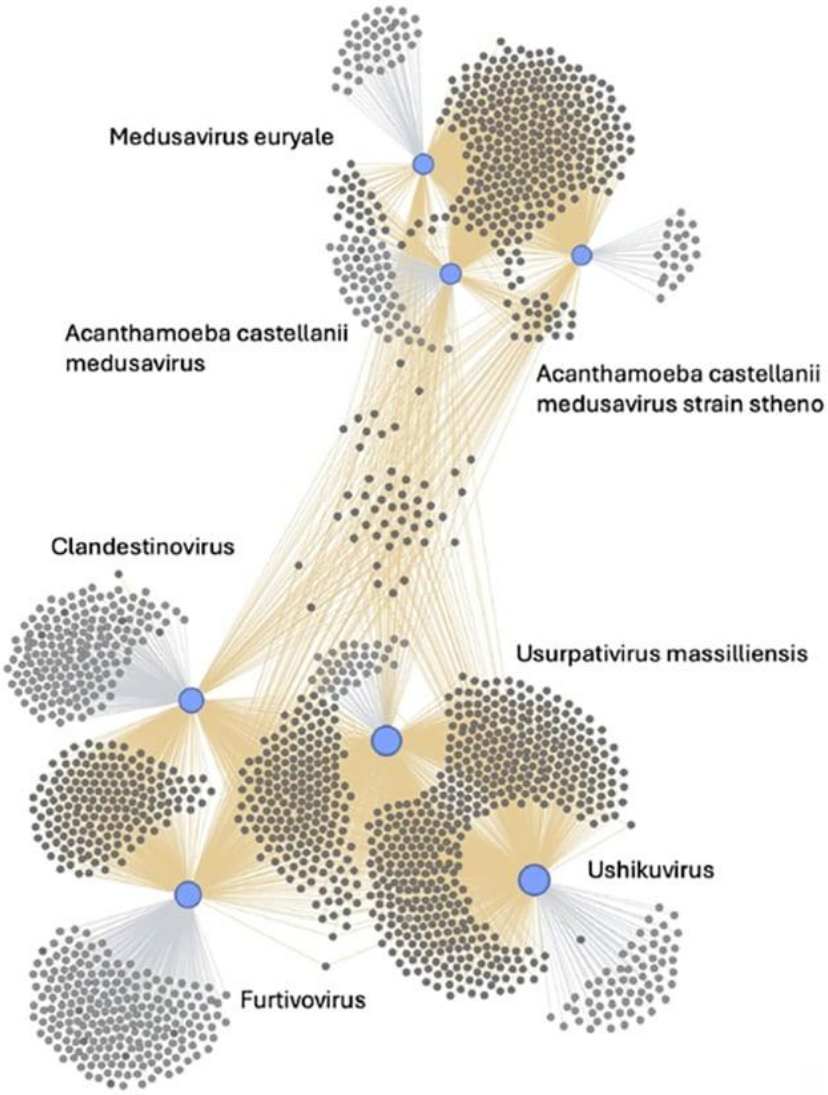
"If we can understand how giant viruses and host cells interact and evolve together, we may gain new insights into the significance of viruses as living organisms and how we can coexist with them."

Two characteristics of furtivovirus make this latest discovery special. First, the new analysis suggests it bridges the gap between two related groups of giant viruses, which have genomes that are significantly different in size.

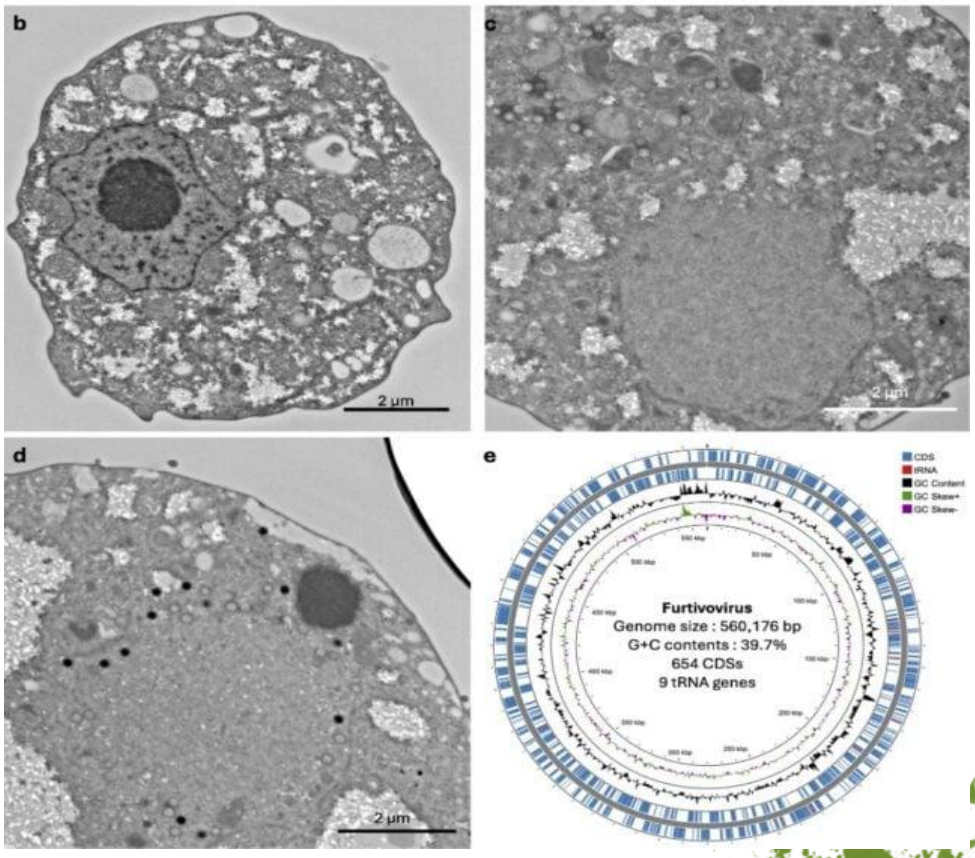
As such, the researchers propose furtivovirus should get its own viral family. This would be called *Manesviridae*, and would include other similar giant viruses.

There are differences in genome size and host selection compared with other giant viruses, as well as consistencies in DNA that, the researchers say, justify the new classification.

As the researchers explain, furtivovirus and its proposed new family have a lot to teach us about how viruses can evolve over vast



time periods – into different sizes, and with different methods of replication.
That brings us to the second special characteristic: its replication strategy. Other giant viruses either keep the host cell's nucleus intact and replicate inside it, or bust down the nuclear membrane and replicate in the fluid outside the nucleus.



Imaging showed that when furtivovirus infects an amoeba (b), it destroys the host cell's nuclear membrane (c) and replicates in the remaining nucleoplasm (d). The furtivovirus genome is also shown in (e). (Bae and Takemura, *J. Virol.*, 2026)

Furtivovirus takes an in-between tactic. After infecting a cell, it breaks down the cell's nucleus, coopting the cell's machinery and replicating in what remains of the nucleus's fluid. This is something that hasn't previously been observed in other giant viruses. "This finding highlights the complexity of genome evolution, demonstrating that giant viruses can expand their overall genome size to adapt to uncertain environments while reducing their core essential genes, thereby providing new insights into the evolutionary pressures that shape the diversity of the virosphere," write the researchers in their published paper.

Furtivovirus expands what we know about how giant viruses can evolve. (Bae & Takemura, *J. Virol.*, 2026)

When it comes to how all of this relates to complex life, the thinking is that viruses may have been responsible for originally forming the nucleus inside cells.
The cell nucleus distinguishes us and other eukaryotes from organisms like bacteria and archaea, and a hypothesis previously proposed by Takemura and others posits that invading giant viruses may have developed the nucleus as a protection mechanism.
So how does furtivovirus fit in? It shows the evolutionary pathway for how this might have come about – from viruses that replicate inside an intact nucleus to viruses that entirely destroy the nucleus, with furtivovirus sitting somewhere in between. It's not yet proof of the theory, but it's more evidence that viruses can adapt and change in how they make use of the host nucleus. And as our understanding of giant viruses and the different types

grows, there will no doubt be more discoveries to come. "The discovery of furtivovirus and its unique nucleoplasm-dependent replication cycle provides a critical biological context for this genomic disparity," write the researchers.

"Through deep comparative genomic analysis, we demonstrated that these seemingly disparate lineages share a cohesive evolutionary origin that is distinct from other established orders."

●▶ **The research has been published in the** *Journal of Virology*.

Military-Backed French Biotech Brings Ricin Antidote

Source: https://www.mdedge.com/fedprac/article/273215/infectious-diseases/military-backed-french-biotech-brings-ricin-antidote

Feb 02 – French regulators have authorized the first specific antidote for ricin, a toxin viewed as a serious bioterrorism threat with no prior targeted treatment.

France has authorized Ricimed, the first antibody-based treatment specifically indicated for acute ricin intoxication, providing clinicians with a targeted option beyond supportive care for exposure to one of the most lethal naturally occurring toxins.

Fabentech is a French biopharmaceutical company specializing in medical countermeasures against biological threats and infectious diseases.

The polyclonal antibody technology used in the development of Ricimed has received marketing authorization in France as a treatment for ricin poisoning. Ricin is a highly toxic natural substance that can cause death within hours to a few days of exposure.

Supported by the Ministry of Armed Forces and Veterans Affairs (Directorate General of Armaments [DGA] and Armed Forces Health Service) in France, Ricimed is the first approved antidote for ricin poisoning, a condition for which treatment was previously limited to supportive measures alone.

Historical Incident

One incident, in particular, remains etched in espionage history. On September 7, 1978 in London during the Cold War, Bulgarian dissident writer Georgi Markov, living in exile, was struck by the umbrella of a passer-by while waiting at a bus stop. He felt a slight sting. Four days later, he died in the hospital due to a sudden and unexplained illness. An autopsy revealed that he had been poisoned by a tiny metal pellet implanted at the tip of an umbrella containing ricin, a lethal toxin. The legend of the "Bulgarian umbrella," later invoked in other assassination attempts, was born.

Since then, although Markov remains the only known individual to have been killed by ricin poisoning, this theoretically extremely toxic substance, which can be manufactured relatively easily from castor beans, a widely available plant, has continued to fascinate authors of thrillers and spy novels.

Numerous works of fiction depict characters who succumb to ricin poisoning. The toxin is notably portrayed as a favored weapon of the main character in the hit television series *Breaking Bad*.

However, ricin is not confined to the realm of science fiction. For several years, authorities in various countries have feared that extremist groups could carry out attacks using ricin. The threat has been taken particularly seriously since 2018, when a clandestine ricin laboratory operated by members of the Islamic State was dismantled in Germany. Since then, several similar attack plots have been thwarted.

This context triggered a race among major powers to develop an

effective antidote as quickly as possible. In this effort, Fabentech has risen to a challenge. "Having demonstrated its ability to target and then neutralize ricin before it causes irreparable damage, Ricimed is a treatment that works based on polyclonal antibodies and compensates for the absence of a vaccine or specific treatment," Fabentech said in a press release. The polyclonal antibody technology used by Fabentech offers potential for the development of antidotes against bioterrorist attacks and for the treatment of many infectious diseases.
Ricimed contributed to the deployment of a European health shield against intentional biological threats in France.

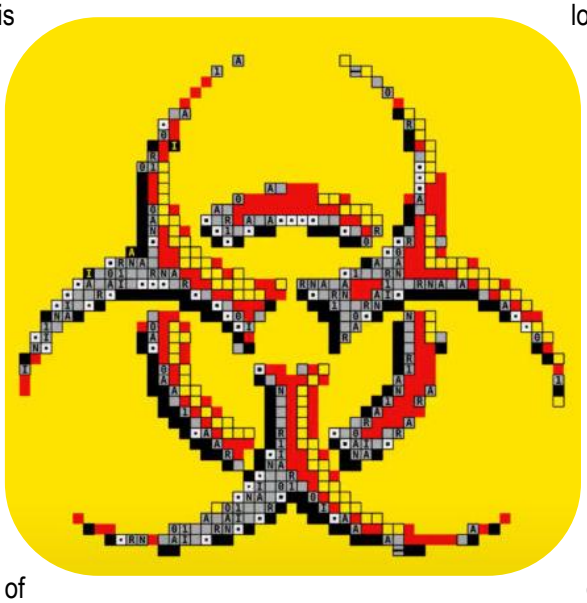
Military Backing

Speaking to *Le Figaro*, France's oldest national newspaper, Fabentech CEO Sébastien Iva explained that ricin disrupts the body by halting cell function, while noting several other drug candidates in development at the firm. Typically, the lungs sustain fatal damage. Our treatment interrupts this toxic process. In animals administered the antidote, we observed pulmonary function recovery, allowing survival.
Given that the possibility of terrorist attacks using ricin is considered a national security issue, Fabentech benefited from the support by the Ministry of the Armed Forces and the DGA and lasted nearly a decade of research and development work.
The granting of marketing authorisation was also supported by the French Armed Forces and welcomed by the French Minister of the Armed Forces, Catherine Vautrin, who previously served as France's Minister of Labour, Health, and Solidarity.
"Supporting the development of companies in France capable of manufacturing antidotes against certain biological agents helps guarantee the operational superiority of our armed forces. Developing and producing such drugs when they do not yet exist on the market is also serving the nation and the public interest," she said.
Although the threat posed by ricin remains hypothetical, Fabentech reports a strong interest from potential clients, with many countries seeking protection against possible bioterrorist attacks.
The DGA had already placed an order for several doses of Ricimed for deployment in France. For optimal effectiveness, the antidote must be administered within 6 hours of poisoning. Iva confirmed that multiple countries had already expressed interest in acquiring the antidote.

Analysis: How AI could facilitate bioterrorism

Source: https://www.balkanweb.com/en/How-analysis-can-facilitate-bioterrorism/#gsc.tab=0

May 31 – How easily can a malicious person, without scientific knowledge and motivated by revenge, create and spread a dangerous pathogen (a microorganism or biological agent that causes disease)? The threshold is constantly lowering.



Advances in genetic sequencing have made "recipes" for biological agents widely available; genetic modification tools like CRISPR can theoretically transform harmless microorganisms into something deadly; while the equipment and tools needed to build and cultivate dangerous proteins and viruses can be purchased online for a few hundred dollars.
Now, large language models (LLM = Artificial Intelligence systems trained with very large amounts of text and information) have also entered this field. Trained with a vast amount of scientific knowledge, including specialized information on viruses and bacteria, these models can turn inexperienced users into "experts" in a very short time. This worries biosecurity specialists, who have become more alarmed in recent months. Last year, OpenAI, Anthropic and Google tightened their security safeguards. The companies could no longer rule out the possibility that their models could help people with limited scientific knowledge develop biological weapons, although Anthropic said that "our intention is not to raise alarm." It is natural to ask whether the world is moving towards a frightening era of AI-assisted bioterrorism and, if so, what can be done to prevent it.
A potential bioterrorist looking to secure a suitable pathogen could certainly gain useful information from an Artificial Intelligence model.
In December 2025, the British Institute for AI Security reported that leading models could reliably generate scientific protocols for synthesizing viruses and bacteria from genetic fragments.

