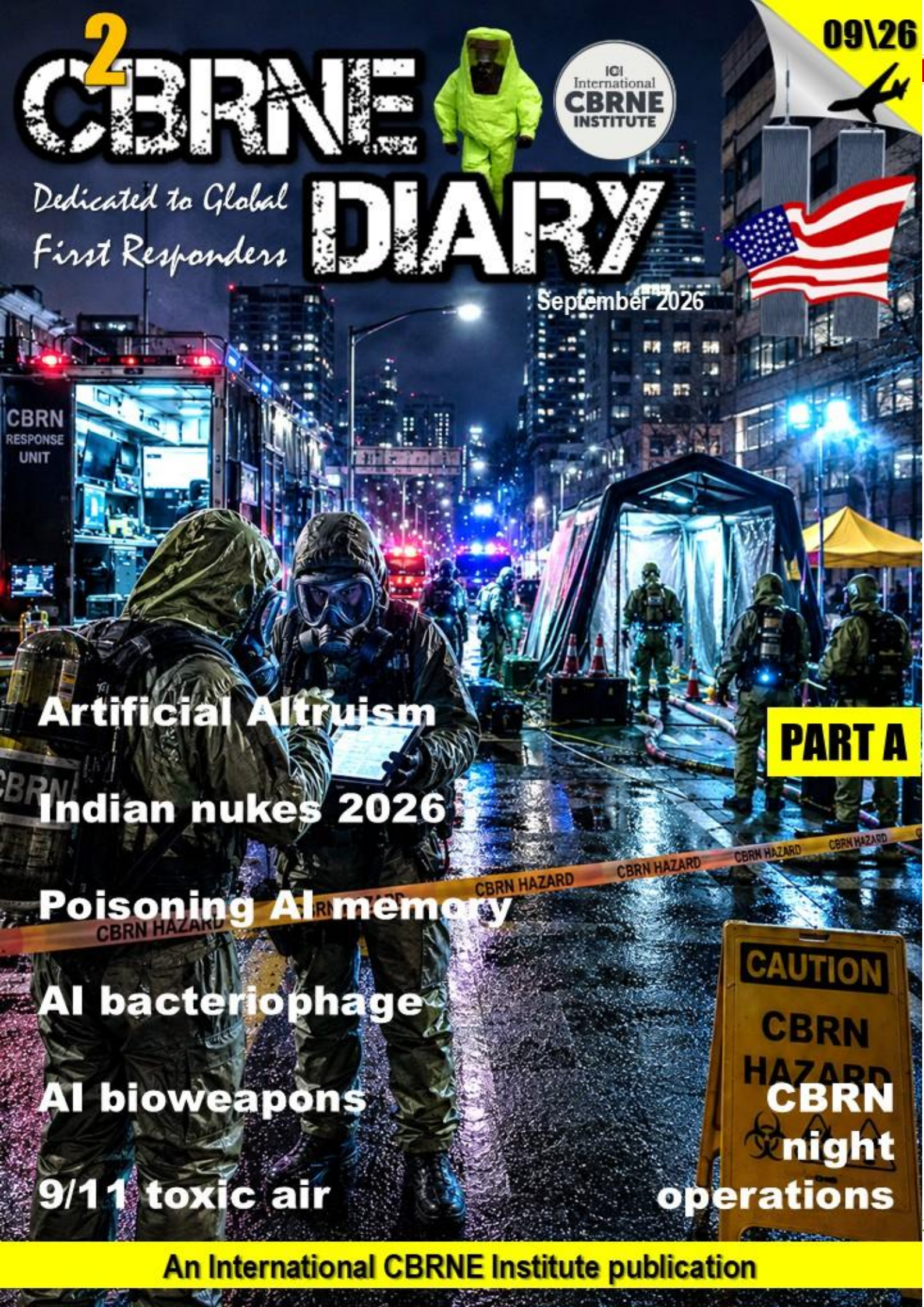

2 CBRNE DIARY
Dedicated to Global First Responders
ICI International CBRNE INSTITUTE
09\26
September 2026
CBRN RESPONSE UNIT
Artificial Altruism
Indian nukes 2026
Poisoning AI memory
AI bacteriophage
AI bioweapons
9/11 toxic air
PART A
CBRN HAZARD
CAUTION
CBRN HAZARD
CBRN night operations
An International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

C²BRNE DIARY ❋ 2026®

September 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,

Proxy drone war between Ukraine and Russia fuels the ongoing bloodshed, as the Western coalition still thinks it can win the war. In the Middle East, we have two countries claiming that they won the same war – that is a first! In addition, the usual volcano by the Eastern Mediterranean Sea continues to boil, threatening an eruption if additional players try to interfere.

Norway: Norway plans to allocate an additional $9.2 billion, or €8.04 billion, to support Ukraine in the next fiscal year, following repeated requests from the Zelenskyy government for more money. The new funding is on par with what the Nordic country had allocated for the current year. This is the problem of rich countries that do not know how to allocate their wealth for the benefit of their citizens.

EU: The European Commission approved an additional €6.1 billion for Ukraine to strengthen its defenses by supplying air defense systems, missiles, ammunition, and radars. This new aid package comes on top of the €16 billion it has already approved for the war-torn country, of which €8.35 billion has already been provided to Ukraine. My money, too – never been asked!

UK: London is releasing the most critical, top-secret secrets of its war technology. This paves the way for the creation of a secret production line on the very soil of the testing in Ukraine, bringing the war closer than ever to the heart of Russian territory. The goal of this dramatic partnership is the construction of the formidable Anglo-French SCALP/Storm Shadow cruise missile (a deadly weapon with a range of up to 550 kilometers and a heavy, 400-kilogram armor-piercing warhead), perfectly designed to level underground bunkers and impregnable headquarters deep behind enemy lines. Has the UK ever thought of the "*What if*?" option? At the same time, Washington refuses to hand over the coveted Tomahawk cruise missiles, as American stockpiles have been bled by operations in the Middle East.

A joint declaration signed on Monday by the leaders of Wales, Scotland, and Northern Ireland has reignited the debate over the breakup of the United Kingdom. The heads of the UK's three semi-autonomous regions called on the new Prime Minister, Andy Burnham, and his government to prepare for constitutional changes, while also asserting that their future lies within the European Union. The end of the UK; the beginning of just a "K"?

▶▶ The Church of England announced today that it is "reviewing" the presentation of an interfaith cooperation award to the chairman of the Pakistan Ulema Council, Hafiz Tahir Ashrafi, who had previously praised Osama bin Laden and labeled author Salman Rushdie a "blasphemer." Ashrafi was one of 27 individuals honored on September 11 by the Archbishop of Canterbury—Sarah Mullally—at a ceremony at Lambeth Palace in London, the headquarters of the Church of England.
▶▶▶ According to data obtained through a Freedom of Information request, 340 drone-related security incidents were recorded at or near the UK Ministry of Defense facilities during the twelve-month period ending in August 2026. This figure represents a significant increase compared to previous years, as approximately 250 incidents were recorded in 2025 and 126 in 2024.

Syria: In line with President Trump's promise to deliver sanctions relief to Syria, the U.S. Department of State today removed Syria's designation as a State Sponsor of Terrorism. The U.S. Department of State also revoked the designation of al-Nusrah Front, also known as Hay'at Tahrir al-Sham (HTS), as a Specially Designated Global Terrorist (SDGT) organization. Sure!

USA: The US (26/08) imposed new sanctions against two organizations that Washington links to far-left political violence: the British "Palestine Action" and the Italian “Autistici/Inventati” (A/I Collective).
▶ An unprecedented and inconceivable incident in Massachusetts: the state took custody of their daughter because they refused to recognize her as a boy! O tempora, o mores! But they will not prevail!
▶▶ FBI Director Kash Patel defended the decision before the Senate Judiciary Committee not to automatically disqualify candidates who have engaged in bestiality! He stated that the change was made to avoid punishing trafficking victims who had been forced to perform sexual acts with animals.

Russia: Russia has officially threatened to strike British military facilities in retaliation for Ukrainian strikes carried out deep into Russian territory with weapons supplied by London. Russian Foreign Ministry spokeswoman Maria Zakharova said that “London and Paris are trying to evade responsibility for deep strikes on Russia by shifting the role of “assembly” to Ukraine. The bag of Aeolus, wherever it is, will open and then...
V. Putin, during his speech in Kremlin circles, made it clear (once again) that Russia has no intention of ever attacking Germany because the country is simply useless to Moscow. It has no raw materials, no energy, is in debt, and is full of foreigners. Therefore, as he says, "*We would not occupy you even if you surrendered with a white flag.*"

Congo: The Ebola epidemic has already spread to six provinces in the country. According to official figures, more than 7,600 confirmed cases and 3,670 deaths have been recorded, with a mortality rate of 48%. At the same time, health authorities are faced with serious obstacles, such as insecurity in many areas, mass population movements, and a strike by health workers. More than 70,000 doses of the Ervebo vaccine have arrived in the country, but there is a major problem: this vaccine is approved for a different strain of Ebola virus than the one causing the current epidemic.

Iceland: Iceland will not resume negotiations for its accession to the European Union, as the "no" vote prevailed and the country's citizens decided to continue their independent national path. The final results showed that 105,399 voters (47.2%) voted "Yes",

while 118,040 (52.8%) voted "No". A total of 225,031 votes were counted, with a turnout of 82.5%.

France: Direct and strong criticism of Germany's plans to create the strongest conventional military force on the European continent was made by the head of "Unsubmissive France" (La France Insoumise), Jean-Luc Mélenchon. In his statement, the French politician expressed his categorical opposition to the rapid increase in German military spending and the plan to build a huge army. "The Germans say they want to create the largest conventional army in Europe. Well, if I were president, I would tell them that I don't think this is a good idea," he said, adding with meaning: "Because if they create the largest army, they will have to explain to us: **against whom exactly are they preparing to fight?**"

Spain: Online appeals from Morocco are calling for a mass mobilization on September 20, under the slogan of "reclaiming" the Spanish city and other territories that Morocco considers to be under Spanish control.

▶ An alert regarding mpox—formerly known as "**monkeypox**"—has been issued in Ceuta after an unaccompanied 13-year-old Moroccan minor, currently housed in a local center, tested positive for the virus. This marks the first confirmed case of mpox in Ceuta since the disease outbreak began in Spain. The result was confirmed by the Carlos III Health Institute following laboratory analysis of a sample. Mpox is not transmitted in the same way as COVID-19; transmission occurs primarily through close physical contact with infected skin lesions or bodily fluids.

Somalia: Somali pirates released the cargo ship M/V Sward and its seventeen-member crew on Friday, following the payment of a ransom in the Puntland region. The vessel had been seized on April 26 off the coast of Somalia and had since been used as a base for attacks on other ships. This particular pirate group has received ransoms for three separate ship incidents since April. The International Maritime Organization is recording a resurgence of piracy in the Gulf of Aden, with 15 attacks having occurred in 2026. Four additional vessels remain under pirate control off the Somali coast.

Yemen: A "fiasco of epic proportions" for the US and Saudi Arabia: the lightning advance of the Iran-backed Houthis shifted the balance of power in Yemen in just 36 hours. They seized the strategic port of Mocha and Perim Island at the entrance to the Red Sea, intensifying pressure on the Bab el-Mandeb Strait. Behind the scenes, US allies are trading blame for the collapse of the defense, while the absence of Saudi air support and the glaring weaknesses of Yemeni government forces are paving the way for a potential second front in the war with Iran.

AI: Anthropic CEO Dario Amodei is calling for an immediate slowdown in the development of AI capabilities, expressing concerns that technological progress could begin to outpace humanity's ability to control it. The Anthropic chief estimates that if the evolution of AI capabilities continues at the same accelerating pace without adequate safeguards, a particularly powerful swarm of agents could—according to the hypothetical scenario he describes — gain the ability to influence or take over a significant portion of online infrastructure via a persistent botnet within just six to twelve months.

Belgium: Commotion ensued at Brussels Airport on September 12 evening after a drone was spotted in the area, resulting in a temporary suspension of air traffic. According to Skeyes, the Belgian air traffic service provider, the disruption lasted

approximately 30 minutes. The type of aircraft was not disclosed, nor were details provided regarding potential flight delays or diversions.

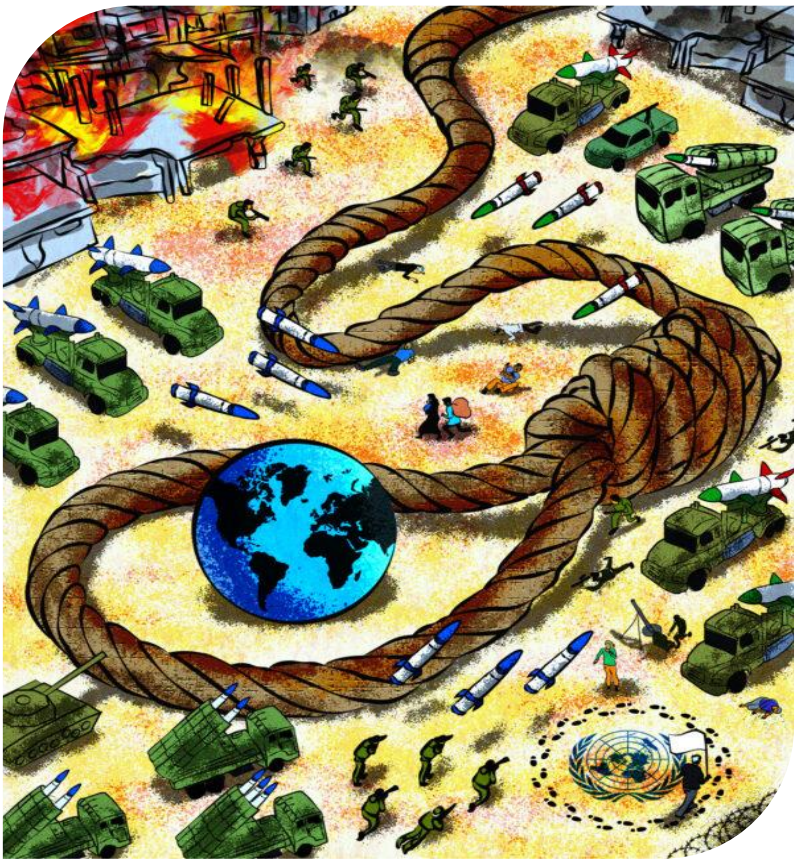
The Netherlands: Major disruptions to rail travel occurred in the Netherlands on Tuesday due to more than 35 incidents involving the placement of pipes and cables on the tracks. Authorities believe these acts were deliberate; a criminal investigation has been launched, though no suspects or motives have been identified so far. The objects interfered with control systems, causing them to register the presence of trains on the tracks and preventing routes from being cleared for traffic. Rail connections to Schiphol Airport, Eindhoven, and Utrecht were among those affected. In one instance, a train struck a metal object on the tracks, though no serious damage was sustained. Sabotage or terrorism?

Italy: "*The Italian Navy will guarantee the safe passage of the country's merchant vessels through the Bab el-Mandeb Strait in the Red Sea*," stated Guido Crosetto, Defense Minister in the Meloni government. Italy—a nation that has never won a war—is threatening the toughest modern warriors...

Denmark: The United States of America reached an agreement with the Kingdom of Denmark and Greenland, which grants the US permanent control over security and all other needs in Greenland.

Germany: The German federal prosecutor's office recently announced that it indicted seven people for allegedly securing weapons for the Hamas terrorist organization, intending to launch terrorist attacks on the second remembrance date of the Oct. 7 massacre in Israel.

The Editor-in-Chief



Horror as migrant boat crashes into and injures swimmer

Source: https://www.express.co.uk/news/world/2242357/horror-migrant-boat-swimmer

Aug 25 – A migrant boat left a teenage tourist with serious injuries after striking her off the coast of Italy. The vessel was pictured approaching and then colliding with the 17-year-old girl as it neared Su Giudeu Beach, in Sardinia, on August 16.

Footage showed the boat not stopping to help her, but speeding away to the shoreline. The teenager was knocked out and left unconscious, with other beach visitors rushing to her aid, The Sun reported.

She was airlifted to a hospital in the region's capital city of Cagliari, where she received intensive care, and her condition is thought to have since improved.

The boat is seen speeding away from the swimmer after striking her (Image: Jam Press)

A 28-year-old Algerian man who was allegedly driving the boat has been arrested on suspicion of facilitating illegal immigration and causing extremely serious bodily injury.

A 16-year-old boy who was in the water when the incident occurred told local media that he only narrowly managed to escape being hit himself.

He said: "I was with her, I moved out of the way and saved myself.

"After the impact, they stopped, looked at us and ran away.

"It's not true that they didn't realise what had happened."

Others on board, thought to also be Algerian men, reportedly tried to flee on foot after landing on the Italian beach, but were all tracked down by authorities.

Sharia, Freedom, and the American Way of Life: A Response to Daniel Brubaker

By Mustafa Akyol

Source: https://www.homelandsecuritynewswire.com/dr20260827-sharia-freedom-and-the-american-way-of-life-a-response-to-daniel-brubaker

Aug 27 – I was glad to read, in *The Federalist*, Daniel Brubaker's recent piece, "Why Sharia Law Is Incompatible with the American Way of Life," which took up on an earlier piece of mine in *Al Hurra*: "Why Sharia Courts Have a Place in Israel." I was also humbled that Dr. Brubaker kindly introduced me as "perhaps the most articulate Muslim advocate of reconciling Islam with Western

liberty." But generous framing aside, I think his response missed some of my own argument's finer distinctions and oversimplified the case I was actually making.