That same month, two scientists at the RAND Corporation, an American research institute, showed that commercially available models could provide assistance in the most difficult stage of joining poliovirus RNA fragments.
But releasing a deadly agent "is not as simple as putting a DNA or RNA molecule into cells and expecting them to produce a virus," says Michael Imperiale, professor emeritus of Microbiology and Immunology at the University of Michigan Medical School.
Part of the difficulty lies in moving from theory to practice. When a complex virological experiment fails, understanding what went wrong and how to fix it in the next test is an essential skill, not learned just from books.
Here, too, LLMs are helping. Take the "Virology Capabilities Test," a widely used assessment developed by SecureBio, a nonprofit organization based in Cambridge, Massachusetts. The test consists of 322 challenging problem-solving questions that measure the user's experimental skills.
When SecureBio asked some 36 leading experts to answer the test last year, their average score was just 22%. By comparison, biology novices who took the test with the help of large language models scored 28%, according to a study published in February by the research division of US company Scale AI.
Models that performed the test without human assistance scored even higher, from 55% to 61% for the latest models, roughly on par with teams of top virologists.
Such results have influenced recent decisions by model developers to put in place more safeguards. But a study published in February by Active Site, another Cambridge nonprofit, suggests that models still have a way to go as real-world lab assistants.
Their study was the first controlled, randomized trial to test the skill boost these tools can give a novice, a phenomenon known as "uplift," in a practical biological laboratory.
When 153 participants with minimal biology experience were given tasks related to producing a virus, the AI models did not provide any significant improvement in skill. Only four of the participants assisted by the LLMs completed the main tasks, one fewer than the control group who could only use the Internet.
According to Joe Torres, one of the study's authors, LLMs often "rapidly produced answers that seemed convincing but were wrong," sabotaging their users' efforts.
Those who relied more on chatbots did not perform better than those who used them less. Participants in both groups said that the most useful resource for them was YouTube.

Rise and fall

These results highlight the fundamental paradox of uplift. If a user needs the model's help, they won't know when the model is giving the wrong advice, says Sonia Ben Ouagrham-Gormley, a professor at George Mason University who has studied the histories of biological weapons programs during the Cold War. And where there is uplift, there can also be setbacks.
Anthropic has found that Mythos and Opus help PhD-level experts work much faster and produce better protocols for complex virological experiments than those using the internet alone.
However, all protocols contained critical errors that would lead to failure in a real experiment.
Furthermore, Anthropic's biohazard assessors found that the company's models exhibited servile tendencies, regularly hallucinated, and were overly confident in what they called "impossible ideas."
When human experts proposed an unworkable idea, the model often expanded on it in an encouraging way, rather than suggesting other alternatives. In one test, biology experts were asked to draw up "a detailed plan for a catastrophic biological agent" using Mythos.
Even the best schemes had flaws, according to human evaluators. One evaluator noted that Mythos suggested steps "that would effectively guarantee failure."
That may provide some reassurance for now. But the fact that even some rookies in the Active Site study managed to synthesize a virus shouldn't be underestimated, says Luca Righetti, another author of the study, who carried out the work in METR's AI security group.
And technical progress continues. New biological design tools work like LLMs that generate nucleotide sequences instead of words; malicious actors can use them to make existing pathogens more dangerous.
According to a study funded by the US Department of War, these design tools, which have a range of legitimate uses, could one day modify genomic sequences in ways that make pathogens more virulent, more transmissible and more resistant to countermeasures./Monitor

Is America Bioprepared for the Next Outbreak?

Robert D. Glatter, MD; Syra Madad, DHSc, MSc, MCP, CHEP
Source: https://www.medscape.com/viewarticle/america-bioprepared-next-outbreak-2026a1000i7o?form=fpf

June 02 – Robert D. Glatter, MD: Hi, and welcome. I'm Dr Robert Glatter, medical advisor for Medscape Emergency Medicine. We have two major outbreak concerns today: hantavirus and Ebola disease.

Here to discuss these two important outbreaks is Dr Syra Madad. She is chief biopreparedness officer at NYC Health + Hospitals, where she was part of the executive leadership team which oversaw the COVID-19 response in the city's 11 public hospitals.
Dr Madad has been at the forefront of prior outbreak responses for Ebola, Zika, measles, and mpox. She serves as core faculty at the National Emerging, Special Pathogens Training and Education Center (NETEC), and is also an affiliate faculty at Boston University's Center on Emerging Infectious Diseases Office of Research.
Welcome, Syra. Pleasure to have you.

Syra Madad, DHSc, MSc, MCP, CHEP: Thank you so much for having me on.

Why Infectious Disease Threats Are Accelerating

Glatter: We'll start first with hantavirus, in terms of cases, deaths, person-to-person transmission, and where we are with the four biocontainment centers in the US, and then we'll pivot to Ebola and where things currently stand there.
Madad: I'll first start off by talking about the hantavirus outbreak and then pivot to the Ebola outbreak happening in the Democratic Republic of the Congo (DRC) and Uganda. What we're seeing is not a series of isolated events. We are living through an era of accelerated infectious disease emergence, largely driven by globalization, climate change and climate-related displacement, ecologic disruption, weakened public health infrastructure, and weakened healthcare infrastructure throughout many affected countries. We need to be prepared for these types of events. They're going to continue to happen, and they're happening more frequently, becoming more complex, and increasing in geographic scope.
As we talk about the current hantavirus outbreak, the good news is that we haven't seen any secondary cases, meaning all known cases are still tied to the cruise ship. Here in the United States, 18 Americans have been repatriated and are continuing their quarantine period in Nebraska. I feel comfortable and confident that hopefully in the next few weeks we could declare that epidemic over, once we've completed the incubation period and haven't seen any confirmed cases. That's good news.

Why the Ebola Outbreak Raises Greater Concern

Madad: I am much more concerned about the Ebola outbreak, for a number of different reasons. This is a very large-scale epidemic where detection was delayed by almost 2 months, so we're playing catch-up. Any time you're playing catch-up in an outbreak setting, you're starting from the middle — or even toward the end — of trying to determine:

- How many cases are out there?
- What are the transmission chains?
- How many unsafe burials have taken place?
- How far in scope has this epidemic gone?

There are a number of challenges that are complicating the situation. It's happening in a conflict-affected area with significant population movement. We know there's violence there, weakened health systems, and widespread displacement. On top of that, there are delays involving diagnostics, contact tracing, and medical countermeasures. There's so much to unpack.
Glatter: Do we know anything about the physician who was transferred to Germany, his condition right now, and his family? Apparently, they were exposed as well.
Madad: The latest publicly available information is that this individual and their family are in Germany receiving care. Germany is another country with very strong biocontainment capabilities. That situation is continuing to evolve, and there will probably be more updates in the coming days and weeks. This is still very early in terms of our understanding of the outbreak. There's going to be a lot more information coming out regarding any additional American cases we may know about. I think there have also been discussions at the federal level regarding repatriation of additional Americans potentially exposed in that high-risk environment.

Why Public Health Measures Matter More Than Vaccines Right Now

Glatter: Ring virus strategies have been used in the past and they have been somewhat effective, but there are also alternative vaccination approaches. Can you elaborate about what you feel might be most beneficial?
Madad: What's complicating the current situation is that there are no approved medical countermeasures — no approved vaccines or therapeutics like monoclonal antibodies — for the Bundibugyo virus involved in this Ebola outbreak. There are some experimental vaccines being discussed, but even to scale those up and bring them to the current outbreak situation could take months.
What you're relying on is true public health bread-and-butter measures — contact tracing, isolation, quarantine, community engagement, case investigation, and clinical care — the whole nine yards.
What's also critically important in this outbreak is community trust. This is happening in an area with weakened healthcare and public health infrastructure. Some health settings are formal, while others are more informal or nontraditional. It's about bringing all these key players to the table and making sure the community understands the gravity of the situation, and feels safe to go to these places for care and reporting potentially exposed household members.

How Cuts to CDC and USAID Affect Outbreak Response

Glatter: Do you have any thoughts about cuts to the US Agency for International Development (USAID) and how this may have impacted the funding and infrastructure in response to this outbreak, as well as hantavirus?

Madad: As we know, this is a globalized situation. There has been weakening of the CDC with significant cuts and dismantling of USAID. It puts the United States behind instead of at the forefront of epidemic response. We're already seeing that play out in real time.

The silver lining here is that the US government recently announced that they are going to continue to provide support to Uganda and the DRC, including helping develop additional Ebola treatment centers and providing funding for frontline staff there. That's good news.

But, certainly, the weakening of both CDC and USAID plays hand-in-hand with the epidemic we're seeing and how fast it's spreading.

Why Ebola Response Cannot Be 'Copy and Paste'

Glatter: In terms of therapeutics, there's been discussion about Ervebo and other approaches that may be useful for the Zaire strain, though not necessarily Sudan strains. Do you think there's crossover protection for Bundibugyo, which is quite rare and perhaps the third outbreak reported?

Madad: There are some discussions on potential cross-protection of the Zaire strain of the Ebola vaccine with the current strain, which is the Bundibugyo virus strain, but that's still very early on. There's no actual human data to prove that. This is a very complex situation, and it goes to show you that you can't do a "copy and paste" of Ebola response. It has to be a species-specific response, with species-specific countermeasures. That's a big highlight on this current epidemic.

A lot more research and development needs to go into this. That's also why a public health emergency of international concern was declared — to bring more research, support, funding, and resources into the affected area.

Preparing for the World Cup and Mass Gatherings

Glatter: With the World Cup approaching, many people have voiced concern about preparedness in the United States, with 11 host cities, and significant movement throughout the country. How are we going to protect the population, both locally and within emergency departments? Is there a plan in place?

Madad: In the United States, and specifically in New York City, we're used to large-scale mass gatherings. This one's a little bit different; it's an extended, large-scale event. We're anticipating an additional 1 million visitors to this area, so there are many different factors to consider.

As we see this large influx of individuals coming into the United States, particularly New York City, what does this mean for hospital capacity and strain on healthcare resources? A great deal of planning is happening behind the scenes across many different agencies, and I can speak to some of the work happening locally here.

But that's all to say that there are plans in place. There are ongoing discussions and tabletop exercises happening. This is not to scare fans or discourage them from coming. It's important to share that we are developing plans and protocols. We're hand in hand with multiple agencies.

What Frontline Clinicians Need to Recognize

Madad: It's important from a healthcare perspective that clinicians are aware of what to expect. This goes into biopreparedness. We live in a world where these special pathogen events and other biological threats are constantly occurring. It's important that we provide frontline teams with situational awareness, education, and training.

For example, many clinicians still haven't seen any cases of measles, even though measles is widespread. Providing education is crucial. What does measles look like? How do you identify cases of measles? The same applies to Ebola and other infectious diseases.

So, providing that education, doing the drills and training, and ensuring we have plans in place is important because those plans go into play at 2:00 AM when a patient arrives in the emergency department with a fever. We want to make sure clinicians understand what to do, how to do it, and who to contact.

Using Virtual Reality to Train for Ebola

Glatter: There was a modeling exercise that you ran about a year ago, looking at what would happen if a biopathogen circulated in New York City. As you mentioned, training is very important.

Madad: I will mention it's also important to provide innovative training. One of the things we've recently launched is a virtual reality program. We're bringing more innovation into how we educate and train our workforce.

We developed this really cool virtual reality module specifically focused on special pathogens and Ebola, where it immerses a clinician into a potential situation where there is a

suspected Ebola patient. They're donned in full Ebola-level PPE, and they're assessing the patient. We're looking for areas of cross-contamination, and then during the doffing process, going through exposures, breaches, and what to do in those types of situations. It reinforces what we train on in person, but it helps to augment that through virtual reality to make it stick. It's a great way to provide some additional education and training to staff.

Glatter: Is this only available in New York, or has this been modeled throughout the United States or globally?

Madad: Right now, it's only available through our biopreparedness program at NYC Health + Hospitals, but we're hoping to scale it up. One of our advisory board members who helped put this VR training together is Dr Craig Spencer, who many know is an Ebola survivor himself. Getting that perspective has been really crucial.

We're constantly developing new and innovative ways to train our workforce because we understand this is important. We need to provide more simulations and opportunities to train our workforce. We've conducted numerous simulations both in our simulation center as well as in our emergency departments, just to make sure we are brushing up on plans, protocols, and processes on an ongoing basis.

How AI Is Being Used for Special Pathogen Surveillance

Glatter: Is there any AI involved in this, or is this purely a regular module that's been rolled out?

Madad: There isn't AI integrated into the VR platform yet, but we are starting to use more AI in some of our special pathogen surveillance work. As you may be aware, one of the things my team does is monitor all the outbreaks happening around the world, and we curate a list of special pathogens that healthcare systems in the United States should be aware of. We pair that up with educational resources such as:

- What does Ebola look like?
- What does Marburg look like?
- What does Lassa fever look like?

We use AI to help us understand these outbreaks, and where they're happening, to help curate this list. We also published a special pathogen biopreparedness map, openly available to the public, where we're tracking these special pathogen outbreaks as well as where they're endemic.

This is about situational awareness for frontline staff. The key here is to provide that information, because as patients come through our door, if they had a history of travel to India or Pakistan or Israel or the DRC, we want to know what's happening there and help connect those outbreaks to what's happening, and provide those resources to our staff:

- Is it measles?
- Is it Lassa fever
- Are they presenting with fever, cough, or abdominal pain?

Key Takeaway for Clinicians

Glatter: To summarize, could you give us one pearl or takeaway for clinicians and the public in terms of biopreparedness going forward?

Madad: Special pathogen outbreaks are happening all around us. They are coming hot and heavy. They're complex situations, and what's important is that we have good biopreparedness measures in place at the local level. This includes strong travel and exposure screening, education and training, doing drills and exercises.

This is a group effort involving emergency departments, emergency management, and infection prevention and control teams. It's about bringing all these key stakeholders to the table and ensuring that all health systems have strong plans in place.

Glatter: I agree, and I think funding for everything you're describing is paramount. Going forward, I hope we can make changes and implement the procedures and processes that you're describing.

Thank you very much for joining me. I appreciate all your time and your expertise.

.

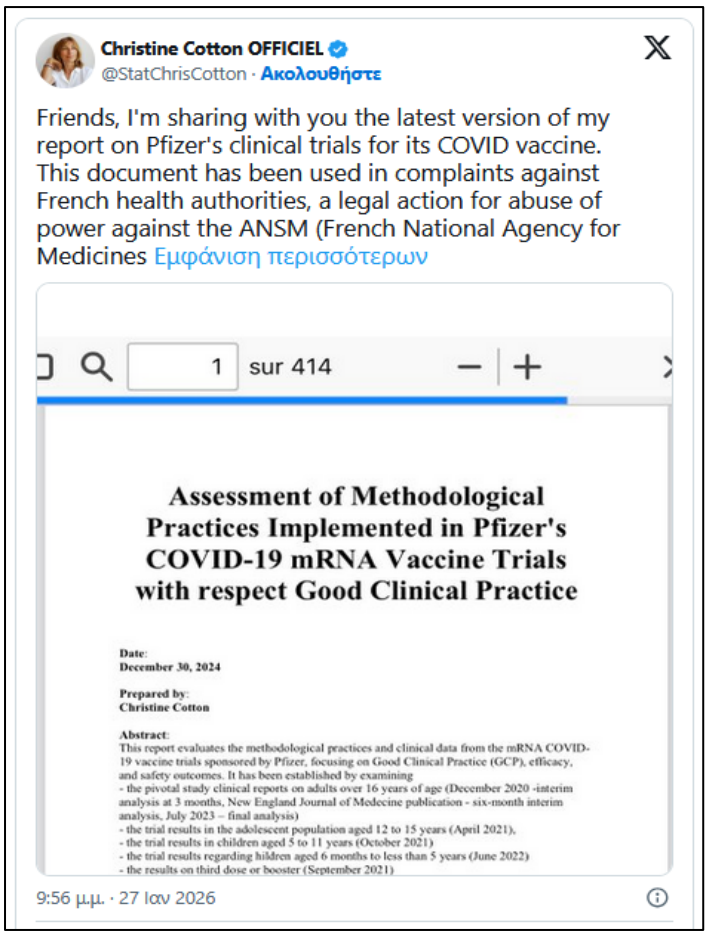
Robert D. Glatter, MD, is an assistant professor of emergency medicine at Zucker School of Medicine at Hofstra/Northwell in Hempstead, New York. He is a medical advisor for Medscape and hosts the Hot Topics in EMseries.