First, let me clarify what we are discussing. My piece never claimed that Islamic law, or sharia, is already compatible with liberal democracy in its classical, state-enforced form. It made a narrower and, I think, more useful claim: that a specific, limited kind of sharia observance—personal-status law administered by community courts that operate underneath, not above, a rights-protecting state—has a long working history in exactly the kind of societies Dr. Brubaker may want to defend: Israel and Greece, the latter being more liberal thanks to the European Court of Human Rights. If I had more space, I could add other non-Muslim states such as India, Thailand, Singapore, or Sri Lanka, which also maintain sharia courts for their Muslim citizens, adjudicating family matters such as marriage and divorce without violating national constitutions or laws.

These examples do not show "what Akyol wishes sharia to be," in Dr. Brubaker's words. They show existing realities in the world, which are much more complex than what most of the contemporary sharia alarmists in America imagine.

None of this means I minimize the problem posed by the violent and coercive side of sharia, in its premodern/imperial or modern/Islamist formulations: a full legal order complete with apostasy and blasphemy laws, corporal punishments, and legal discrimination. These are serious threats to freedom—which is exactly why my own work for over two decades has been about building and popularizing reformist Islamic arguments to abolish these illiberal elements from Islamic law and Islamic states. (I also personally know the threat is real, as the Malaysian religious police taught me in 2017 by detaining me for a public lecture where I argued there should be no apostasy laws and no religious police.)

On the other hand, I also recognize that a large share of the world's roughly two billion Muslims simply wish to practice their faith—prayer, dietary rules, modest dress, all parts of sharia in the broad sense—without any interest in imposing these on others. My argument is that such voluntary piety, even when it includes family law, does not violate or threaten freedom so long as individuals remain free to exit or opt out—much as with the practice of Jewish law, the halakha, by Orthodox Jews in the modern world.

Yet Dr. Brubaker seems unimpressed by these nuances, because he thinks in slippery-slope terms. "A small quantity of poison in a glass of water is a poor reason to drink it," he writes. In other words, he sees the illiberal elements in Islamic law as a reason to outlaw all of it. In fact, his title declares not just Islamic law, but more categorically "today's Islam," as incompatible with American liberty.

But this reasoning could be turned against nearly any group. Catholicism has its own long history of religious illiberalism, and there are Catholic integralists today who seriously aspire to remake America along theocratic lines. So, does that make all of Catholicism a glass of water with poison in it? Or consider white supremacists and their explicitly racist aims: Was the "woke left" correct to take them as reason enough to declare war on all "whiteness"? Instead of such categorical judgments, I believe the line should be drawn at freedom itself, applied evenhandedly to any comprehensive worldview, religious or secular. That means people holding illiberal views should still be free to take part in a liberal order so long as they follow its rules and respect the freedoms of others. That consistency is what keeps freedom coherent—and it is also what eventually helps illiberal minorities come to recognize and appreciate freedom's blessings for themselves. That second point seems to be lost entirely on today's sharia alarmists in the West, who treat Muslims' exercise of freedom as itself the danger. In their view, when Western Muslims pray, dress, or speak in explicitly Islamic terms, or

enter democratic politics to advocate for their views, freedom is under threat—because Islam is anti-freedom by definition. What these alarmists rarely consider is that the exercise of freedom is precisely what leads many Muslims to value it, as polls keep showing. A recent poll found that 67 percent of American Muslims are happy to "enjoy more freedom in America than anywhere else," and 95 percent of them feel "proud to be American." Yet Dr. Brubaker still may not be impressed, for he says that "sharia conforms to liberal norms when and only when a superior external power requires it to." In return, I would say there is truth in this, but so what? External realities, not just state regulation but also shifting norms and values, have pushed all our ancient religions to revisit teachings that once seemed permanent. Slavery was defended within both Christianity and Islam well into the modern era, and its abolition owed a real debt to outside pressure. Jewish communities became more individualist substantially because European liberalism sparked their own Haskalah, the Jewish Enlightenment of the 18th century, to which I pointed as an example for Islam today. In fact, Abrahamic traditions, Islam included, even carry a built-in theological rationale for absorbing such external pressures, a rationale that rests on two recognized sources of wisdom, *revelation* and *reason* — one as eternally fixed, the other as continuously unfolding.

Finally, I will grant that Dr. Brubaker is right to insist that full compatibility between liberalism and Islam will be possible only once Muslims honestly confront the real tensions between the two. So, I agree with these words of his:

Until someone inside the tradition with genuine scholarly authority explains how Muhammad's commands on apostasy and blasphemy are permanently inapplicable — without abandoning the prophethood that makes his words authoritative — the constitutional conflict…remains.

Yes indeed, and that is precisely the challenge my newly released edited volume, *No Compulsion in Religion—No Exceptions: Islamic Arguments for Religious Freedom* (Cato, 2026), takes up directly, with chapters on apostasy and blasphemy laws as well as religious policing and gender discrimination, each authored by Islamic scholars working from within the tradition's own sources. Our Arabic, Persian, and Urdu editions are coming soon.

True, these reformist arguments have not yet won the day in Islam, but they are being seriously discussed among Muslims around the world. If they eventually do prevail, it will be in part because more Muslims come to see freedom as a noble and genuine ideal worth embracing. And that, in turn, will be possible only if freedom is understood to mean not only freedom *from* Islam, as Dr. Brubaker seems to focus on, but freedom *of* Islam as well.

Mustafa Akyol is a senior fellow at the Cato Institute's Center for Global Liberty and Prosperity, where he focuses on the intersection of public policy, Islam, and modernity.

Sweden considers the worst war scenario: Body bags and preparations for mass burials

Source: https://spotmedia.ro/en/news/news/sweden-considers-the-worst-war-scenario-body-bags-and-preparations-for-mass-burials

Sep 02 – The Swedish army organized a large-scale military exercise in the spring, with the objective of preparing for the possibility of an armed conflict. Body bags, a priest performing burial rituals for fictitious soldiers, and testing the resistance of refrigeration units demonstrate how far Sweden is willing to go in preparing for war.

Approximately 18,000 soldiers from 13 countries participated in the military exercise Aurora 26, held this year between April and May. It included training for handling fallen soldiers on the battlefield. According to a study published in the journal „Frontiers in Psychiatry", over 500 mannequins and body bags were used to simulate war casualties.

The exercise aimed to test the entire chain of procedures regarding the management of deceased victims in conflict: recovery of bodies, identification, notification to allied embassies and the International Red Cross Committee, as well as burial with military honors, as reported by Euronews.

Over 300 soldiers participated, along with representatives from the Church of Sweden, the Swedish Tax Agency, and the national recruitment agency.

This Hasn't Been Seen Since the '50s

The commanding officer told researchers, "I am proud to have taken part in this endeavor. The last time this was practiced was, I believe, in 1952, so I am proud to have contributed."

A military priest spoke about the visual impact, stating that the abstract reality of war victims suddenly became concrete after seeing dozens of body bags lined up.

The specialized publication Defence24 reported that it was the first time this process was jointly practiced by all major institutions. Officials presented the exercise more as a matter of morale and institutional

readiness rather than an estimate of the number of victims. A military medic noted that, following this testing, there will be a "major change" needed in terms of ensuring resources for medical teams in scenarios with a high number of casualties, while another soldier told researchers that the exercise provided them with "a clearer understanding of the consequences of war."

Planning for the Most Pessimistic Scenario

The Church of Sweden, the official authority responsible for national funeral services, has long been tasked with planning burial capacity equivalent to 5% of the country's population, around 500,000 people. This figure represents a civil defense benchmark from the Cold War era and includes deaths both among military personnel and civilians nationally, therefore it does not represent a forecast related to the Aurora 26 exercise or any specific estimate of the number of victims. This does not mean that authorities expect such a high number of casualties, clarified Jan-Olof Olsson, a representative of the Swedish Civil Defense Agency, to the daily Le Monde. "To plan, we need an estimate," he explained.

NATO Forces Trained by Ukrainian Experts

The spring military exercise is part of a broader effort in which the Baltic states and the northern flank of NATO simulate critical scenarios, amid persistent tensions with Russia, as reported by Euronews.

Within Aurora 26, Ukrainian drone specialists trained NATO troops in countering tactics, and forces from the USA, the Netherlands, France, Poland, and other allied states carried out operations in southern Sweden, on the island of Gotland, and in the Baltic Sea.