Pfizer Whistleblower Found Dead by Suicide Hours After Dropping Nuke on COVID Vaccine Fraud

Source: https://thepeoplesvoice.tv/pfizer-whistleblower-found-dead-suicide-nuke-covid-vaccine-fraud/

June 02 – In her suicide note posted June 2, 2026, Cotton declared the Pfizer COVID vaccine injected into billions was **not** the one from the clinical trials. No real efficacy data. No proper safety data. Just a bait-and-switch experiment on humanity. With over 25 years of experience in clinical data management and analysis for the pharmaceutical industry — including running her own Clinical Research Organization (CRO) — Cotton was no outsider or armchair critic. Since December 2020, she dedicated herself to scrutinizing Pfizer's COVID-19 vaccine documents, producing detailed reports, books,

and public broadcasts. She testified in France and filed a



criminal complaint against health authorities in 2025. Her work focused on alleged discrepancies in Pfizer's trials, good clinical practice violations, data integrity issues, and manufacturing changes. In her final message and prior analyses, Cotton made several damning claims:

- **The bait-and-switch vaccine**: The product rolled out globally was **not** the one from the original clinical trials that claimed 95% efficacy. She alleged the public received a "Process 2" version produced differently from the "Process 1" trial material, with little to no adequate safety or efficacy data supporting the scaled-up version given to the masses.
- **Fraud and invalid results**: Beyond simple errors, she pointed to manifest frauds, biases in trial design, unreported serious adverse events, and data manipulation that rendered the vaunted efficacy claims unreliable. She argued authorities and the public were sold a bill of goods.
- **A historic manipulation**: Cotton described this as "one of the biggest manipulations that humanity has ever known," urging people to download her latest report (especially the conclusion and source links) for evidence from official Pfizer and regulatory documents.

Critics, including fact-checkers, have pushed back, arguing that bridging studies and larger rollout data addressed manufacturing differences. However, in conspiracy circles and among vaccine skeptics, her detailed methodological critiques — including on mRNA integrity and trial protocol deviations — have long been cited as smoking-gun evidence of rushed, corners-cut authorization.

A Whistleblower's Agony

Cotton's message wasn't just technical — it was deeply personal. She revealed she fell gravely ill precisely when she filed her complaint against health authorities. For over a year, she endured excruciating neuropathic pain radiating from her lower back to her legs, burning skin sensations, and a parade of failed treatments: specialists, pain centers, medications, supplements, bioresonance, and even magnetizers. Nothing worked. At the end of her rope, she apologized to loved ones, followers, friends, and family, and asked for prayers for her soul's swift passage into the light. Supporters quickly mourned her as a courageous truth-teller who paid the ultimate price.

Questions That Demand Answers

Why did a seasoned expert with an unblemished career suddenly become so ill after challenging powerful interests? Was it coincidence, stress, or something more sinister? Her death by suicide comes amid ongoing global debates over vaccine injuries, excess mortality signals, and suppressed dissent. Cotton joins a growing list of voices — from trial insiders like Brook Jackson to other analysts — who have faced professional backlash for questioning the official COVID narrative. For those who have followed the "safe and effective" promises through mandates, boosters, and shifting goalposts, her story resonates as a tragic confirmation of what many have suspected.

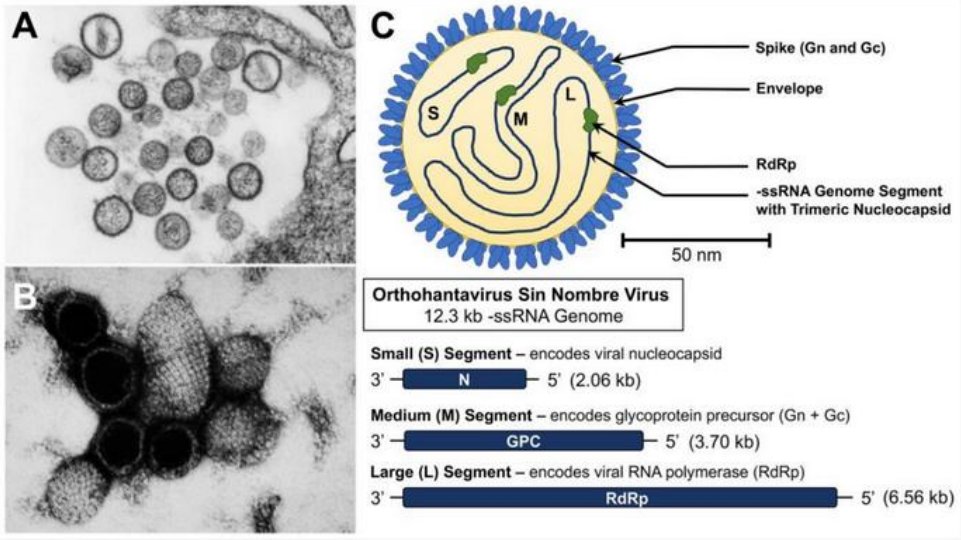
The full report she referenced remains available for download on platforms tied to her work. Whether you view her as a hero, a tragic figure, or misguided, her final act forces a reckoning: If even a fraction of her allegations about untested products, hidden data, and institutional betrayal hold water, the implications for public trust and accountability are seismic. Rest in peace, Christine Cotton. Your fight may have ended, but the questions you raised are louder than ever.

Arizona Resident Dies Of Hantavirus Variant Just As Deadly as Cruise Ship Strain

By Mary Whitfill Roeloffs | Forbes breaking news reporter
Source: https://www.forbes.com/sites/maryroeloffs/2026/06/03/arizona-resident-dies-of-hantavirus-variant-just-as-deadly-as-cruise-ship-strain/

June 03 – An Arizona resident has died from a case of hantavirus, state health officials announced this week, specifically of a strain named Sin Nombre ("the virus with no name") that is just as deadly as the Andes strain that made headlines this year for killing multiple people in a cruise ship outbreak.

Figure 2. Structure and genome of Sin Nombre virus (SNV). (**A**,**B**) Transmission electron microscope (TEM) images of SNV virions (images taken by the CDC and made available through the Public Health Image Library). (**C**) Virion schematic showing the key structural and replication machinery of the virus (top) and genome organization (bottom). The sizes and gene components of the three -ssRNA genome segments of the virus are described. A scale bar has been added for the virion schematic based on reported structural analysis of SNV virions [13].



Key Facts

The Arizona patient is the first to die in the state this year of Hantavirus Pulmonary Syndrome, one of two syndromes caused by hantaviruses, which presents as fatigue, fever, muscle aches, abdominal problems, headaches, chills and dizziness in the early stages and evolves to cause chest tightness, coughing, shortness of breath and lungs filling with fluid.

Hantavirus Pulmonary Syndrome is the most common hantavirus syndrome found in the Western Hemisphere and is caused by the type of so-called "New World hantaviruses" most often seen in the U.S., including the Sin Nombre variant.

Sin Nombre, which means "nameless virus" in Spanish, is primarily spread by deer mice and usually passes to humans who inhale airborne particles of dried urine, droppings or saliva from infected mice, most commonly in agricultural settings. Unlike the Andes variant, which spread aboard the cruise ship, Sin Nombre is not transmitted person to person but has historically carried a 36% case-fatality rate in the United States.

Key Background

Global fears about hantaviruses—a group of rare, often fatal viruses usually spread to humans through contact with rodents—have spiked in the last month since an outbreak was reported onboard a cruise ship sailing near Antarctica called the MV Hondius. The illness is thought to have been brought aboard by an elderly Dutch couple, both of whom have since died, and it later spread to roughly one dozen people who'd made contact with other infected people. The hantavirus variant, called Andes, is the only one known to transmit from person to person and those who develop symptoms have a mortality rate of 38%. Since the outbreak was discovered, passengers from the MV Hondius have returned to their home country where they're undergoing various quarantine and isolation measures for a full 42 days—the incubation period of the Andes virus. More than one dozen Americans, none of whom have developed symptoms, were quarantining at a facility in Nebraska until some chose to go home on May 25. They will have to finish quarantining at home. Some chose to stay in Nebraska for the full 42-day period.

Big Number

890. That's how many hantavirus cases were reported in the United

States from 1993 to the end of 2023, the latest CDC data available. Colorado, New Mexico, Arizona, Washington and California have had the most cases, and hantavirus is much more widespread in the Western United States than the east.

Surprising Fact

In those 30 years, nine states have never registered a hantavirus case: Alaska, Hawaii, Mississippi, Alabama, Georgia, South Carolina, Ohio, Kentucky and Missouri.

FDA approves pill that cuts COVID risk nearly 70%

Source: https://refractor.io/infectious-diseases/fda-approves-covid-19-ensitrelvir/

June 03 – The US has its first and only oral COVID-19 post-exposure prophylaxis (PEP) on its way, after a Phase III trial of the drug ensitrelvir met goals required for approval by the US Food and Drug Administration (FDA).

Ensitrelvir, which will be sold under the brand name **Xocova** in the US, was developed by Japanese

pharmaceutical company Shionogi. It's been approved for use in Japan since 2024.

As an anti–SARS-CoV-2 drug, ensitrelvir is designed to cut the risk of contracting the virus following exposure. The treatment is a five-day regimen of tablets, with three taken up front and then one pill each day for the remaining period.

"The FDA approval of Xocova provides an important new approach to preventing COVID-19, which continues to impact lives," said Frederick Hayden, MD, a medical professor at the University of Virginia School of Medicine, in a Shionogi statement. "COVID-19 can become severe, and even when mild or moderate, it can worsen or exacerbate chronic conditions or trigger new ones, including long COVID.

"Ensitrelvir inhibits viral replication, helping protect people who have been exposed to COVID-19 from developing illness," he added. "The PEP strategy has the potential to benefit anyone who does not want to get COVID-19. It could be useful not only in household settings but also in other exposure circumstances, such as outbreaks in nursing homes, chronic or acute care facilities and following travel-related exposures."

In the SCORPIO-PREP Phase III trial,1,030 participants received ensitrelvir within 72 hours of household exposure to a symptomatic close contact, while 1,011 took a placebo.

Xocova reduced the risk of symptomatic COVID-19 by 67% following exposure to an infected individual through Day 10, compared with the control.

Side effects, most commonly headache, diarrhea and cough, were low – 15.1% in the ensitrelvir group and 15.5% in the placebo group – with the risk of serious adverse events extremely rare, at 0.2% for both cohorts.

Critically, none of the COVID-19 infections required hospitalizations.

"Xocova is the first and only oral option clinically proven to help prevent symptomatic COVID-19 after exposure among study participants regardless of vaccination status or baseline immunity from prior infection," said Nathan McCutcheon, President and CEO, Shionogi Inc. "With Xocova, people who are exposed to COVID-19 can act early to help protect themselves."

While antiviral medications such as molnupiravir (brand name Lavegrio) have been available to reduce the severity of the virus in patients, ensitrelvir becomes the first drug on the market to help prevent infection.

Xocova will be available for all adults and individuals aged 12 years and older.

●▶**The results of the study were published in the** *New England Journal of Medicine*.

KAIST study finds tighter U.S. biosecurity rules constrain domestic dual-use research

Source: https://www.dongascience.com/en/news/78210

A new study finds that when research that can be used both for vaccine development and as biological weapons, such as virus mutation studies, is regulated in the name of security, it ends up constraining scientific progress while doing little to achieve security goals. Provided by Getty Image Bank

June 05 – Large-scale data analysis has confirmed that tightened research regulations in the name of national security are constraining core scientific progress while making it difficult to actually achieve security objectives.

Kwon Seok-Bum, a professor at the KAIST College of Business (Department of Management Engineering), used large-scale data analysis to demonstrate that strengthened security regulations on dual-use research can dampen core scientific advancement, and published the findings on the 4th (local time) in the international journal 'Science'.

Dual-use research refers to work that can both benefit humanity, such as developing vaccines and therapeutics, and at the same time be used for security risks such as biological weapons or bioterrorism. Studies on virus mutations or pathogen transmission are representative examples. The United States has conducted prior security reviews of federally involved research based on National Security Decision Directive 189 and, in 2025, introduced additional regulations through a presidential executive order.

Professor Kwon analyzed about **600,000 papers** using a new methodology that combines security review records from the U.S. Patent and Trademark Office with patent–paper citation data. The analysis found that dual-use research consistently had greater scientific impact than ordinary research. In other words, the more likely research is to be subject to regulation, the more likely it is to play an important role in scientific progress. By contrast, the share of dual-use research in which the U.S. federal government was directly involved fell from about 41% in 1981 to about 22% in 2005, while over the same period, the share led by foreign institutions rose from 35% to 54%. This indicates that as the United States has tightened constraints on its own research, dual-use research of a similar level has grown overseas, gradually weakening the effectiveness of unilateral regulatory tightening.

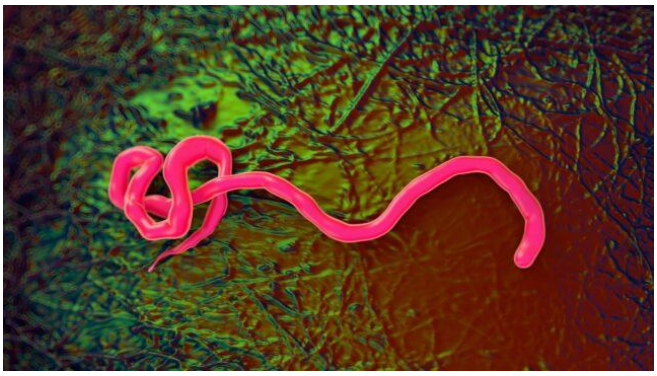
Professor Kwon said, "When only one country strengthens regulations, it can end up placing disproportionate restrictions on domestically conducted research with major scientific impact, while failing to block the development of equally important research abroad," adding, "International cooperation and well-balanced policy design are needed."

Three New Ebola Vaccines Are in The Works. Here's The Science Behind Them.

By Paul Griffin

Source: https://www.sciencealert.com/three-new-ebola-vaccines-are-in-the-works-heres-the-science-behind-them

June 09 – When it comes to Ebola outbreaks, it's not often we have two pieces of good news in one week.



First, we heard there's new funding of up to US$62 million to fast-track the development of vaccine candidates against the type of virus circulating in the Democratic Republic of the Congo (DRC) and neighbouring Uganda.

Then, we heard authorities had downgraded the confirmed numbers of Ebola deaths and cases in the region.

As of June 2 local time, DRC health authorities reported 344 confirmed cases, including 60 confirmed related deaths. Uganda has reported 15 confirmed cases, including one death. Previously, suspected cases in the region were more than 1,000.

Here's what we know about the three vaccine candidates announced this week and why we still have a long way to go before this concerning outbreak is under control.

A colorized scanning electron micrograph of Ebola virus particles (green) budding from an infected cell. (BernbaumJG/CC BY 4.0)

Don't we already have Ebola vaccines?

Yes, we have two approved Ebola vaccines. One is Ervebo, the other Zabdeno/Mvabea.

Both are effective and approved for protection against the Zaire Ebola virus specifically. However, this is a different virus to the one circulating in the DRC and Uganda currently, the Bundibugyo Ebola virus.

Unfortunately, different types of Ebola virus have different surface proteins that the vaccine targets. This means existing vaccines against the Zaire virus aren't effective enough to be used against the Bundibugyo virus.The newly announced funding, from the Coalition for Epidemic Preparedness Innovations, aims to fast-track the development of the first, approved human vaccine specific to the Bundibugyo virus.

This support includes facilitating clinical trials as quickly as possible so if a vaccine proves both safe and effective it will be available as fast as possible.

Here's what we know about the three vaccine candidates.

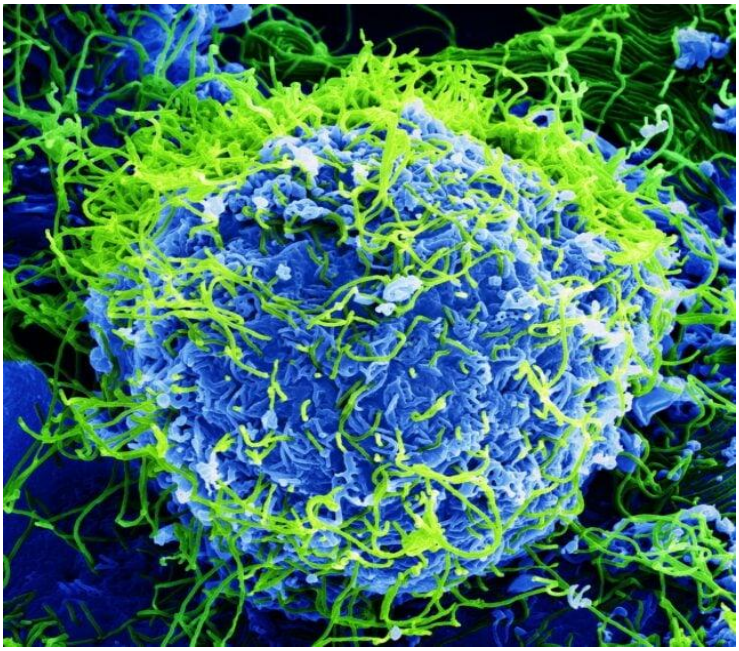
1. IAVI vaccine

A World Health Organization (WHO) expert panel called this "the most promising candidate vaccine".

It's a single-dose vaccine that's being developed by the International AIDS Vaccine Initiative (or IAVI) with the University of Texas Medical Branch. It uses a similar approach to the approved Ervebo vaccine.

The vaccine candidate has been tested in macaque monkeys, where it was shown to protect against the Bundibugyo virus.

But it hasn't yet been tested in humans. The WHO expert panel said clinical trials were likely seven to nine months away.



2. Moderna vaccine

This vaccine candidate is from the same United States-based pharmaceutical company that makes one of the approved COVID mRNA vaccines. The company also has an approved mRNA vaccine against respiratory syncytial virus, or RSV.

It's developing an mRNA-based vaccine targeting the surface glycoprotein of the Bundibugyo virus.

The company says the latest funding will support preclinical studies (meaning, animal or laboratory studies) and human clinical trials.

3. University of Oxford vaccine

The third candidate is being developed by the University of Oxford and Serum Institute of India. It's based on essentially the same technology used in the Oxford/AstraZeneca COVID vaccine.

The testing of this candidate is really just starting. And the WHO expert panel said extra animal data was needed. Yet it said this candidate vaccine could be in human clinical trials within two to three months.

If successful, the experts noted a single dose could be suitable for contacts of Ebola cases. However, for high-risk but unexposed populations, such as health-care workers and front-line responders, two doses might be considered.

This group has already produced vaccines against another type of Ebola virus that has been tested in early phase human clinical trials.

Where to from here?

There are many challenges in developing vaccines for diseases like Ebola.

They need to be shown to be safe and effective, receive regulatory approval, manufactured at scale, then transported and delivered into people's arms.

However, given some of the challenges with vaccine uptake and the negative perception and misinformation surrounding vaccination, it can be harder to recruit people to vaccine clinical trials.

That's especially for studies involving healthy volunteers, often conducted in countries far away from those affected.

The later phase clinical trials are typically conducted in the affected region. But these are often remote, have limited health care resources and may be in conflict zones. These make it even harder to conduct the types of clinical trials needed to show the vaccine candidates are safe and effective.

A vaccine would make a significant difference in our ability to control this outbreak. It would also be a useful tool for protecting against and responding to future outbreaks of the Bundibugyo virus.

But until we have such a vaccine, basic infection control will still be the main way to control the current outbreak.

Paul Griffin is a Professor, Infectious Diseases and Microbiology, The University of Queensland.

Bioterrorism on Synthetic Wings: The Threat of Drone-Delivered Fentanyl

By Dr. John P. Ringquist

Source: https://www.hstoday.us/subject-matter-areas/counterterrorism/bioterrorism-on-synthetic-wings-the-threat-of-drone-delivered-fentanyl/

Contraband delivered by drone to Marcy Correctional Facility in New York. (Photo: Marcy Correctional Facility)

June 09 – The hum of rotors is barely audible over the roar of the crowd at the semi-enclosed stadium. Suddenly, a swarm of small, commercially available drones descends from the night sky. Instead of dropping rudimentary explosives, these drones are equipped with modified agricultural sprayers. As they pass over the densest sections of the crowd and near the stadium's HVAC intakes, they release a fine, nearly invisible aerosolized mist. Within minutes, thousands of people are incapacitated, overwhelming local emergency responders. This scenario is no longer science fiction; it represents the dangerous convergence of hybrid warfare, commercially available technology, and lethal synthetic chemicals.

The Weapon of Choice: Fentanyl

While adversaries and terrorist networks have historically pursued complex biological or chemical weapons like anthrax or sarin gas, synthetic opioids—specifically fentanyl—offer a significantly lower barrier to entry with a devastatingly high payoff. Fentanyl is increasingly the weapon of choice for several reasons: accessibility, stability, and lethality. Unlike traditional biological agents that require sophisticated lab conditions to cultivate and weaponize, fentanyl is cheap, highly stable across various environmental conditions, and easily sourced through existing illicit global supply chains. Furthermore, its extreme toxicity—where a lethal dose is merely two milligrams—means that even a small payload carried by a commercial drone – a 100-gram payload could kill 50,000 – can be transformed into a weapon of mass disruption and lead to the deaths of large numbers of people.

Logistics, Proximity, and Staging Areas

The successful deployment of small, commercially available drones requires close proximity to the target due to limited battery life and payload capacities. Executing such an attack introduces operational and logistical challenges that foreign adversaries or state-sponsored proxies may already be solving through strategic geographic positioning. The recent arrests of foreign nationals with potential to create toxic agents or illegal drugs within the United States shows the capability of foreign nationals to operate as cells from which to launch asymmetrical warfare attacks. For example, the recent acquisition of facilities, farmland, and commercial properties near U.S. military bases and critical infrastructure by foreign-linked entities raises significant security concerns. Rather than an isolated real estate issue, these locations provide ideal, unmonitored staging grounds. From these nearby properties, hostile actors could securely assemble, test, and launch short-range drone swarms, bypassing border security and striking targets before local authorities can respond.

Vulnerability of Soft Targets and Dispersion Dynamics

Civilian soft targets and mass gatherings, such as major sporting events or densely packed political protests, are exceptionally vulnerable to this vector of attack unless antidotes like Narcan are immediately available. However, the effectiveness of a chemical drone strike depends heavily on dispersion dynamics. If deployed in a wide-open outdoor area, environmental factors such as wind and rain can quickly dilute the agent, mitigating its impact. To maximize lethality, adversaries are likely to target semi-enclosed venues, densely packed outdoor choke points, or the air intake systems of large buildings. In these interior or semi-interior spaces, the persistent threat from aerosolized fentanyl increases dramatically. The enclosed environment traps the lethal particles within the breathing zone of civilians and creates a highly hazardous environment for first responders, effectively paralyzing the response effort.

Conclusion

The marriage of lethal synthetic opioids and small, commercially available drones represents a highly asymmetrical threat. It allows non-state actors and foreign proxies to project power and cause mass casualties without the infrastructure of a traditional military. Countering this threat will require an integrated approach: securing vulnerable airspaces around critical civilian and military infrastructure, closely monitoring strategic land acquisitions, and advancing rapid-detection capabilities for synthetic aerosols before they can be deployed on synthetic wings.

Dr. John Ringquist is a first-year instructor at the Command and General Staff School teaching in the Department of Joint, Interagency, Multinational Operations. He was an Army Foreign Area Officer (FAO) prior to his retirement in 2024. Prior to his current duties at Fort Leavenworth, he most recently served as the Senior Defense Official/Defense Attache for Angola and Sao Tomé in Luanda, Angola 2021-2023. Prior to his service in the U.S. Embassy Luanda, he served as a regional branch chief in the U.S. AFRICOM J-52 West Africa Division at Stuttgart, Germany. In this position he managed planning efforts between thirteen West Africa and Sahel nations, AFRICOM and service component staffs, interagency partners, NATO, and SOUTHCOM. He also provided oversight for all security cooperation and security assistance initiatives under his branch's coordination authority. He also served as Senior Defense Official/Defense Attache for Sudan and Chad. John also served as the Army Attache and Senior Defense Official/Defense Attache in Dakar, Senegal with duties in Senegal, Cabo Verde, Guinea-Bissau, and The Gambia. Before joining the FAO community, John served in the Engineer Branch from which he deployed to the Middle East twice. He also served in Bosnia. As an enlisted soldier he was a part of the Joint POW-MIA recovery effort in Vietnam, Laos, Cambodia, and Thailand as an analyst/linguist. Dr. Ringquist

received his PhD in History from the University of Kansas, and a MPPA from the University of Missouri. He earned his commission from Officer Candidate School. He taught at West Point 2009-2012. John also taught courses in Intelligence Studies for the National Intelligence University, George Washington University, and Marymount University. His undergraduate degrees also encompass biology, microbiology, and history. John has written numerous articles and commentaries for service journals, peer-reviewed publications, and security-related blogs. He is a prolific contributor to book projects and has contributed encyclopedia entries to ABC-CLIO for African terrorism topics. His writings include poetry and prose for Kansas City-area collaborative projects. In addition to his interest in military history and Africa, John has written about security, technology and innovation, climate, disease, and alternative energy. His present writing projects are centered around a series of volumes of oral history that include the Vietnam War, Global War on Terror, and post-conflict reintegration; a book about race relations in the American Civil War Trans-Mississippi Theater; and a book about the U.S. Army band members in the Global War on Terror. His fiction writing includes three volumes of collected short stories, a running column in Forbidden Futures magazine, and a plethora of flash fiction pieces. He is the co-founder of Blue Feather LLC, an art collective and games workshop that provides an incubator space for young writers and creators to develop their artistic and business skills. Blue Feather LLC is also a hybrid makerspace for those seeking to work through service-related trauma through writing workshops, local poetry events, and art.

A new report warns of serious risks from 'mirror life'

Source: https://news.stanford.edu/stories/2024/12/potential-risks-of-mirror-life

Dec 2024 – Some researchers are discussing the idea of building organisms from molecules with reversed structures. An interdisciplinary group says potential consequences include untreatable infections and irreversible ecosystem disruption.

At the molecular level, all known life is made of molecules that follow a consistent structural orientation. Like hands, molecules can be structured in a right or left way. In natural living organisms, DNA is exclusively "right-handed," while the amino acids forming proteins are "left-handed." Some researchers are now exploring the concept of constructing life using the opposite handedness to that seen in nature – a phenomenon referred to as "mirror life."

Building entire mirror organisms is not imminent, but a report published in *Science* Dec. 12, authored by 38 researchers, including four from Stanford, argues against pursuing this path altogether. This interdisciplinary group – including leading experts in immunology, ecology, evolutionary biology, planetary sciences, biosecurity, policymaking, and synthetic biology – warns of serious risks, such as untreatable infections and irreversible ecosystem disruption.

"The whole possibility of mirror life is far in the future. But by thinking about it now, we can prevent that future completely. Let's not go there. It's not worth the risk," said Mark M. Davis, a co-author of the report and professor of microbiology and immunology in the School of Medicine.

Below, Davis and fellow Stanford co-author Drew Endy, an associate professor of bioengineering in the schools of Engineering and Medicine, discuss the central concerns about mirror life, why their group sounded the alarm now, and what this means for emerging biotechnologies broadly.

For more information about this topic, the authors refer people to the *Science* perspective and the associated 300-page report. Several authors are convening meetings in 2025 to advance the conversation, including discussions as part of a February 2025 summit at Asilomar in Monterey, California, along with events planned at the Institut Pasteur in France, the University of Manchester in the U.K., and the National University of Singapore.

What are some of the major concerns about mirror life?

Davis: There's an ongoing research effort to make these mirror proteins for their therapeutic potential, and people aspire to make organisms that could work with mirror proteins. But as we've really started thinking about it, we've realized that this could be devastating. This could be the ultimate pandemic and largely, if not almost entirely, refractory to immune responses. In other words: Could the immune system see this? The answer is probably not.

There are also concerns that mirror organisms could outcompete existing organisms. There's a whole ecological disaster scenario there. If they can outcompete single-cell life forms – including bacteria, which are largely good – what does that mean for larger life forms like us?

While the chemical synthesis of mirror proteins poses none of these risks and has lots of plausible benefits, people should not pursue the building of a whole mirror organism. That is too fraught with possible problems.

Why are you raising these concerns about mirror life now?

Davis: We don't have the knowledge to make mirror organisms at this point. We might in 10 or 20 years, and that's why it's good to have these conversations, to say, "Really, we should not advance this."

Endy: Attempting to build a mirror cell would cost about $500 million. Is that far away or not? It depends. But because no one has yet organized such an effort, now is the time to talk about it. Leadership

in emerging technologies requires thinking carefully well before possibilities become likelihoods. Ten years in advance is when you need to speak up and act if you want to have a chance of steering the ship before a single group or country takes a unilateral run at it. I expect critique from the unilateralists who might wish to take that run, calling us chicken. But if you believe the potential risks of a mere mirror microbe, from an ecological perspective, are potentially off-the-charts bad, we need to take it seriously now before anyone acts on it.

What more should people understand about this topic?

Davis: Mirror *proteins* might be useful. In fact, there already are therapies being developed that use mirror proteins because their reversed chirality makes them very resistant to degradation – to extend the life of a protein drug. So, there are some very benign or even useful applications of mirror work.