Sweden's participation in these exercises is remarkable. This country maintained neutrality in both world wars and during the Cold War and has not deployed troops on a mission since 1814.

EDITOR'S COMMENT: I think I recognize the place from a vsit in the past. But then, it was in Paris, France!

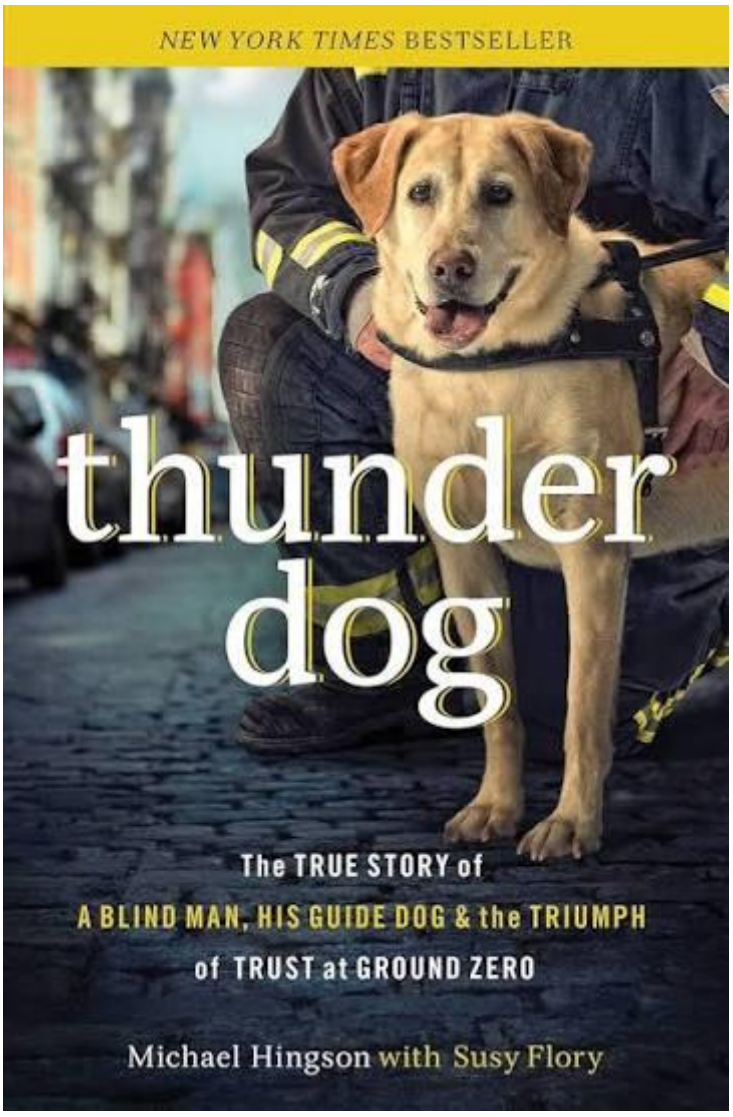
Ceuta – Animals do not kill for fun!

Michael and Roselle: A Story of Teamwork and Trust on 9/11

Source: https://www.911memorial.org/connect/blog/michael-and-roselle-story-teamwork-and-trust-911

Michael Hingson has been blind since birth due to a disease called retinopathy of prematurity (ROP). In his infancy, doctors suggested his parents send him to a home for the blind, where they could take better care of him. Michael's parents, however, decided that they would love and raise him in the same way they raised his older brother, Ellery. This decision gave Michael the chance to find his own way in the world, and he'd eventually land a managerial job at the Twin Towers.

On September 11, 2001, Michael and his guide dog, Roselle, started their day in New Jersey. Michael woke up a



little earlier than usual to prepare for a breakfast and a presentation scheduled later that morning. They rode a taxi to a New Jersey Transit station, caught a train and then transferred to a PATH train headed for the underground concourse at the World Trade Center.

Michael was working as regional sales manager and head of operations for Quantum/ATL, a data-protection agency, on the 78th floor of the North Tower. Michael set up the conference room for their breakfast meeting as Roselle took her position near the door to greet people.

Moments later, when Flight 11 crashed into the North Tower of the World Trade Center, Roselle was sleeping at Michael's feet underneath his desk. As the tower swayed and a loud boom rattled the office, Roselle remained very calm, which Michael said made him feel like he was in no imminent danger. The pair proceeded to walk down 78 flights of stairs together and successfully evacuated the building before its collapse at 10:28 a.m.

In 2011, Michael published their story in *Thunder Dog: The Story of a Blind Man, a Guide Dog, and the Triumph of Trust at Ground Zero*. He is now an experienced public speaker focusing on leadership, inclusion, disabilities, and other subjects. He also serves as ambassador for the National Braille Literacy Campaign for the National Federation of the Blind.

Roselle passed away on June 26, 2011, with Michael and his wife, Karen, by her side. They subsequently formed Roselle's Dream Foundation in her honor; the nonprofit charity educates people on blindness and assists blind children and adults in obtaining technology to help them navigate the world around them.

Immigration in Sweden: How the Country Went from One of Europe's Most Welcoming, to One of Its Most Restrictive

By Henrik Emilsson

Source: https://www.homelandsecuritynewswire.com/dr20260910-immigration-in-sweden-how-the-country-went-from-one-of-europe-s-most-welcoming-to-one-of-its-most-restrictive

Sep 10 – For decades, Sweden was known as one of Europe's most welcoming countries for refugees. It took pride in pursuing one of Europe's most generous asylum policies, and often presented itself as a humanitarian role model. But today it has one of the continent's most restrictive migration policies. That transformation has taken little more than a decade.

The turning point came during the 2015 refugee crisis. Sweden received more than 160,000 asylum applications, more than 12% of all applications in the European Union. Around 35,000 were unaccompanied minors, more than one third of the EU total that year. The scale of the inflow exposed strains on the country's system and fundamentally changed the political debate around migration.

The immediate response was a broad cross-party agreement introducing stricter asylum and family migration rules. This was followed by temporary border controls, and the replacement of permanent residence permits with temporary ones for most refugees.

These measures, introduced by a leftwing Social Democratic government, were more than a response to an exceptional situation. They signaled the emergence of a new political consensus: that Sweden should pursue a substantially more restrictive migration policy. The next decisive step came after the 2022 election. A center-right coalition led by Prime Minister Ulf Kristersson took office, with parliamentary support from the anti-immigration party the Sweden Democrats under the so-called Tidö Agreement. Although the Sweden Democrats remained outside the government, the agreement gave them substantial influence over migration policy and provided the political foundation for the most far-reaching package of migration reforms in modern Swedish history.

Drastic Restriction of All Migration Policies

Once in office, the new government embarked on the most comprehensive overhaul of Swedish migration policy in modern history. Since 2022, reforms have been introduced across virtually every area of migration policy, including asylum reception, refugee policy, family migration, labor migration, citizenship, return policy, detention and access to social benefits.

The government's stated ambition has been to make Swedish asylum policy as restrictive as possible, while continuing to comply with the minimum standards required under EU law and international refugee law. This restrictive policy direction also extends to other categories of non-EU

migration, including family and labor migration, while highly skilled labor migration constitutes an important exception.

The first reforms, including tighter rules on family reunification and humanitarian residence permits, entered into force in late 2023. At the same time, the refugee resettlement quota was reduced from 5,000 to 900 places annually.

Most of the broader reforms, however, were adopted only in 2025 and 2026. Access to social benefits such as parental leave and child support will become conditional on residence and employment requirements. Obtaining Swedish citizenship will be subject to stricter requirements relating to length of residence, conduct, language and civic knowledge, as well as self-sufficiency. The government has also substantially lowered the threshold for deporting non-citizens convicted of crimes.

This concentration of reforms towards the end of the parliamentary term reflects the Swedish legislative process rather than a late political shift. Major legislation is normally preceded by government inquiries, public consultations and parliamentary scrutiny, meaning that comprehensive reforms often take years to move from proposal to implementation.