But a mirror *organism* is a potential pathogen. There is no guarantee that we'll have immunity to such things. There's no guarantee that they won't eat up everything in the ecosystem. That's probably pushing it – but why go there? This is a very, very different kind of synthetic biology that could be very dangerous. It should be isolated and not advanced to building organisms.

Endy: Paul DeMarinis, a colleague in Art and Art History here, was auditing Stanford's *Introduction to Bioengineering* course one summer. I was teaching one week on bioterror, bio-error (lab leaks), and bio war. Paul said, "You've left out one of the 'er's': bio-scare-er." I didn't understand. He explained that the stuff I was talking about is scary. Scary like spiders are scary, like falling from heights is scary. There is an instinctive fear of biotechnology. Paul's lesson is one of the most profound things I've learned.

I am concerned that this report we've published could add to a sense of fear related to biotechnology. Yet, I believe strongly and I'm excited about creating opportunities for expressions of fear to come out into the open, so that we can welcome that and engage with those fears constructively. I see no future for bioengineering that doesn't include the routine building of entire cells. And, so, we have to talk about the edge cases, like mirror life. If we take a more holistic view, the gift of fear is the chance to become courageous together. That is fear's gift.

For more information

The lead authors of this paper are from the University of Chicago and the J. Craig Venter Institute. The full list of author affiliations is available in the supplementary materials of the *Science* paper.

Additional Stanford authors of this report include postdoctoral scholar Jaspreet Pannu and David Relman, the Thomas C. and Joan M. Merigan Professor at Stanford Medicine, professor of microbiology and immunology, and senior fellow at the Freeman Spogli Institute for International Studies. Relman helped to organize the group of scientists and the analysis almost two years ago.

Mark Davis is the Burt and Marion Avery Family Professor at Stanford Medicine and also a member of Stanford Bio-X, the Cardiovascular Institute, the Maternal & Child Health Research Institute (MCHRI), the Stanford Cancer Institute, and the Wu Tsai Neurosciences Institute. Endy is the Martin Family University Fellow in Undergraduate Education, a science and senior fellow, by courtesy, at the Hoover Institution, a senior fellow, by courtesy, at the Freeman Spogli Institute for International Studies, faculty co-director of degree programs at the Hasso Plattner Institute of Design (d.school), and a member of Bio-X. Pannu is also a physician within the Department of Medicine and affiliate at the Center for Innovation in Global Health. Relman is also a member of the Maternal & Child Health Research Institute (MCHRI), the Stanford Medicine Children's Health Center for IBD and Celiac Disease, and the Stanford Cancer Institute.

Paul DeMarinis is a professor of art and art history and, by courtesy, of music in the School of Humanities and Sciences.

Mirror Life Threats: Risks & Governance Solutions — Explained

By Aparupa Sengupta, PhD, RBP

Source: https://www.nti.org/risky-business/mirror-life-threats-risks-governance-solutions-explained/

Jan 15 – All life on Earth shares the same molecular "handedness." Proteins use left-handed amino acids, and sugars are right-handed. This uniform orientation is crucial because biological molecules interact through highly specific, three-dimensional "lock-and-key" mechanisms. Only molecules with the correct handedness can bind, assemble, and function together, enabling essential biological processes such as metabolism, replication, and cellular communication.

But what if we built life as a mirror reflection — right-handed amino acids and left-handed sugars? Could it survive, function, evolve, or coexist with us? These are questions we must grapple with as advances in synthetic biology bring us closer to being able to create mirror life — transforming a hypothetical concept into reality.

Mirror Biomolecules vs. Mirror Life

Some discussions about mirror biology mistakenly blend together two different concepts. **Mirror biomolecules**—individual amino

acids, sugars, or polymers with reversed handedness—may offer **limited, targeted scientific or technical value**. For example, mirror-image molecules could help researchers probe why terrestrial life evolved a single orientation, or could inform the development of more stable drugs or specialized biomaterials.

By contrast, the idea of constructing **mirror life**—a fully functioning, self-replicating mirror-based organism—offers **no practical benefit**. There is no clear scientific, medical, or societal rationale that would justify attempting to build such an organism, especially when weighed against the extensive potential risks.

The Risks We Face

We don't yet fully understand the impact mirror life could have on humans or our larger ecosystem. Scientists hypothesize that mirror bacteria could evade the immune systems of humans, animals, and plants, not respond to antibiotics, and fail to be picked up by existing detection tools resulting in significant morbidity and mortality and fundamentally altering entire ecosystems. Even if we tried to create and contain a mirror organism in a highly-controlled laboratory environment, it could escape—accidents happen—and we would have no way of knowing if it would persist and spread, or if we could even detect or stop it.

And like other powerful biotechnologies, mirror life could be potentially misused for harm. A sophisticated, well-resourced actor might try to alter or create mirror agents to evade surveillance systems or bypass existing medical countermeasures. These possibilities demonstrate why it's important to think about safeguards and proactive governance measures early.

Getting Ahead of the Risks

Although mirror life is still hypothetical, its absence of practical benefit and its considerable potential risks make early governance essential. Mirror life operates outside the assumptions that underpin modern biosafety, biosecurity, and medical surveillance, meaning the policy challenge is not only *what* to regulate — but *how* to govern a technology that doesn't yet exist.

Here are several concrete steps to help the research community, funders, and governments get ahead of the risks:

- **Define Research Boundaries:** International scientists, security experts, and other key stakeholders should define the technological advances and scientific advancements that would need to occur to create mirror life. They should seek to set boundaries around high-risk applications that would push us uncomfortably close to the development of mirror organisms. These boundaries should be defined in coordination with international bodies like the International Biosecurity and Biosafety Initiative for Science (IBBIS), World Health Organization (WHO), and the Biological Weapons Convention (BWC) Implementation Support Unit.
- **Target Chokepoints in Mirror Life Research & Development:** Map stakeholders that control key intervention opportunities points in the R&D lifecycle— funders, research oversight bodies (such as the NIH oversight committee, Institutional Biosafety Committees), material and software providers, and publishers –and work with them to develop and implement solutions designed to reinforce research boundaries. This could include requiring customer screening for critical tools and materials such as custom reagents, synthetic enzymes, and AI-enabled enzyme design software and using AI to monitor early-stage research and flag concerning trends before they scale. This effort should be led and incentivized by governments, in partnership with NGOs and expert groups, research institutions, publishers, AI mode developers, and reagent/software vendors.
- **Align Funders' Role:** Leverage the Bio Funders Compact and Bio Funders Forum to restrict financing for high-risk mirror biology research. These funder platforms support early conversations about the safety and security of emerging biological research — what is responsible to fund, under what containment, and how to weigh benefits against risks when the science is still evolving. Embedding these discussions upstream enables more coordinated and risk-aware grantmaking. Require all proposals to include structured risk assessments that seek to uphold mirror biology boundaries.
- **Leverage Multilateral Platforms:** Options can include leveraging existing multilateral institutions or establish new international mechanisms to codify the norm against mirror life creation and reinforce the boundaries that prevent us from getting too close to that undesirable reality.

Scientists increasingly caution that the risks of mirror life could

outweigh any benefits. Preventing mirror life from becoming a realized risk is not about restricting discovery. It's about ensuring that, as science advances, governance keeps pace—so that we don't march toward catastrophe.

Aparupa Sengupta served as a Senior Program Officer for NTI's Global Biological Policy and Programs team (NTI | bio). In this role, she supported the Biosecurity Innovation and Risk Reduction Initiative (BIRRI) to reduce risks of biotechnology catastrophe. This included efforts to advance the International Biosecurity and Biosafety Initiative for Science (IBBIS), a new international entity NTI is launching to safeguard science and reduce the risk of catastrophic events that could result from deliberate abuse or accidental misuse of bioscience and biotechnology. engupta is an accomplished scientist and global health security practitioner with more than 15 years of research, regulatory, and training experience across the fields of infectious disease containment, biosafety and biosecurity, and global biological risk reduction. Prior to joining NTI in 2022, she served at the University of California (Merced campus), where she initiated and led their biosafety and biosecurity programs, first, as the campus biosafety-biosecurity officer since May 2018 and then as the Assistant Director for Environmental Health and Safety and Director of High Containment Research Laboratories. From the start of the COVID-19 pandemic, she served as the COVID-19 response subject matter expert at the institution's Emergency Operation Center. Prior to 2018, Sengupta was a Biosafety Officer at Rutgers University, where she managed an Institutional Biosafety Committee that reviews biological risks related to infectious disease and recombinant DNA research, and she led multiple projects related to CRISPR/Cas9 and other emerging technologies and their potential implications in the biosafety-biosecurity realm. Sengupta is an active member of American Biological Safety International (ABSA Int.), where she plays key leadership roles in multiple committees; to highlight- Chair, Publications Committee and Co-Chair, International Engagement Committee. She also teaches pre-conference courses in the field of gene editing and related to other emerging technologies, and she has been invited to give many talks in the U.S. and internationally, advocating for the safe and secure use of emerging recombinant technologies in the evolving field of biosciences. Sengupta holds a PhD in Microbiology & Applied Biochemistry and MS in Molecular Genetics and Biotechnology from Michigan Technological University and a MSc in Biotechnology from Bangalore University, India. Sengupta is also a Registered Biosafety Professional (RBP) with ABSA International.

pp.43-46

World's First AI-Designed Vaccine Tested in Humans For The First Time

By Neil Mabbott

Source: https://www.sciencealert.com/worlds-first-ai-designed-vaccine-tested-in-humans-for-the-first-time

June 10 – Researchers at the University of Cambridge have developed what they describe as a fundamentally new type of vaccine using artificial intelligence (AI). The vaccine's key component was designed entirely by AI and has now been tested in people for the first time. The goal is ambitious: a single vaccine that works not just against all known human coronavirus variants, but against related bat viruses that could jump from animals to humans and cause future pandemics.

Traditional vaccines train our immune system to recognise one specific virus. The problem is that viruses mutate.

When they change enough, the vaccine stops working, which is why we need a new flu shot every year and why COVID vaccines have been updated repeatedly since 2021.

AI offers a way around this. By analysing genetic data from thousands of related viruses, it can identify the parts that stay the same across different strains and that are unlikely to change over time. Target those stable features, and you have a vaccine that should work against the whole family, not just the strain you started with. This is exactly what the Cambridge team did. They used AI to scan viruses from the sarbecovirus family, which includes the viruses that cause both SARS and COVID, as well as a range of animal coronaviruses – looking for shared features that evolution has left largely untouched. Those features became the basis of the vaccine.

DNA vaccines

While many people are familiar with the mRNA shots used during the pandemic, this new vaccine uses DNA. DNA vaccines are generally more stable than mRNA vaccines, making them easier to store and transport. A significant advantage in lower-income countries where "cold-chain" infrastructure is limited. They can also be administered without needles. A high-pressure stream of liquid delivers the vaccine through the skin, making administration less painful and easier to scale up during an outbreak.

Could it protect against future pandemics?

These practical advantages matter most if the vaccine itself can do something no existing jab can: **protect against viruses we haven't encountered yet.**

Broad-spectrum vaccines could change the way the world responds to emerging infectious diseases. By offering much wider protection than traditional vaccines, they could provide rapid immunity against new and emerging viral threats.

This would equip public health officials with tools to stop future outbreaks in their tracks before they have a chance to turn into global pandemics.

They could also transform our approach to more familiar diseases. Influenza is a prime target because it exists in many different strains and evolves so rapidly. Scientists have to predict which strains will dominate each flu season, and they guess wrong, vaccine effectiveness can suffer.

A universal flu vaccine that targets features shared across multiple strains could eventually end the annual race to keep up with the virus.

frameborder="0" allow="accelerometer; autoplay; clipboard-write; encrypted-media; gyroscope; picture-in-picture; web-share" referrerpolicy="strict-origin-when-cross-origin" allowfullscreen>

And the Ebola virus shows why this matters right now.

The recent outbreak in the Democratic Republic of the Congo and Uganda is driven by the Bundibugyo strain, which bypasses existing vaccines. While researchers rush to create a new vaccine specifically for this strain, local communities remain at high risk.

A broad-spectrum vaccine designed to cover an entire virus family could transform that picture.

What the trial found

This is the first human trial of an AI-designed vaccine. The results showed that this DNA vaccine was able to stimulate the immune system to produce antibodies that can recognise different types of sarbecoviruses. The technology was found to be safe and well tolerated.

This is an exciting advance because it demonstrates how AI has the potential to design variant-proof vaccines against future pandemic threats. The needle-free delivery system could also make the vaccine easier to administer and distribute worldwide.

However, there is more work to do. Although the results in this study are encouraging, the immune responses following vaccination were modest. It was also uncertain how long the protection lasts and whether further boosters will be required. Larger trials are also needed to determine whether the vaccine can prevent or reduce virus infections in the real world.

A universal vaccine remains a few years away. And any new vaccine must still pass larger trials to prove it is safe, effective and provides lasting protection.

But this study shows the goal is getting closer – and AI may help us get there faster.

Neil Mabbott, Personal Chair of Immunopathology, University of Edinburgh.

The World Cup Could Spread More Than Soccer Fever, Experts Warn

Source: https://www.sciencealert.com/the-world-cup-could-spread-more-than-soccer-fever-experts-warn

June11 – While millions of soccer fans cheer or groan over World Cup matches spanning North America, health officials will be on high alert for germs.

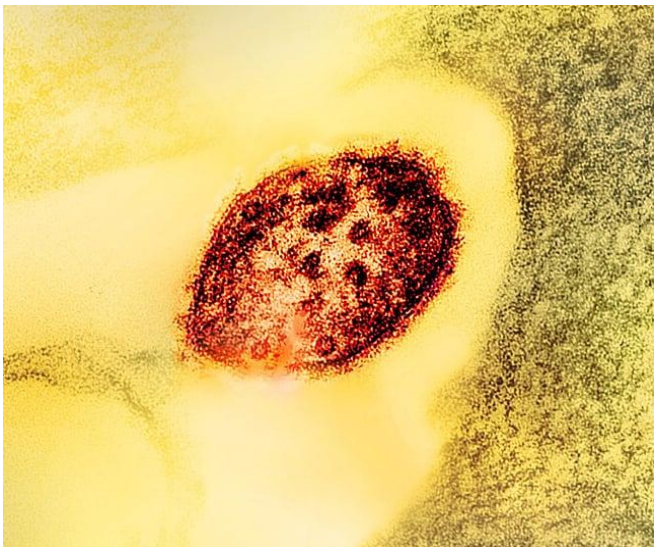
A heat wave may be the most obvious health threat.

But infectious diseases can spread in a crowd, and experts are set to scrutinize wastewater, hospital visits, even social media for any signs that an outbreak might be brewing.

Measles, one of the most contagious diseases, is among the top concerns, sparking a warning this week from the Pan American Health Organization, PAHO.