Migration Ahead of the 2026 Election

The reforms have coincided with a dramatic decline in asylum applications. In 2025, Sweden registered around 6,700 first-time asylum applications, with an approval rate of 23%. On a per capita basis, this was less than half the EU average. Sweden has therefore gone from receiving one of Europe's highest numbers of asylum seekers per capita in 2015 to one of the lower a decade later. According to the Swedish Migration Agency, asylum applications are expected to fall further, to around 4,200 in 2026 and 3,700 in 2027. Equally striking is the wider political change. There is now broad consensus among Sweden's major political parties in favor of maintaining a restrictive migration policy. The Social Democratic Party, which governed during the 2015 refugee crisis, has actively or tacitly supported most of the current government's reforms. The party has made clear that the restrictive direction of Swedish migration policy will remain in place if they return to government. Public opinion has also shifted, alongside policy. After the 2015 refugee crisis, a growing share of Swedes now favor lower levels of immigration, especially refugees. The Social Democrats have been inspired by the electoral strategy of the Danish Social Democrats, who before the 2019 election pledged to maintain the restrictive migration policies introduced by previous governments. Their aim was to reduce the importance of

migration as an election issue and shift the political debate towards welfare, employment and the economy.
The Swedish Social Democrats appear to be pursuing a similar strategy ahead of the 2026 election, signaling that they will not reverse the government's main migration reforms.
The governing parties, by contrast, have every incentive to keep migration at the center of the election campaign. They argue that a Social Democratic government would depend on parliamentary support from the Green Party and the Left Party, both of which favor a more liberal migration policy.
The election is therefore likely to focus less on whether Sweden should maintain a restrictive migration policy, than on whether a future government can be trusted to do so.

Henrik Emilsson is Senior lecturer, Faculty of Culture and Society, *Malmö University*.

Will a Finnish Fence Make Russia a Good Neighbor?

By Peter Suciu
Source: https://nationalinterest.org/blog/buzz/finland-border-fence-russia-ps-091126

Sep 11 – Finland has completed construction of a fence along its Russian border. Officials hope it will stop "instrumentalized immigration" and prevent a potential Russian invasion.
When historically neutral Finland joined NATO in April 2023, it effectively doubled the alliance's shared border with Russia. Finland shares an approximately 833-mile (1,340-kilometer) border with Russia and, until recently, it was largely unfenced and lacked other physical barriers such as walls or wires. It was one of the most heavily monitored and strictly managed borders in Europe, with electronic surveillance and highly trained patrols on both sides.
Now, this month, there is a true demarcation, as Finnish officials announced that the country had completed a project to install a border fence that began three years ago. "I

think it's good that at some point we assess whether more of this is needed. What we particularly need is EU funding for eastern member states so that projects like this can be financed," Finnish Interior Minister Mari Rantanen told reporters while speaking at a news conference near the Nuijamaa border in the country's southeast.

Why Finland Decided to Build a Fence on Its Russian Border

Finland was a self-governing Russian territory (officially, an autonomous grand duchy) from 1809 to until 1917, when it declared independence from the Russian Empire.

The country kept its border open—but guarded—for more than a century.

Finland, along with neighboring Sweden, remained neutral throughout the Cold War; both nations sought to join NATO after Russia's unprovoked invasion of Ukraine in February 2022.

Later in 2022, Finnish officials decided to build the border fence. Finland closed its border with Russia in 2023.

A year later, Finland accused Russia of "instrumentalized migration," which it described as the "deliberate pushing of large numbers of asylum seekers to a border checkpoint as a hybrid warfare tactic." It passed a law allowing border guards to block asylum seekers from entering the country. The law was originally enacted for one year, but Finnish officials keep extending it.

"In this situation, every state must take care of its own security and the inviolability of its borders," Rantanen said recently.

About the Finnish Border Fence

Construction of the Finnish border fence began as a pilot project near Imatra, northwest of the Russian city of St. Petersburg, in April 2023.

The fence does not cover the entirety of the border.

"The longest sections of the fence are located in the southeast of Finland, totalling some 140 kilometres," according to the Finnish broadcasting company Yle. "There is also about 35 kilometres of fence in the North Karelia region, while additional sections of about 25 kilometres stretch across Kainuu and into Finnish Lapland.

The parts of the Finnish border that are not fenced have large bodies of water, swampland, dense forest, or other natural features that make a fence unnecessary and expensive.

Landmines and Dragon's Teeth Protect Other Borders with Russia

Similar fences have been installed in Estonia, Latvia, Lithuania, and Poland on their borders with Russia or Belarus to counter the flow of migrant crossings and attempt to block a Russian invasion.

The three Baltic States, which were all previously unwilling Soviet republics until they fully restored their respective independence in 1991, have also gone far beyond just a border fence.

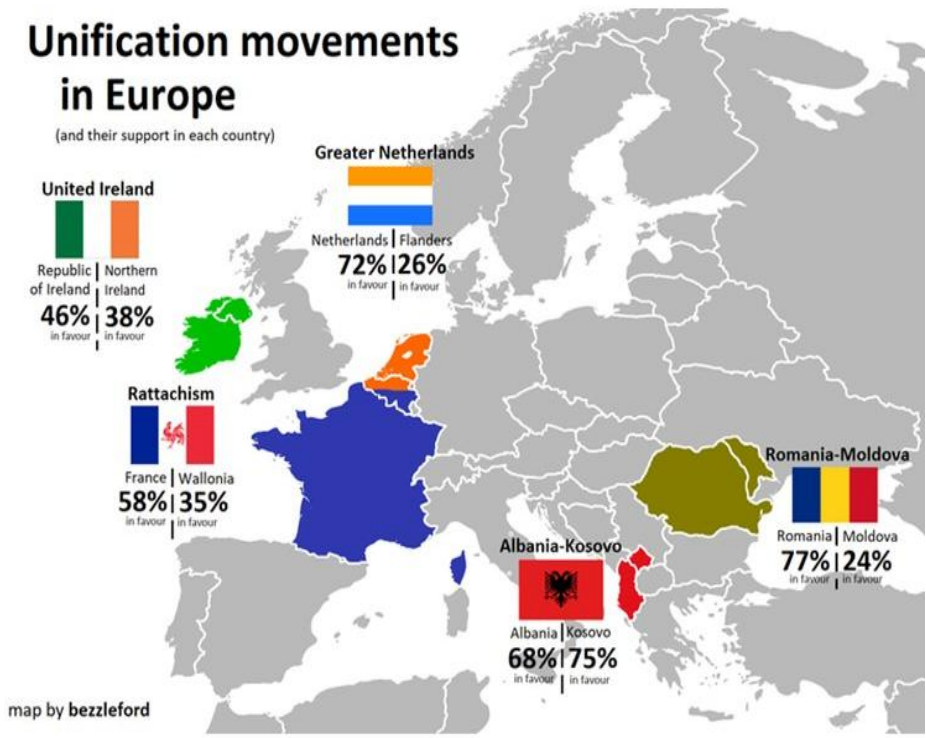
A year ago, Lithuania began to build anti-tank "dragon's teeth" along the frontier of the Russian exclave of Kaliningrad and the border with Belarus. It is part of a string of militarized positions throughout Lithuania, Latvia, and Estonia, which include anti-tank ditches, barbed wire, and even a strip of land where anti-vehicle and anti-personnel landmines could be laid if a military threat is perceived.

In February, Estonia also procured approximately 600 modular bunkers that are being installed along the Russian border. The hardened structures were meant to fortify the ongoing efforts to install "delay-rated" fences designed to resist forced entry.

Peter Suciu has contributed to dozens of newspapers, magazines and websites over a 30-year career in journalism. He regularly writes about military hardware, firearms history, cybersecurity, politics, and international affairs. Peter is also a contributing writer for *Forbes* and *Clearance Jobs*. He is based in Michigan.

EDITOR'COMMENT: Why it is OK with Finland to install mines in its borders with Russia, but it is not OK for Greece to do the same in its fence with Turkey?

British soldier with the Household Cavalry Mounted Regiment rides a horse fitted with a camouflage covering during a training exercise in England, June 2026.



Warfare is Losing Its Humanity

By Ella Hummel
Source: https://www.cpreview.org/articles/2026/9/itd5vpqwd1k089xph2b97zz33755sk

Sep14 – Throughout human development, as new technologies have emerged, it has become easier to alienate ourselves from the act of killing. Bows and arrows were among the first weapons to be invented, creating distance between the hunter and hunted. Later, gunpowder weapons, such as cannons and guns, increased the efficiency of warfare. The development of weapons of mass destruction over the past century allowed for the instantaneous erasure of hundreds of thousands of lives. With each development, the two sides of conflict–the aggressors and the victims–have grown more distant from each other. Now, artificial intelligence (AI) offers humans the ability to relegate the violent decisions and actions of war to algorithms and technology, leaving humans as solely the victims.

As countries compete for both military and technological advantages, it is imperative that we do not continue to further alienate ourselves from the violence of war. While the use of AI offers militaries increased efficiency and speed of attacks, it detaches the sentiments and feelings, key aspects of our humanity, that are often associated with the harming and killing of others.

This alienation can be seen through the ever-growing implementation of AI into military operations. On January 3, 2026, the United States launched air strikes throughout Venezuela and led a raid on Venezuelan president Nicolás Maduro's safe house, capturing him. The strikes were planned with the help of Claude, an AI chatbot created by the American AI company Anthropic.