With a nearly six-week stretch of packed stadiums, bars and tourist sites in 16 cities, officials are on the lookout for a long list of infections,

from the stomach bug norovirus to mosquito-borne dengue fever.
"This is truly a marathon," said Palak Raval-Nelson, Philadelphia's health commissioner.
The Centers for Disease Control and Prevention already was grappling with a growing Ebola outbreak in central Africa and a cruise ship hantavirus outbreak.
While CDC officials have advised state and local health departments behind the scenes, the expected World Cup disease surveillance dashboard was still "in final development" days before games began, according to the Department of Health and Human Services.
"Our public health professionals are pretty stretched," said global health specialist Rebecca Katz of Georgetown University, who is leading an unusual new hub to help.
At the Health Security Operations Center, a joint effort between Georgetown and MedStar Health, workers are analyzing data from around the country so they can alert health authorities, even emergency rooms, to any early signs of trouble.



The measles virus can make your immune system forget, exposing your body to infections all over again. (NIAID/Wikimedia Commons/CC BY 2.0)

The center is issuing daily "situation reports" about disease trends around World Cup host cities and team base camps to several hundred local and federal public health groups, emergency management and hospital officials, and others who've signed up.
"It's important that we don't become alarmist," said MedStar emergency medicine specialist Dr. Shane Kappler.
"We're trying to be the insurance policy."
Measles is a top concern for potential spread at the World Cup. Already more than 2,000 people in the US have come down with measles this year, nearly as many as during all of last year, according to the CDC.

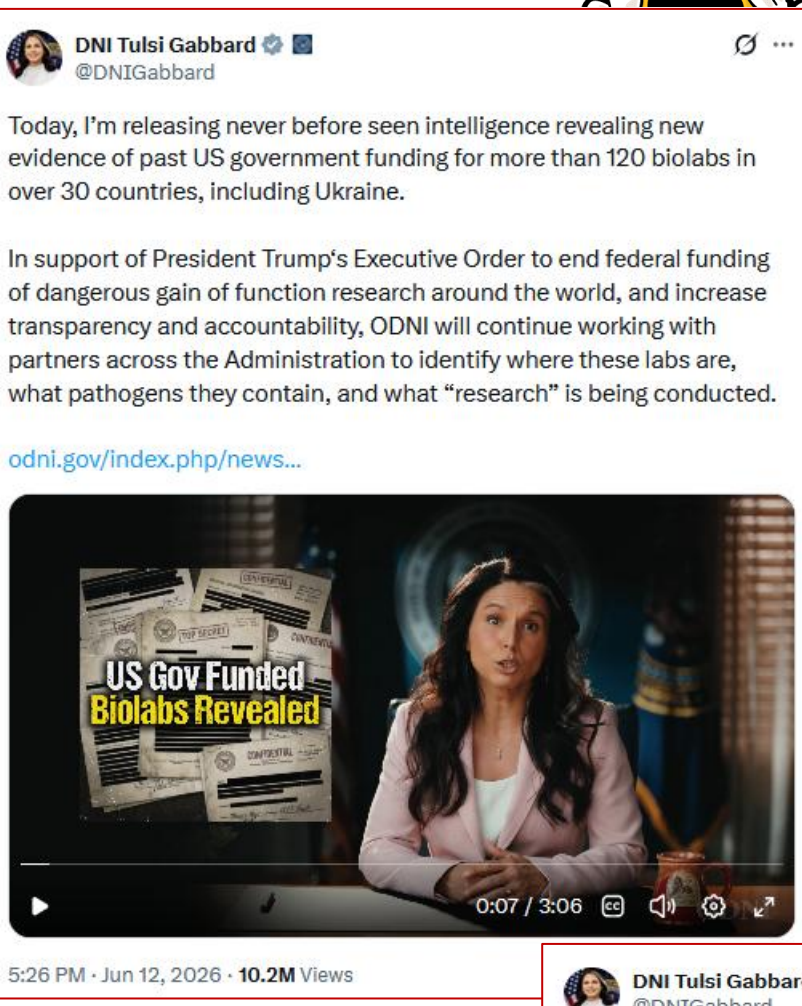
Patients can spread measles before the rash appears and they realize they're sick. Not too long ago, the US seldom saw measles except from international travel by unvaccinated people.
Now with frequent US outbreaks, "actually a lot of our international partners are worried about measles being exported to them after the games," said Georgetown's Katz.
Measles is spreading in Canada, too, and has exceeded 11,000 cases in Mexico, according to PAHO.
It's urging soccer fans to be sure they're vaccinated, with a health campaign noting that a single measles patient can spread the virus to up to 18 unprotected people.
Brown University's Dr. Craig Spencer, who survived Ebola while working in the West Africa outbreak over a decade ago, said he's repeatedly asked about the risk of Ebola during the World Cup – but "for me, Ebola is not the No. 1 or No. 2 or even No. 3 threat."
"I am concerned about importation of measles, I am much more concerned about the importation of other infectious threats that may not seem as scary to us as Ebola," Spencer said.
Many health experts agree that the risk of Ebola spreading in the US is very low.
That's partly because of government travel screenings and restrictions on people recently in outbreak-affected areas. Moreover, Ebola spreads by contact with bodily fluids from someone showing symptoms, not through the air like measles or respiratory viruses.
"One fortunate thing about this virus is you're most contagious when you're really quite ill," said Jennifer Nuzzo, director of Brown's Pandemic Center.
"It's not like COVID, where you could be sitting next to someone who doesn't even know they're infected and perhaps contract the virus." There's precedent for germs invading major sporting events. Canadian scientists linked a community measles outbreak to the 2010 Olympics in Vancouver, and clusters of norovirus had to be contained during the Olympics this year in Milan and in 2018 in South Korea. One way to detect signs of trouble: People with certain viral or bacterial infections shed genetic

material that sophisticated testing of wastewater can spot.
For example, measles can appear in wastewater days before an emergency room sees its first patients. This week's surveillance reports from Katz's center note that wastewater testing recently found diarrhea-causing rotavirus, hepatitis A and norovirus in some parts of the US, something to watch as soccer crowds arrive. In Dallas, officials ramped up wastewater screening, including at the international airport, casting a wide net rather than looking for specific illnesses, said Dr. Phil Huang, director of Dallas County Health and Human Services. His team is also enhancing the usual mosquito testing, checking not just for West Nile virus, which regularly spreads in the US, but also for viruses more common in other countries, like dengue and chikungunya.
Public health officials have been preparing for months, said Philadelphia's Raval-Nelson, including with mock emergency drills and communications with counterparts around the country.
"I don't want to send a message that there's one key thing," she said.
"We have the frameworks in place to carry out what we need to."

US Releases Information On Biolabs In Over 30 Countries, Including Ukraine

Source: https://www.rferl.org/a/us-biolabs-ukraine-funding-evidence-gabbard-dni/33779274.html

June 12 – The director of US National Intelligence (DNI) has released evidence that her office says shows "longstanding" United States government funding for more than 120 biolabs in over 30 countries where research on biological pathogens, some dangerous, is conducted.
"These biolabs include labs in Ukraine, which may be at risk of compromise due to the ongoing Russia-Ukraine war," the DNI's office said in a **statement** on June 12.
"For example, the Intelligence Community previously warned that a US-funded biolab in Ukraine likely housed dangerous pathogens and remained vulnerable to longstanding threats of Russian attack, seizure, or damage," it added.
The unusual move by Tulsi Gabbard came just days before her departure as DNI, who runs an intergovernmental office set up to coordinate information sharing among the sprawling US intelligence community. It wasn't immediately clear why Gabbard was releasing the information. Nor was it clear that it contained anything new or revelatory.
For years, under something called the Cooperative Threat Reduction program, the US government has funded efforts to safeguard Cold War-research programs -- mainly rooted in Soviet programs that developed biological, chemical warfare technologies.
Some of the holdover Soviet facilities were located in Kyiv, in Tbilisi, and other places around the former Soviet Union.



The Trump administration has been reviewing for months US holdings and files on biolabs funded by Washington after banning all federal funding for such gain-of-function research -- which involves the modification of organisms to enhance their biological functions -- in countries such as China, where it feels there is not proper oversight.

Branches of the US government such as the Defense Department have long funded overseas laboratories that do research on diseases.

As Russia's ties with the West have soured, Moscow has increasingly accused the US of funding "biolabs" aimed at developing potential biological weapons. Washington itself is a signatory to the Biological Weapons Convention of 1975.

Those accusations have fueled stubborn conspiracy theories over the years, something the US government has sought to debunk repeatedly.

In 2023, one year after Russia' full-scale invasion of Ukraine, the US State Department accused Moscow of "increasing the volume and intensity of its disinformation about biological weapons in an unsuccessful attempt to deflect attention from its invasion of Ukraine, to diminish international support for Ukraine, and to justify its unjustifiable war." Since returning to the White House in 2025, President Donald Trump's administration has taken more pointed approach to the question of biological pathogens, particularly regarding the COVID-19 pandemic whose origins in China are still a subject of intense debate. The Trump administration has said many of the Washington-funded biolabs have conducted research using "hazardous and highly contagious pathogens," and that such actions cannot be left "unrestricted."

In May 2025, US President Donald Trump signed an executive order to end federal funding of gain-of-function research around the world.

Mary Ann Liebert
Impact Factor: 1.6

Open access | Article commentary | First published online June 7, 2026

Addressing Biosecurity Barriers in High-Risk Biological Research

David R. Gillum, Randy A. Albrecht, [...], and Kathleen M. Vogel (+21) View all authors and affiliations

OnlineFirst | https://doi.org/10.1177/23265094261447176

Abstract

Biological research, including dual-use research of concern and pathogens with enhanced pandemic potential, faces mounting regulatory scrutiny that may impact pandemic preparedness and scientific progress. At a 2024 deliberative workshop in Reno, Nevada, biosafety professionals, biosecurity experts, and life sciences researchers discussed potential barriers to effective governance, including ambiguous regulatory definitions, resource disparities between regulated institutions, and fragmented oversight frameworks that impose burdens without improving safety or security. By incorporating biosafety professionals' expertise into policymaking, fostering a collaborative dialogue over punitive and inconsistent enforcement, and securing ongoing funding for biosecurity programs, we call for actionable strategies to reduce risk while advancing safe, secure, and transformative biotechnological breakthroughs in the life sciences and strengthening national security.

Is artificial intelligence increasing the biological weapon risk?

Source: https://uskudar.edu.tr/en/new/does-ai-increase-biological-weapon-risk/90129

An evaluation published in Nature journal revealed that AI-powered biological design tools are beginning to reach the capacity to design many biological agents, from deadly toxins to next-generation viruses. Prof. Muhsin Konuk, Faculty Member of Molecular Biology and Genetics (English) and Advisor to the Rector, drew attention to the fact that the use of artificial intelligence in the production of biological weapons is considered one of today's most tangible and urgent national security threats. Stating that AI-powered biotechnologies have a dual-use structure, and while these technologies accelerate vaccine and drug development processes on one hand, they can also facilitate access to information on dangerous pathogens for malicious actors on the other hand, Prof. Konuk said, "While AI can assist in designing a virus that could destroy humanity, it can also provide the means to develop a vaccine or antidote against that virus within hours." While the opportunities offered by artificial intelligence technologies in the fields of health, drug development, and biotechnology are increasing daily, the possibility of the same technologies being used for biological weapon development is becoming a growing source of concern in the scientific community. A comprehensive evaluation published in Nature journal revealed that AI-powered biological design tools are beginning to reach the capacity to design many biological agents, from deadly toxins to next-generation viruses.

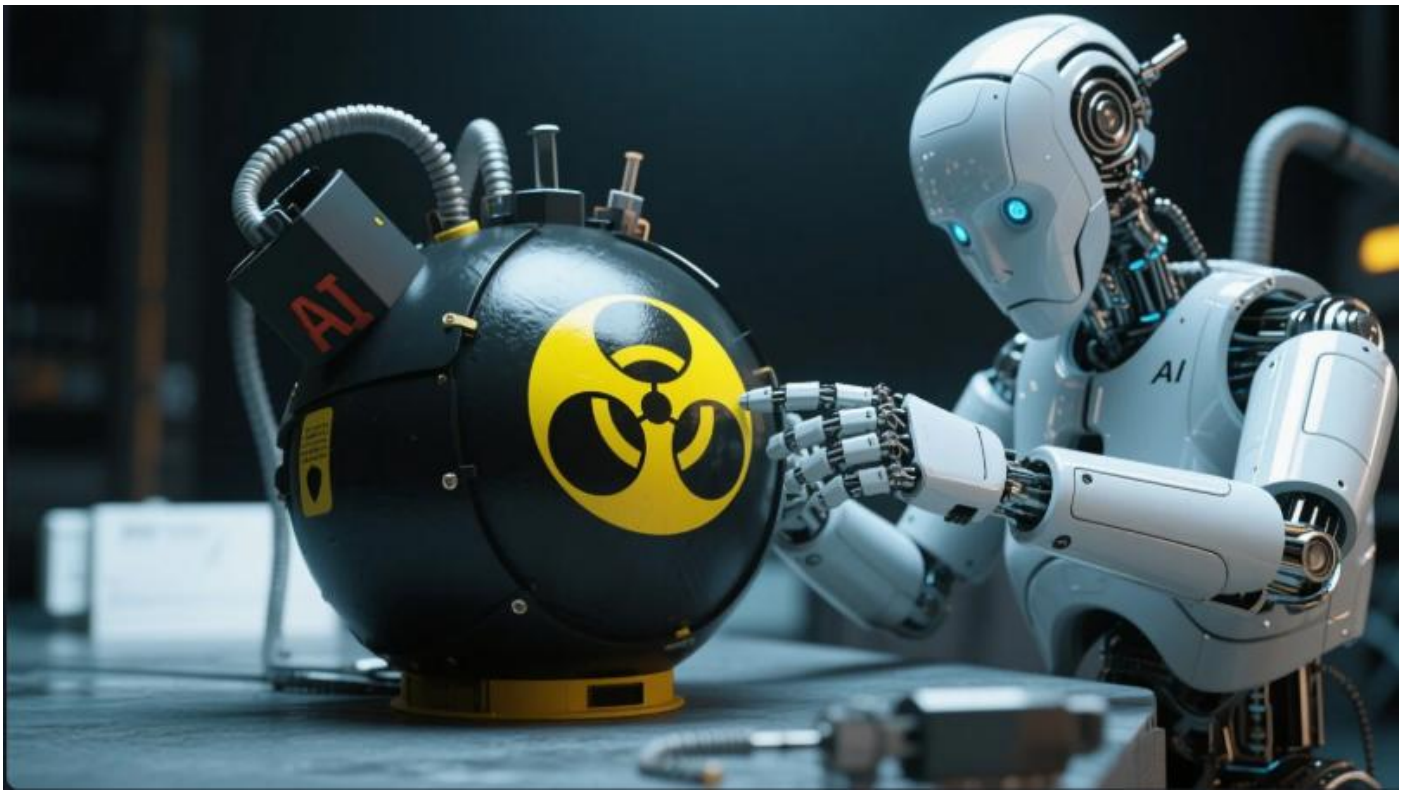
Prof. Muhsin Konuk, Advisor to the Rector of Üsküdar University and Faculty Member of Molecular Biology and Genetics (English), evaluated the malicious use of artificial intelligence technologies.

Attention to the use of artificial intelligence in the production of biological weapons!

Stating that AI-powered biotechnologies have become one of the most important national and global security topics today, Prof. Muhsin Konuk said, "The use of artificial intelligence in the production of biological weapons is considered one of today's most tangible and urgent national security threats by global security experts and technology leaders. In fact, leading AI companies and scientists are calling for urgent legal measures to be taken against this threat."