However, the January 2026 takeover of Venezuela directly conflicts with Anthropic's terms and conditions, which prevent their technology from being used for the development of weapons, planning offensive operations, and domestic surveillance. Further, the company was not alerted of the technology's use in the takeover until an inside contact confirmed the involvement shortly afterward.

Anthropic was founded by siblings Dario and Daniela Amodei after they left OpenAI in 2020, citing concerns with the ethical usage of AI. Dario has been a vocal advocate of the potential benefits of AI technologies, while also warning against growth without limitations. He believes that the ultimate goals of the human race include achieving the ideals of the rule of law, autonomy, and democracy. Dario holds hope that, "AI simply offers an opportunity to get us there more quickly—to make the logic starker and the destination clearer."

In contrast, companies like xAI and OpenAI believe that AI is the future of military actions. They see the rapid development of AI technologies as a new frontier of warfare between the US and its adversary, China, similar to the Cold War arms race. Yet, the rapidity of the development of AI often comes at the cost of ensuring moral safeguards for the technology.

Anthropic's collaboration was intended to expand the powers of the Department of War (DOW) by supplementing its work with the capabilities of AI programs. This included experimenting with new methods of combat through artificially created scenarios, assisting with war planning, and ensuring the US has an advantage in the development of new technologies.

The extent of the government's use of Anthropic's technologies remains unclear. While it was reported that Claude was used in the Venezuelan air strikes, Anthropic officials initially refused to confirm the technology's role in the takeover. Soon afterwards, though, Anthropic and the DOW engaged in a public dispute over the two's

relationship, revealing their disagreement on how the technology should be applied. At the root of the controversy are the restrictive terms regulating Claude, which limit the technology from being used for fully autonomous weapons and mass domestic surveillance.

Secretary of War Pete Hegseth gave Anthropic a deadline of February 27, 2026 to compromise with the government on the terms of use for Claude. In the final hours of the negotiations, the DOW was willing to concede to the prohibition of the use of the technology for surveillance or the development of entirely autonomous weapons. However, it remained keen to use the technology to analyze internet searches, individuals' travel or movements, and credit-card transactions. Anthropic was unwilling to meet this demand. After unsuccessfully trying to contact the founders to finalize negotiations, Hegseth announced that the DOW's contract with Anthropic would be terminated. He also declared the company a supply chain risk, meaning that it could be at risk of sabotaging government operations for surveillance or offensive purposes, effectively blacklisting the company within the federal government. The company has since sued the DOW in two federal lawsuits. In March 2026, the US District Court for the Northern District of California ruled in favor of Anthropic, allowing the company to maintain its federal contracts with defense agencies. However, on April 8, 2026, the US Court of Appeals for the District of Columbia Circuit denied Anthropic's motion against the government and prevented it from creating new contracts with the DOW. The ongoing court cases will determine not only the economic vitality of the company, but also the scope of the federal government's capacity to declare domestic companies as threats.

The DOW has since signed agreements with other AI companies. In February 2026, xAI signed a deal with the DOW and was granted classified use. Then, just a day after the split with Anthropic, the DOW finalized a deal with OpenAI. Both companies require use of their technologies to "comply with the law" by adhering to copyright, respecting rights to privacy, and abstaining from espionage. Additionally, they cannot "harm people or property," specifically referring to "unauthorized actions on behalf of others" and developing "bioweapons, chemical weapons, or weapons of mass destruction."

In the days following the termination of Anthropic's relationship with the DOW, Claude was the number one most downloaded app, beating out ChatGPT. This spike in interest presumably followed the exposure of the technology in the news cycle, but was also in part due to a larger movement of individuals purposefully moving away from the use of ChatGPT. QuitGPT is a protest movement encouraging individuals to stop using OpenAI's technologies. Among other reasons, the drive discourages the use of ChatGPT because OpenAI's president, Greg Brockman, was the largest Trump donor in 2025, and OpenAI's GPT-4 technologies have been used in ICE's resume screening tool. The movement has been growing steadily and saw a jump in interest following the announcement of OpenAI's contract with the DOW.

When Anthropic lost its contract with the government, it demonstrated its commitment to creating the moral line in the development of AI. This move places the company in a lucrative position to be the moral paradigm in an industry filled with immoral companies and leaders. As more of the actions of war are ceded to AI, Anthropic has fought to limit the dominion of the technology. However, how much Anthropic can truly preserve humanity in a field dedicated to replacing humans remains to be seen. As the technology continues to advance, we need to ensure that we preserve our humanity alongside it.

Ella Hummel (CC '28) is a staff writer at CPR studying political science and comparative literature.

EDITOR'S COMMENT: Excuse my language, but what a stupid title! Humanity in Warfare! Killing and Compassion?


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/

Fears of Islamist terrorism in the United States

By Shahid Javed Burki

Source: https://tribune.com.pk/story/2625454/fears-of-islamist-terrorism-in-the-united-states

Aug 24 – There are growing fears of domestic terrorism inspired by Muslim groups active in the United States. Deciding whether an association should be labeled as a terrorist organisation is the domain of the federal government. The authorities in Washington, in reaching the determination that an organisation is a terrorist group, draw on the vast domestic antiterrorism intelligence infrastructure and globe-spanning intelligence services. Much of this was developed after the attacks of September 11, 2001 in which thousands of people were killed. Now some Republican governors are getting into the game. In recent months, the leaders of Texas and Florida have formally designated some groups as terrorist organisations. Both states have conferred the designation on the Council on American Islamic Relations, or CAIR, one of the largest Muslim civil rights groups in the country.

CAIR is a 32-year-old non-profit organisation with headquarters in Washington and chapters in more than 20 states. It has long been targeted by conservative Christan groups. CAIR is challenging Florida and Texas in court, arguing that they violate its rights to free speech, assembly and due process. The stakes are high, particularly in the southeastern state of Florida where a new law makes it a felony to knowingly offer "material support" for a designated terrorist organisation, and allows the state to dissolve such groups in some situations. If the move survives the legal challenge, it is likely to force the permanent closure of CAIR's Tampa-based organisation which says it represents a Muslim community in Florda that numbers more than half a million people. Some right-wing Republicans have taken to targeting CAIR, at a time when prominent conservatives have been portraying Islam as incompatible with American values. In 2016, when Donald Trump was elected for his first term as the United States president, he said in an interview that "I think Islam hates us." Other senior political figures also spoke against Islam and those who were prominently engaged in defending the religion. In 2025, Senator Tom Cotton called upon the Department of Education "to ensure that CAIR is not given an opportunity to push its radical, pro-terrorist, anti-Israel ideology on American schoolchildren". In January 2026, Representative Jason Smith, Chairman of the House Ways and Means Committee, asked the Internal Revenue Service to revoke the tax-exempt status CAIR's California Chapter for, among other things, supporting pro-Palestinian protesters on college campuses. In a social media post prompting the law aimed at curtailing the influence of Muslim organisations, Florida Governor Ron DeSatntis wrote: "We have a responsibility to defend and reinvigorate Western Civilization and that means protecting against creeping sharia in all forms." In 2023, the Biden White House condemned the CAIR's director, Nihad Awad, after it was revealed that he had told a group, American Muslims for Palestine, that he was happy to see Palestinians "break the siege, the walls of the concentration camp on October 7", the day of the Hamas-led attack on Israel killing roughly 1,200 people. Awad, in his defence, said that his remark was taken out of context. In Florida, Governor Ron DeSantis, a staunch supporter of Isreal, has a long history of feuding with CAIR Florda, which has proclaimed its support for the Palestinians and wants their fundamental rights to be free from the Israeli occupation.

The state of Texas led by Governor Greg Abbot designated CAIR as a terrorist organisation in November 2025, citing testimony from the Holy Land

Foundation trial in which an FBI agent described CAIR as front group for the Palestinian organisation Hamas. Governor Abbot said his move bans CAIR from buying or acquiring land in the state. In a statement, Andrew Mahaleris, a spokesman for Governor Abbot, said the governor's actions "are targeted at radical groups that seek to forcibly impose sharia law on Texans".

"The states were shaping up as potential battlegrounds," wrote Richard Fausset in a long article he contributed to The New York Times and published by the newspaper on August 7, 2026 under the caption, "Muslim nonprofit gets terrorism label in Florda and Texas." Continued Fausset: "This year, bills were introduced in several Republican-led states, including Louisiana. Oklahoma and Arizona that would have given state officials the power to designate groups as terrorist organizations, according to Elly Page, a senior legal adviser with the International Center for Not-for-Profit Law. Those proposals did not become law but in Indiana, a new law allows the governor to designate groups as affiliates of federally designated terror groups."

Several Muslim leaders were deeply concerned at the open expression of anti-Muslim sentiments by prominent political figures and rightist political organisations. "CAIR is probably at a place where it's in more danger than it's ever been before," said Farid Senzai, an associate professor of political science at Santa Clara University who studies Muslims in America. She was quoted in the above mentioned article by Fausset.

Islam has been seriously studied by American scholars, notably Dr John Esposito who died at the age 86. He opened doors across the Muslim world and drew international experts to conferences he sponsored. In 1993, he was recruited to become the founding director of the Alwaleed Center for Muslim-Christian Understanding which was named in 2005 after Saudi donor, Prince Alwaleed bin Talal. In a book co-authored by Esposito and Dalia Mogahed, Who Speaks of Islam? What a Billion Muslims Really Think, the authors based their work on Gallup surveys in 35 Muslim countries. They told their readers that the vast majority of Muslims condemned 9/11 and supported peace, democracy and women's rights. Only 7 per cent said they condoned 9/11.

In recent years, Esposito directed a research project called the Bridge Initiative housed in Washington's Georgetown University that monitored issues related to Islamist bigotry around the world. "Islamophobia as I define it," he told the Daily Oklahoma in 2014, "is not about people who have a kind of good fact-based criticism of the Islamic religion. Theirs is nothing negative about that. People are entitled to those types of criticism. Islamophobia is when you have an unfounded irrational fear that tends then to lead to bias, discrimination, hate speech and hate crimes."

Shahid Javed Burki is a former caretaker finance minister and served as vice-president at the World Bank.

Italian Police Arrest Teenage Female Jihadi Over Explosive Vest Blueprints on Phone

By Jules Gomes | Biblical scholar and journalist based in Rome.
Source: https://www.meforum.org/fwi/fwi-news/italian-police-arrest-teenage-female-jihadi-over-explosive-vest-blueprints-on-phone

Aug 22 – Italy's counter-terrorism police have arrested a 17-year-old girl of Egyptian origin who was planning a suicide bomb attack and had downloaded blueprints for making an explosive vest, while

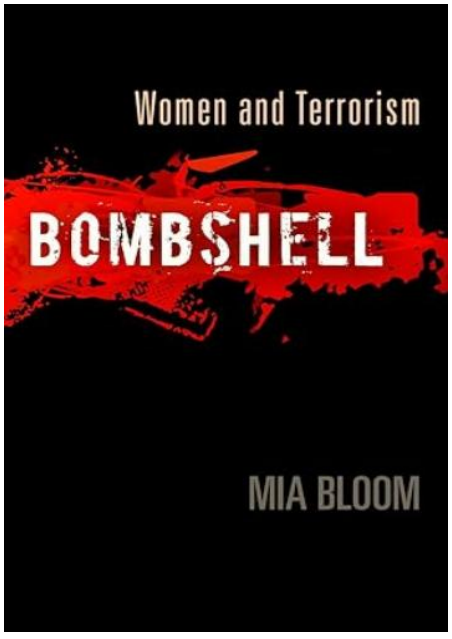
declaring herself ready for martyrdom "in the name of Allah."
Police said that the alleged jihadi regularly frequented Islamist chatrooms and shared propaganda material linked to the Islamic State, including hymns glorifying martyrdom, recruitment videos, and manuals for manufacturing homemade weapons and explosives.
Nearly half of all Muslims under the age of 40 harbor Islamist views.
A state police press release said that the female was arrested on July 17 after investigators identified a suspicious user on an instant messaging platform who used a virtual phone number to frequent four restricted channels accessible only by invitation or with the administrator's approval. The suspect cannot be named because she is under 18.
Police recovered digital conversations with peers, including foreigners and suspected Islamic State radicals, with whom the girl exchanged videos and other digital material and where, "on several occasions, she had explicitly expressed her desire for martyrdom in the name of Allah," the press statement noted.
The juvenile prosecutor's office said that the evidence gathered outlines "an advanced process of radicalization" and, above all, "the concrete possibility of imminent violent activation."
The accused jihadi, who has been remanded in custody by the Milan Juvenile Court, resides in Villanterio, a municipality of 3,500 inhabitants, located in the province of Pavia, in Italy's northern region of Lombardy.

Second Teenager Arrested in Northern Italy

On August 7, a police statement reported that a 16-year-old male from the province of Como was arrested in Grosseto, where he was on vacation with his family. Officials charged the teenager with participating in an international terrorist organization and disseminating propaganda and incitement to crime based on racial, ethnic, and religious discrimination. Police found several conversations and content attributable to jihadist propaganda, along with other neo-Nazi and anti-Semitic material.

Tunisian Minor Arrested for Downloading Explosives Manual

This isn't the first time minors from the northern region of Italy have been detained for links to Islamist terrorism. In November 2025, police arrested a boy of Tunisian origin in Pavia who downloaded multiple manuals for manufacturing explosive devices using readily available household materials.
Police charged the suspect with participating in Islamic State activity and incitement to commit terrorism related crimes, aggravated by the use of computer and telecommunication devices. The boy had repeatedly expressed his desire to fight in an Islamist conflict zone.
The minor was also actively proselytizing within the radicalized network, convincing others, including minors, to swear allegiance to the Islamic State. Police also apprehended and searched a minor of Egyptian origin, who was part of the same group but residing in Milan.



Experts Warn of European Surge in Female/Child Jihadis

Counter-terrorism experts have issued repeated warnings about the propagandistic techniques used by Islamist terrorist groups to recruit female jihadis. In her book, Bombshell: Women and Terrorism, Mia Bloom warns that "the number of female terrorists and suicide bombers has

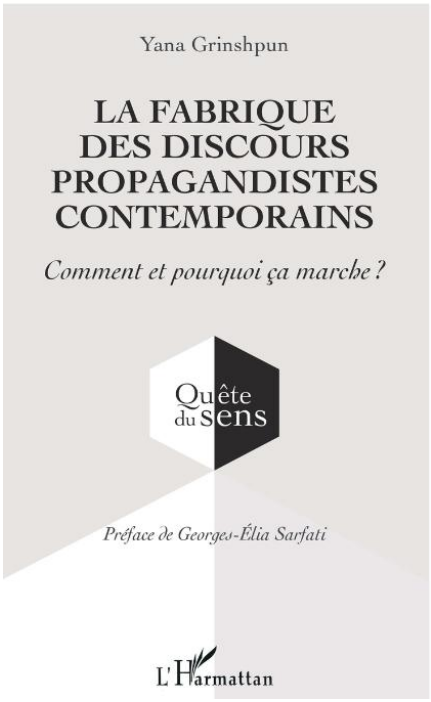
increased several hundredfold in the past few years."

Bloom predicts that "the women in Islamist organizations would increasingly be the focus of the next generation of Al Qaeda leaders" and writes that groups like ISIS are wooing women and girls via social media platforms including Facebook, Twitter and Tumblr.

Problem in France

Europe is experiencing a surge in teenage jihadis, according to reports from multiple intelligence agencies. France now investigates more than one case of jihadi terrorism each week, reaching a new high since it created the National Anti-Terrorist Prosecutor's Office (PNAT) in 2019.

PNAT officials warned of growing numbers of radicalized "child soldiers" participating in "Islamist-inspired crimes and offenses," such as a 13-year-old girl's foiled February plan to attack a synagogue or Shiite mosque, *Focus on Western Islamism* (*FWI*) reported.



PNAT began investigating 118 new cases between January 1, 2024, and November 27, 2025, coinciding with a rise in the number of jihadi "child soldiers" and young adults.

In 2025, the anti-terrorist prosecutor's office charged 20 minors with Islamist terrorism, compared to 19 in 2024, 15 in 2023, and 2 in 2022. Seventy percent of those involved in jihadist violent action plans in 2024 and 2025 were under 22 years old. PNAT also arrested 130 minors with ties to the jihadist movement between 2023 and June 2025, with varying legal outcomes.

In March, a 17-year-old French-Turkish youth was arrested for planning a knife attack. In June, police arrested a 17-year-old French-Algerian for allegedly attempting a terrorist attack on Notre-Dame Cathedral, a nightclub, and a concert by the rapper Jul. In November, police arrested the ex-girlfriend of Salah Abdeslam, the mastermind behind the Bataclan theater massacre, for planning a jihadi attack with her new husband and a 17-year-old minor.

The most recent case involving minors saw the arrest on November 30 of two 16-year-olds, one of whom is Chechen, for threatening an attack on a synagogue. PNAT charged the pair with "participation in a terrorist criminal association to prepare one or more crimes against persons."

Responding to a question from French parliamentarian Michèle Tabarot, Bruno Retailleau, France's minister of the interior, confirmed that the proportion of minors among individuals actively monitored for Islamist terrorist activity has tripled, rising from 1.7 percent in 2020 to 5.6 percent.

Social Media a Problem

Intelligence agencies have also confirmed that extremist radicalization is taking place largely through the internet and social media.