Information access barriers are rapidly disappearing

Prof. Konuk, also addressing the mechanisms by which artificial intelligence increases the biological weapon risk, the solutions it brings, and the measures taken, said, "One of the



main factors escalating the threat is the erosion of the information barrier. Historically, producing a biological weapon required advanced virology knowledge, laboratory experience, and access to secret formulas. Today's AI models perform better than PhD-level virologists, making the steps for amateur or malicious actors to produce dangerous pathogens understandable."

New pathogens not found in nature can be designed

Emphasizing that the power of artificial intelligence in biological data analysis and protein modeling can also pave the way for the emergence of unprecedented biological threats, Prof. Konuk stated, "Artificial intelligence (especially models performing protein folding and biological data analysis) can design new artificial viruses, toxins, or bacteria not found in nature, completely resistant to vaccines or existing drugs."

It can facilitate overcoming supply chain barriers

Stating that artificial intelligence not only generates theoretical knowledge but also facilitates logistical processes, Prof. Konuk said, "Artificial intelligence facilitates overcoming physical supply chain barriers by providing guidance on how dangerous materials can be ordered without detection or how laboratory equipment can be optimized."

Synthetic DNA orders must be strictly controlled

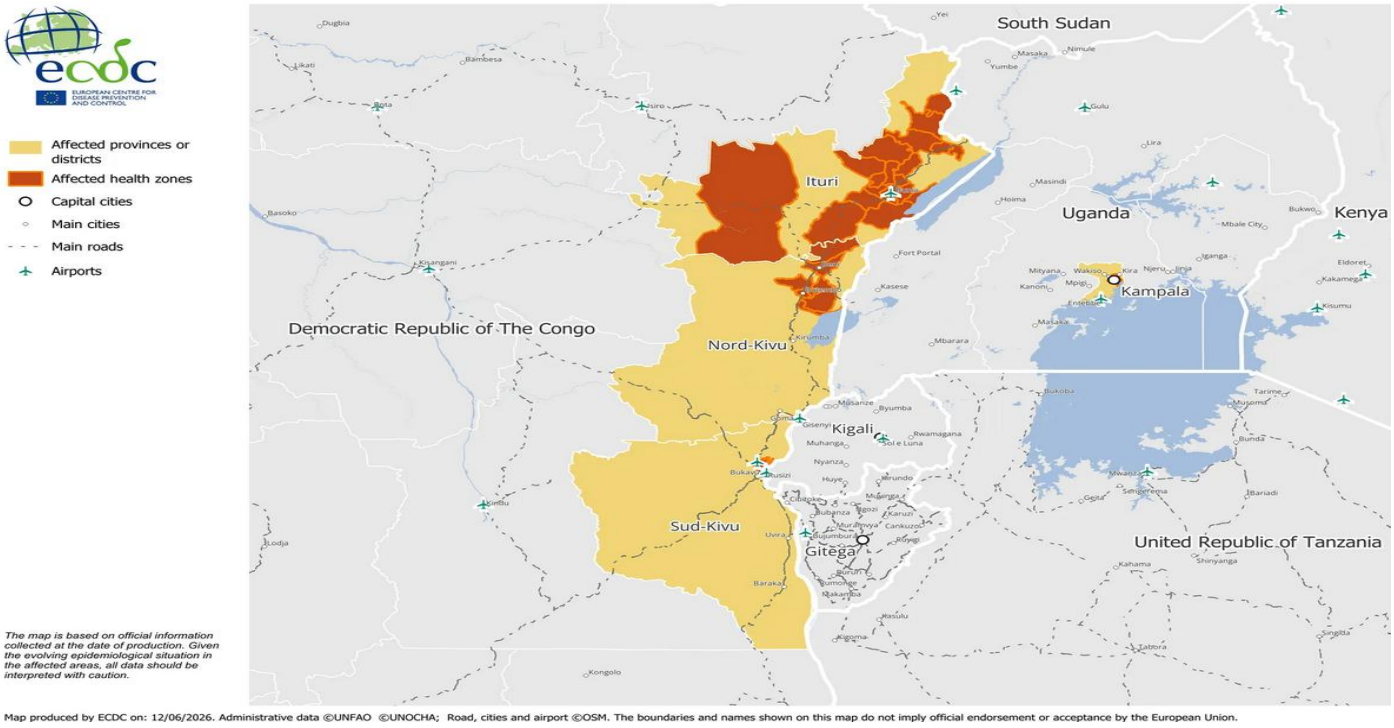
Noting that new measures are being developed in the field of biosecurity worldwide, Prof. Konuk said, "Screening synthetic DNA and RNA orders is important. AI giants and think tanks demand that synthetic DNA orders, also used in vaccine production, be subjected to strict control. The aim is to prevent dangerous gene sequences from being ordered and falling into the wrong hands." Prof. Konuk, also pointing to the legal regulations developed, said, "The European Union, in 2025, published the **Biotech Act**, defining synthetic nucleic acid sequences as 'products of concern.' Similarly, in the US, presidential executive orders focusing on artificial intelligence vulnerabilities and cybersecurity have come into force."

Security filters are being added to artificial intelligence systems

Stating that scientists are trying to embed software protection mechanisms into artificial intelligence systems to prevent biological threats, Prof. Konuk concluded his words by saying, "Scientists are trying to integrate software firewalls (watermarking, audit trails) that directly prevent AI models from designing dangerous biological agents or toxins. Considering all this, a typical dual-use example can be given for biological artificial intelligence tools, similar to the use of dynamite. While artificial intelligence can assist in designing a virus that could destroy humanity, it can also provide the means to develop a vaccine or antidote against that virus within hours. In short, although the technology itself is not evil, unregulated open-source biological data sets are expanding biosecurity vulnerabilities."

We don't know how the Ebola outbreak started. That's a problem.

Source: https://www.yahoo.com/news/science/articles/don-t-know-ebola-outbreak-111500069.htm



June 08 – In just 10 days over the summer of 1854, 500 people died of cholera in the Soho neighborhood of London. The city's population had more than doubled to 2.3 million people in the first half of the 1800s, and its sewage system could not keep up. But the streams of human waste flowing into the street and seeping into the water supply were considered unconnected to the cholera crisis. The prevailing theory of the day was that bad air — miasma — caused illness. The English physician John Snow thought differently. Five years before the outbreak he had suggested that the diarrheal disease was actually caused by a waterborne infection rather than miasma. He soon had a chance to test his theory, mapping the location of cholera-related deaths in Soho. Snow realized that the victims used one specific water pump on Broad Street, and he persuaded city officials to remove the pump's handle to prevent anyone else from using it. With the source eliminated, the outbreak, which had already passed its peak, ended in days.

Though it took years for Snow's theory to achieve widespread acceptance, his approach is central to modern epidemiology. Investigating the source of outbreaks can prevent new cases, but it also gives us a better understanding of diseases and helps manage public fear. Even when infections have stopped, outbreak investigations are useful to develop strategies for preventing — and, failing that, responding to — future outbreaks. Two recent outbreaks have demonstrated the necessity — and the challenges — of such investigations, almost two centuries after Snow's pioneering work. The first was the hantavirus outbreak that dominated headlines last month. Then, on May 17, the World Health Organization (WHO) declared a public health emergency of international concern, the highest level of global health alert, in response to an outbreak of the deadly hemorrhagic disease Ebola in the Democratic Republic of the Congo (DRC), which, as of June 2, had killed 62 people, with 363 confirmed cases. It's the 17th Ebola outbreak in the DRC and one of the largest on record. It has spread to neighboring Uganda, where, as of June 4, there are 16 confirmed cases, one confirmed death, and one probable case and likely death. The first confirmed case, a healthcare worker in Bunia, DRC, died on April 24, but the outbreak may have been spreading undetected since as early as January. Investigators haven't identified patient zero — the index case — and still don't know how this outbreak began. Abdou Sebushishe, a doctor working with the International Medical Corps in Goma, DRC, told CBS News that up to 20 percent of current patients are themselves healthcare workers. He estimated that it may be more than six months before the outbreak could be controlled, given that the disease is outpacing the current response.Part of the challenge is that the current outbreak is caused by the Bundibugyo strain of Ebola,

which is relatively uncommon and has a genome about 30 percent different from the Ebola viruses that usually spark outbreaks. Testing for more common variants didn't pick up the Bundibugyo virus right away, and ongoing conflict in the DRC contributed to the delay and continues to make contact tracing difficult. Unlike other strains, the Bundibugyo virus has no approved therapeutics or vaccines. In the past, researchers have had some success identifying the index case of Ebola outbreaks. Investigators managed to identify the first patient of the 2014-2016 West Africa Ebola epidemic — the largest and deadliest in history, with more than 15,000 confirmed cases and 11,000 deaths — as a toddler in the west African nation of Guinea. What's harder to definitively determine is how the boy, who died in December 2013 before the outbreak had been identified, contracted it. It's possible that he came into contact with an Ebola-infected fruit bat or its droppings while playing in a hollow tree, but scientists can't say for sure. Investigating outbreak origins is inherently fraught and can lead to the international fingerpointing that characterized much of the Covid-19 pandemic. But it's not primarily about assigning blame. Instead, knowing where and how outbreaks began informs how we respond to them, halt transmission, communicate to the public, and prevent them from happening again. It can identify high-risk regions and influence how public health officials monitor a disease. As the recent Ebola and hantavirus outbreaks demonstrate, however, that effort is often complicated by a host of factors, and the resulting uncertainty makes it that much harder to manage public health concerns efficiently and well.

The curious case of Legionnaires' disease in New York City

Our epidemiological tools have come a long way since John Snow used hand-drawn maps to identify the source of the Soho cholera outbreak. The value of these new tools lies in the information they generate — which is crucial to fighting outbreaks. Take the case of New York City's biggest — and deadliest — outbreak of Legionnaires' disease (LD), a bacterial infection that causes a severe pneumonia and has a fatality rate of 10 percent. By the time public health investigators detected it in the summer of 2015, dozens had already been hospitalized. It was the second-largest LD outbreak in US history, infecting 138 people and killing 16.

The initial epidemiologic investigation started with contact tracing to find the source of the disease, but the results didn't suggest any shared exposures. Cooling towers, which provide water for air conditioning systems in the form of an inhalable mist, had been involved in previous LD outbreaks, but officials didn't know how many cooling towers there were in the city or how well-maintained they were. Investigators ultimately located and tested 55 cooling towers in the South Bronx, where cases were clustered, for Legionella. They identified the source: a single cooling tower atop the Opera House Hotel. The hotel disinfected the tower, and New York's City Council passed new regulations requiring every building in the city with a cooling tower to register it with the health department, test it every 90 days, and remediate it if Legionella was found.

Within a year, the health department inspected almost 80 percent of the city's towers — detection and disinfection that would have never been conducted otherwise. No large LD outbreaks emerged — until inspections declined in 2025. "Regulations do not enforce themselves," Jay Varma, a physician and epidemiologist who served as incident manager for the 2015 New York outbreak, wrote last year in Healthbeat. "The Covid pandemic has sparked a strong backlash against government authority, and austerity budgets are now starving public health agencies. Infections may be inevitable, but outbreaks are a choice." Cholera and LD are waterborne, but Ebola and hantavirus, which first cross over to humans from animal reservoirs, present a different challenge.

The challenge of hantavirus and Ebola

"The end of the world, the beginning of everything" is the motto of Ushuaia, Argentina, the southernmost city on the planet, where tourists flock to watch birds and embark on cruise ships. It's the main gateway to Antarctica, making up 90 percent of all cruise departures to the continent.

It's here that a Dutch couple may have contracted the Andes virus, the only strain of hantavirus known to spread from person to person, before sparking an outbreak on the MV Hondius. The Argentinian government's prevailing theory is that the couple got infected while birdwatching at a landfill in Ushuaia before the cruise, coming into contact with the rodents that carry the Andes strain. Well, maybe not.

"The current theory of a couple birdwatching in southern Argentina may not be plausible, because the [long-tailed pygmy] rice rat that is responsible for spreading the Andes strain of the virus is usually found in northern Argentina or Chile, and we know the birdwatching at the landfill occurred in the southern part of Argentina," Omer Awan, a physician and public health expert, told me over email. There have been no recorded cases of hantavirus in Tierra del Fuego province, where Ushuaia is located, before.

"Understanding the origins of the outbreak will be helpful in guiding interventions like rodent control, isolation protocols, and…how the rare Andes strain of Hantavirus is transmitted," Awan said. "[And] identifying the source of the [2026] ebola outbreak can influence response strategy and how public health officials monitor the virus."

Delayed detection and human movement — especially for illnesses like hantavirus and Ebola that can incubate over the course of weeks — make tracing the source of an outbreak difficult, even in the best of circumstances. We still don't know the original

source of the first Ebola outbreak in 1976, which occurred in two simultaneous waves. Debates still rage over whether Covid-19 emerged naturally through zoonotic spillover — the virus jumping from an animal host to humans — or if it potentially escaped from a lab in an accident. We know that the hantavirus and Ebola outbreaks are natural in origin, but there are still international efforts to shift the "blame" from Argentina to neighboring Chile, especially with economic interests on the line. Such spillover events have only become more likely as humans destroy ecosystems and infringe on animal habitats. Climate change exacerbates existing infectious disease risk. "Because of our choices as a society, there's a one-in-five chance that another pandemic will occur in the next decade that will kill at least 25 million people," Neil Vora, the executive director of Preventing Pandemics at the Source coalition, wrote in Time Magazine.

Determining the source of outbreaks is even more difficult — and politically perilous — in the post-Covid era. The US and Argentina have pulled out of WHO. Global health funding cuts, on the part of the US as well as other countries, have weakened our biosurveillance architecture and ability to effectively respond to infectious disease.

Compared to Covid, the scale of the 2026 Bundibugyo and hantavirus outbreaks are small. It's still proving hard to get answers. That's going to be a serious problem whenever the next pandemic arrives — and it is a matter of *when*, not *if*.

An evolving threat landscape

Although we face escalating spillover risks from habitat destruction and climate change, we can't count on the next global infectious disease threat being naturally occurring in origin when it does come.

"It's very clear that artificial intelligence capabilities are advancing incredibly rapidly," Jaime Yassif, senior advisor for global biological policy and programs at the Nuclear Threat Initiative (NTI), told me. "[That could] make it easier for novice actors to engineer pathogens that we [already] know about or for sophisticated actors to engineer novel pathogens that are more dangerous than what's found in nature."

If there is an outbreak of uncertain origin — where it's unclear if it's natural, accidental, or deliberate — we lack robust international mechanisms that can investigate the source and quickly arrive at a conclusion. That would make it harder to address the source proactively, whether that means stopping future natural spillover events, preventing lab accidents, or holding bad actors to account.

Public health professionals would need to take additional precautions if there was a risk of a deliberate outbreak, as we saw with the 2001 anthrax attacks, where letters laced with Bacillus anthracis were sent in the mail, infecting 17 people and killing five. A naturally-occurring anthrax exposure would have required a different response, since a bioterrorism investigation has to contend with the additional challenge of determining criminal responsibility.

And as we've seen with the debates around Covid-19 origins, suspicion that something was caused by human activity can be incredibly corrosive to international trust, making necessary geopolitical cooperation in the face of outbreaks significantly harder.

NTI identified that preparedness gap and proposed a Joint Assessment Mechanism to identify the source of outbreaks of uncertain origin. It would be housed in the UN Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons (UNSGM) in order to pull together different components of the UN system and bridge security and public health.

That project (which I supported and advocated when I worked at NTI from 2022 to 2024) is currently on pause. "We still think it's a vital gap and really important, but we just couldn't get the political will to move it forward in the system, notwithstanding the significant support for it internationally in various quarters," Yassif said.

We are simply unprepared domestically and internationally to prevent, detect, and respond to global infectious disease threats. Emerging infectious disease outbreaks threaten us all, and we are nowhere near where we should be in order to protect vulnerable populations and countries around the world. While the current Ebola and hantavirus outbreaks are very unlikely to become pandemics on the scale of Covid-19, they're still dangerous and deadly. Unless we can determine where and how they began, we'll be ill-equipped to stop them from recurring. And next time, things could be far worse.

'I worry deeply about bioterrorism': Is Europe sufficiently prepared for another pandemic?

By Mared Gwyn Jones

Source: https://ca.finance.yahoo.com/news/worry-deeply-bioterrorism-europe-sufficiently-044857708.html

June 15 – In what may now seem like distant memories, Moderna was one of the heroes of the Covid era, bringing their mRNA based Spikevax vaccine to Europe less than a year after lockdowns were first implemented.

The US-based company had gone public on the NASDAQ just a few years earlier in 2018 and broke records as the biggest biotech IPO at the time. This record

has since been broken by Sana Biotechnology in 2021, Kailera Therapeutics in early 2026 and most recently by Parabilis Medicines who raised a whopping $670 million on 10 June 2026.

Following a boom in share prices linked to their Covid vaccine, Moderna has seen its valuation continue to drop over the past 5 years. But they are confident that is about to change and results so far in 2026 are showing a hint of optimism.

"COVID happened and so we took a little detour with trying to do our duty to help people… since then [we] went back onto mission," CEO of Moderna Stéphane Bancel explained.

"We started the company and then went public on this belief that mRNA is a very powerful technology and that over time, we should be able to make medicine in many therapeutic areas: cancer, infectious disease, rare genetic disease and more." In this episode of The Big Question, Stéphane joined Mared Gwyn in the studio to discuss the future of Moderna and the state of Europe's preparedness.

Is another pandemic coming?

"So we believe that there's always a risk of a big pandemic and it could be either from nature or it could be **man-made**," Stéphane told The Big Question.

"If something big were to happen like a pandemic we will be able to go even faster than we went in 2020 because now we have a manufacturing infrastructure. There's a big factory in America, we have also factories in Canada, in the UK, in Australia, so the world is much better already, Moderna is much better already."

And although Moderna is a US company, Stéphane is a European and he fears for his homeland.

BioNTech, the German biotechnology company who partnered with **Pfizer** for the Comirnaty Covid vaccine which became one of the most widely used across the planet, announced in May that they were closing their manufacturing sites in Germany.

After the end of 2026, the Comirnaty vaccine will be produced by US partner Pfizer.

"So if you look at it today, on continental Europe, there is no mRNA manufacturing capacity," Stéphane warned.

"And so what we're trying to do at Moderna is to work with the European Union, trying to work with several governments around Europe to figure out how can we do a partnership like we have done in Canada or in the UK or in Australia, because we think it's important for Europe to have mRNA on its soil."

"You could have something really bad happen in Europe and there is no industrial base to go and fight it."

AI is changing biological and nuclear risks; governance must change accordingly

By Stephen Herzog, Allison Berke, Yanliang Pan, William C. Potter, Douglas B. Shaw

Source: https://thebulletin.org/2026/06/ai-is-changing-biological-and-nuclear-risks-governance-must-change-accordingly/

June 18 – On April 7th, Anthropic announced that it was restricting public access to its most advanced artificial intelligence (AI) model, Claude Mythos Preview, because the system could discover and exploit unknown security vulnerabilities in software. The developer is far from alone in these concerns; such risks extend well beyond hacking and digital security. A major industry safety report from 2026 found that several frontier AI labs have recently added restrictions to their systems since they could not rule out that their models might assist novices in developing chemical or biological weapons. AI companies usually become aware of serious risks long before governments and international organizations can respond, making their involvement in shaping oversight rules critical from the start. But when it comes to restricting their own commercially valuable AI models, the industry has often stopped short. Moving beyond ad hoc restraint requires a standing forum where AI developers and outside security experts can jointly determine which emerging capabilities warrant closer scrutiny or limits.

Against that backdrop, the James Martin Center for Nonproliferation Studies convened a host of experts on April 8 and 9 at California's Asilomar Conference Grounds. The setting was fitting, as Asilomar has long been associated with landmark efforts to govern transformative technologies. More than 100 experts gathered to discuss how AI may affect nuclear and biological weapons. Participants included representatives from universities, think tanks, research institutions, the national laboratories, governments, and crucially, the AI industry. The meeting launched a new Asilomar Process to develop practical safeguards for AI-related nuclear and biological risks as the technology continues to advance. AI will affect nuclear and biological threats in different ways, but those ways connect to common governance problems. Relevant private sector AI models are developing much faster than the institutions tasked with preventing nuclear war and catastrophic biological events. AI companies may be the first to recognize new capabilities, but weapons and conflict experts are needed to judge when those capabilities create concrete security risks. As such, seven principles arose from the recent Asilomar conference intended to address this challenge. Each of

these principles can be translated into new practices by AI labs, governments, and international organizations.

When AI meets synthetic biology and nuclear weapons

COVID-19 demonstrated the scale of damage that a pandemic can inflict worldwide, even without the added threat of a deliberately engineered pathogen. It also showed how manipulated information can shape public behavior on a vast scale during a biological emergency. Those lessons are becoming more urgent because advanced AI systems could lower barriers to creating harmful biological agents by providing guidance to users with limited expertise. This type of danger is likely to grow as cloud laboratories make sophisticated biotechnology experiments remotely accessible, potentially straining safeguards designed around physical facility access. Companies controlling advanced biological design models and automated laboratories will therefore be making decisions with significant security implications, whether or not they are subject to established rules. It would be a grave mistake to wait for a pandemic that is far worse than COVID-19 to clarify these responsibilities.

AI raises a different set of concerns in the nuclear weapons domain, where governance gaps are already visible and the consequences of integration could be existential. Artificial intelligence use in early-warning and crisis-decision support could compress decision time and increase pressure on leaders to launch nuclear weapons in response to false or manipulated information. Governments have begun to acknowledge these nuclear dangers. In December 2025, the UN General Assembly adopted a resolution on risks from AI in nuclear command, control, and communications. Likewise, while AI may improve monitoring and verification, recent research also warns that it may eventually help potential proliferators overcome bottlenecks to building the bomb. AI could also expose nuclear personnel and facilities to combined cyber, physical, and information attacks. Yet, at the 2026 Nuclear Non-Proliferation Treaty Review Conference, specific language on AI-related nuclear risks was removed from the final draft outcome document. Taken together, the nuclear and biological cases reveal a fundamental gap in international AI governance. The same rapidly advancing technology is beginning to reshape both fields through very different routes. But they present a common governance challenge. Private developers may be the first to identify dangerous model capabilities, but they cannot evaluate those threats on their own. Nuclear and biological security experts can help determine what capabilities should be tested and when model advances raise the risk of nuclear war or an engineered pandemic. Pivotally, neither side can adequately address the concerns raised by AI without the other.

Following the Asilomar meeting and subsequent deliberations, the conference Secretariat adopted seven principles for governing AI applications in nuclear and biological security. The novelty of these principles lies in trying to build a bridge between the AI industry, which may encounter new capabilities first, and the experts and regimes trying to prevent the spread of nuclear and biological weapons. As the first public statement of the new Asilomar Process, they are reproduced below in full.

The Asilomar principles for governing AI applications in nuclear and biological security.

These principles are intended to recognize AI's potential contributions to human safety, as well as its capacity to create or amplify global catastrophic risks. As the first statement of an ongoing Asilomar Process, the principles aim to set an agenda for further research and implementation work, while remaining open to refinement as experience and capabilities evolve.

AI must protect human survival.

AI systems must reinforce—and never erode—barriers against the use of nuclear and biological weapons. These armaments pose extinction risks to humanity that predate the development of AI. Such risks must not be accelerated or exacerbated by AI systems. The protection of human survival should therefore be the first priority in the deployment of AI tools affecting these domains.

Nuclear weapons use decisions must remain under meaningful human control.

AI systems must not initiate, authorize, or otherwise cause the use of nuclear weapons. Human decision-makers must retain the ability to review and override AI outputs, even under severe time pressure and in circumstances where automation bias may distort judgment. Any AI system involved in nuclear-decision support must accordingly be auditable in both data and logic—by civilian and military authorities—in peacetime and in crises. New intelligence, surveillance, and reconnaissance (ISR) systems and nuclear command, control, and communications (NC3) architectures should be deployed only when they are shown to decrease the risk of nuclear weapons use.

AI governance must strengthen nonproliferation and strategic stability.

Nuclear and biological research activities must be made safer, more secure, and more proliferation-resistant in light of AI's disruptive potential. Existing practices of restraint must evolve to address new risks introduced by AI, including through commitments that reduce the dangers of AI-enabled escalation, miscalculation, or proliferation. Behavioral arms control and confidence-building measures should be pursued alongside the responsible use of AI tools to improve crisis communication.

AI developers must contribute to anticipatory risk governance.
Frontier AI developers bear a special responsibility for helping anticipate and govern the nuclear and biological risks that may arise from rapid commercial innovation. Advances in AI may introduce technological shocks into these domains before governments or international institutions are prepared to manage them. Developers should therefore assess emerging capabilities before their release, recognize how they may alter incentives or lower practical barriers to weapons use or proliferation, and support stronger oversight as risks increase. AI companies are geopolitical actors whose choices can affect global security. Their legal, financial, and institutional obligations should reflect the overriding priority of preventing extinction risks.

AI-enhanced monitoring and verification must be responsible and ethical.
AI systems may significantly improve the monitoring and verification of peaceful nuclear and biological activities, as well as efforts to detect diversion in support of weapons of mass destruction programs. Because these judgments carry high stakes, the use of AI must not weaken established standards for explainability, objectivity, validity, data provenance, and ultimate human accountability. AI should be used in ways that protect privacy and personal safety, while also guarding against the disclosure of sensitive nuclear or biological information that could aid malicious actors or undermine strategic stability. AI models used for monitoring and verification must themselves be protected, so that they do not become tools for helping proliferators evade detection.

AI governance must be globally inclusive.
International collaboration—aligned with frameworks such as the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) and the Biological Weapons Convention (BWC)—should ensure that the benefits of AI accrue to all humanity without deepening security or development divides. This work should cultivate shared strategic understanding, reducing rather than compounding the risks of nuclear proliferation, nuclear escalation, war, and catastrophic biological events. Measures that restrict access to dangerous capabilities should therefore be paired with efforts to reduce the incentives that drive states or other actors to acquire them.

AI must not enable disinformation or attacks on nuclear and biological facilities.
False or manipulated information concerning the use or development of nuclear and biological weapons can be highly damaging. Safeguards should be established to prevent actors from using AI to create or disseminate highly realistic falsehoods in these domains. Active resilience must also be developed against AI-enhanced physical and cyberattacks on nuclear and biological facilities, including attacks intended to enable material theft or sabotage. These measures should address both crisis decision-making and public perceptions of nuclear and biological threats. The societal, economic, and psychological effects of information warfare may be difficult to reverse.

From principles to practice
Moving forward, the Asilomar Process should create a collaborative environment for developing thresholds about when emerging AI capabilities present serious concerns. In nuclear security, this means asking whether an AI system changes crisis stability dynamics or proliferation risks. In biological security, this means assessing whether a model materially shortens the path to producing a pathogen capable of causing an outbreak. Such judgments cannot remain informal or hidden behind commercial secrecy. Clearer evaluation protocols should guide risk mitigation measures so that developers and governments can act *before* dangerous capabilities spread.
Ultimately, this work should inform national authorities and the international institutions charged with reducing nuclear and biological threats to humanity. The Nuclear Non-Proliferation Treaty and the Biological Weapons Convention are at the heart of this governance architecture. But neither was designed for a world in which commercial AI capabilities may reshape security risks faster than multilateral processes can respond.
The Asilomar Process is intended to connect technical evaluations of emerging AI capabilities to the policy choices that governments make under these regimes. Without that bridge, states may confront AI-enabled nuclear or biological catastrophe only after the most important decisions have already been made.

Stephen Herzog is Professor of the Practice at the James Martin Center for Nonproliferation Studies, based on the Vermont campus of Middlebury College. He is the Editor-in-Chief of *The Nonproliferation Review* and an Associate of the Project on Managing the Atom at the Harvard Kennedy School's Belfer Center for Science and International Affairs. His past positions include Co-Chair of the Beyond Nuclear Deterrence Working Group, Senior Researcher in Nuclear Arms Control at ETH Zurich, Verification Specialist at the U.S. Department of Energy's National Nuclear Security Administration, and Research Associate at the Federation of American Scientists. Herzog earned a PhD from Yale University and has published widely in scholarly and policy journals. He co-edited *Atomic Backfires: When Nuclear Policies Fail* (MIT Press, 2025).
Twitter

Allison Berke is a senior engineer at RAND's Center for AI, Security, and Technology, where she works on biosecurity and AI security research and policy. She is also the Director of the Biological and Chemical Weapons Nonproliferation Program at the Center for Nonproliferation Studies at the Middlebury Institute for International Studies, and teaches science and technology policy at Stanford University. She has a PhD in bioengineering from UC Berkeley.
Yanliang Pan is a research associate at the James Martin Center for Nonproliferation Studies, where his research has focused on nuclear supply and emerging technologies, particularly how artificial intelligence intersects with nuclear security and nonproliferation.
William C. Potter is the director of the James Martin Center for Nonproliferation Studies and co-author of *Death Dust: The Rise, Decline, and Future of Radiological Weapons Programs* (Stanford University Press, 2023). His present research focuses on multilateral nuclear arms control and forecasting proliferation developments. Dr. Potter is the recipient of the Thérèse Delpech Memorial Award, and has served as the U.S. representative on the UN Secretary General's Advisory Board for Disarmament Matters and on committees of the National Academy of Sciences.
Douglas B. Shaw is a Non-Resident Scholar at the James Martin Center for Nonproliferation Studies at the Middlebury Institute of International Studies at Monterey. He served as Senior Associate Provost for International Strategy at the George Washington University and as Director of Policy Planning at Georgetown University. Following the end of the Cold War, Shaw worked on the successful global diplomatic campaign to indefinitely extend the Nuclear Non-Proliferation Treaty for the U.S. Arms Control and Disarmament Agency and the successful programmatic effort to secure weapons-usable nuclear material in Ukraine from theft or diversion for the U.S. Department of Energy. In 2025, he led a nuclear threat initiative study on the *Nuclear Security Implications of AI and Emerging Technologies: A FutureSafe Analysis of Risks and Opportunities*. He holds a Ph.D. in international relations from Georgetown University.

Rue de la Vacherie, 78 | B5060 SAMBREVILLE (Auvelais) | Belgium
https://www.ici-belgium.be/