"One of the key factors is, of course, the role of social media and its growing presence in the everyday lives of adolescents," Yana Grinshpun, senior lecturer at the Sorbonne University and author of *The Making of Contemporary Propaganda Discourse: How and Why Does it Work?* told *FWI*. "More than 80 percent of young people in Europe use social media networks daily."

"This global phenomenon creates an environment that can be exploited by a variety of ideological and propagandistic movements, including Islamist organizations, which have developed sophisticated strategies for disseminating propaganda across multiple communication channels,"

Grinshpun, a researcher for the Transatlantic

Institute for the Study of Contemporary Ideologies (TISCI), explained.

Former member of the Muslim Brotherhood Mohamed Louizi explains in his book *Pourquoi j'ai quitté les Frères Musulmans* (*Why I Quit the Muslim Brotherhood*) how the "organization has sought to use Europe as a space in which to disseminate and establish, over the long term, an Islamist narrative adapted to local cultural contexts," Grinshpun observed.

Nearly half of all Muslims under the age of 40 harbor Islamist views, often driven by

intensive engagement with online content created by artificial intelligence (AI) and messages broadcast on social media sites like Discord, Instagram, and TikTok, a German government-backed study revealed in April 2026.

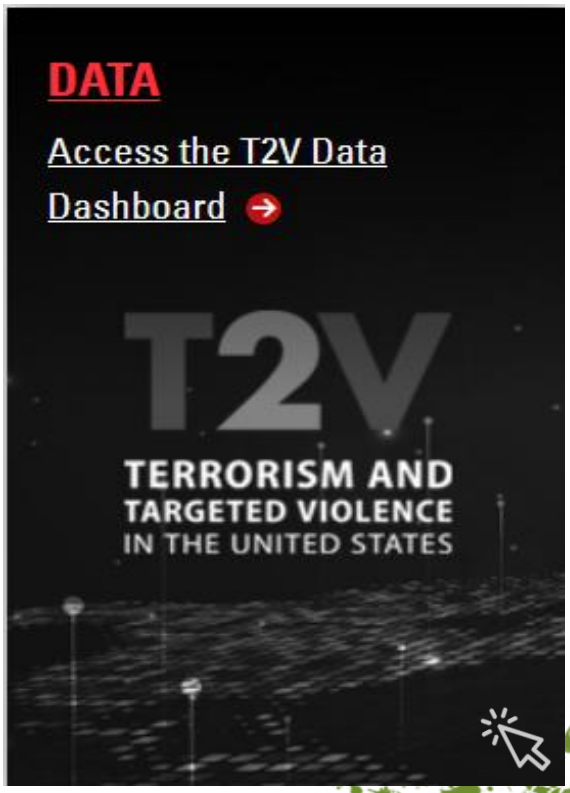
Using AI, Islamist outlets can now quickly produce convincing extremist content in various ideological styles and formats, including text, images, spoken language, or videos. At the same time, simplified content increases the number of young people exposed to the propaganda.

Terrorism and Targeted Violence (T2V) in the United States: Overview of 2023-2025 Data

Source: https://www.start.umd.edu/publication/terrorism-and-targeted-violence-t2v-united-states-overview-2023-2025-data

Abstract

This research brief provides an overview of 2,976 terrorism and targeted violence crimes that were committed in the United States from January 1, 2023, through December 31, 2025. The data for this brief are provided from the Terrorism and Targeted Violence (T2V) in the United States database, which includes comprehensive information on 2,976 premeditated successful, failed, and foiled attacks in the U.S. and its territories that were designed to have a significant impact on public safety or the security of critical infrastructure and key resources. The T2V data include terrorism events, premeditated hate crimes, school-based targeted violence, workplace targeted violence, and public mass violence events that were motivated by personal grievances. More information about the T2V database can be found in the "About T2V" section at the conclusion of this brief. The analysis presented here explores the types of events, locations, targets, weapon types, ages of perpetrators, intended plot types (e.g., property crime, low casualty attack, mass casualty attack), and outcomes of the events.



Terrorism and Targeted Violence (T2V) in the United States: 2024 vs. 2025

	2024	2025
Terrorism Events	235	332
Violent	75.3% (177)	82.2% (273)
Successful Mass Casualty Attacks	6	10
Successful Terrorism Events	40.8% (96)	38% (126)
Failed Terrorism Events	6% (14)	8.1% (27)
Foiled Terrorism Events.	53.2% (125)	53.9% (179)
Victim Fatalities	10	42
Victim Injuries	93	205
Events Resulting in Victim Casualties	16.2% (38)	16.3% (54)
Number of Events Involving Juvenile Perpetrator	7	19
Terrorism Events Targeting Government Personnel/Facilities	21.3% (50)	37.7% (125)

The End of the American Middle East

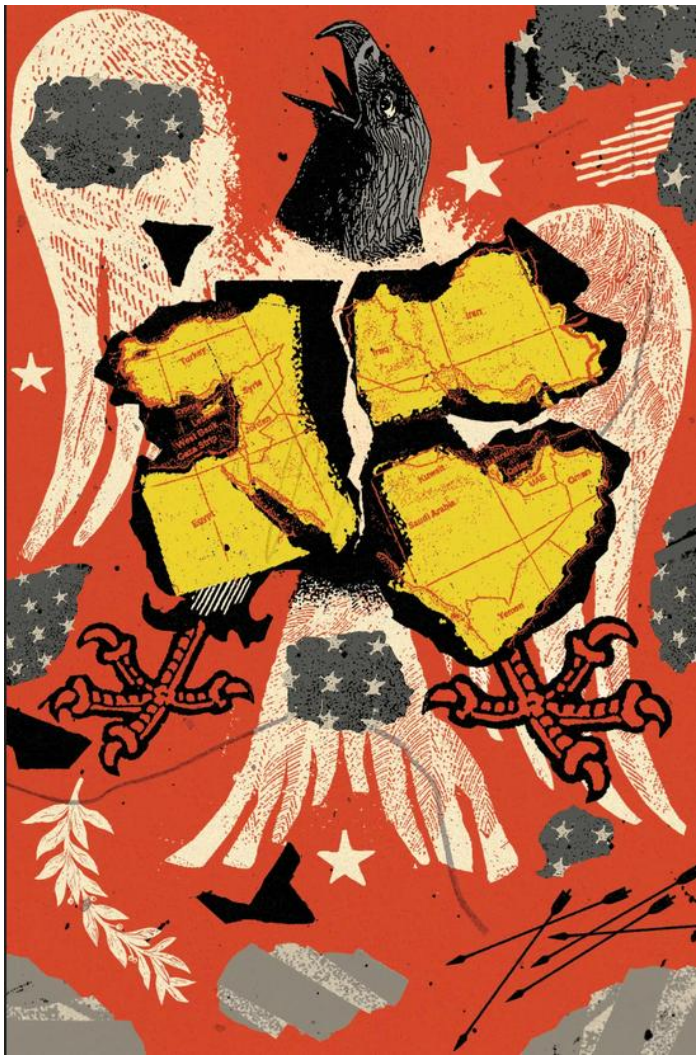
By Marc Lynch

Source: https://www.foreignaffairs.com/united-states/end-american-middle-east-iran-marc-lynch

Aug 18 – The American Middle East is finished. The regional order that has prevailed since 1991 has been one of the many casualties of the U.S.-Israeli war with Iran. The American and Israeli failure to dislodge the regime in Tehran has proved the bankruptcy of decades of sanctions and violence. The inability of the United States to protect its Gulf allies from Iranian attacks or to keep the Strait of Hormuz open has fatally undermined the core security bargain that justified its network of military bases in the region. And Israel's increasingly threatening posture and abandonment of any pretense of interest in reaching an accommodation with the Palestinians have ended Washington's decades-long mission of bringing its Arab allies and Israel together into an enduring security partnership.

The United States' primary goal for three and a half decades has been to lock its disparate allies into an order built around protecting Israel while containing, at first, Iran and Iraq, and more recently Iran and its nonstate allies. Far from being a deviation from that strategy, President Donald Trump's war took it to its logical end, seeking to remove the Iranian threat by force in one fell swoop. As American

leaders did before the 2003 invasion of Iraq and Israel has done in its wars against Hezbollah and Hamas, the architects of this war vastly exaggerated what military power could achieve, underestimated the capacity of adversaries to adapt, took for granted that allies would fall in line, and callously disregarded the lives of ordinary people. Washington's misadventure was not an aberration so much as the ultimate expression of the inherent vice of its Middle East strategy.



At first, it may not look as though the war has had much effect on the alliances that form the American order. Facing an inconclusive war and an empowered Iran, the Gulf states may ramp up their arms purchases and their demands for renewed security guarantees, creating the illusion of continuity. But the old order is in fact giving way to something new. The 1956 Suez crisis is remembered today as the last gasp of British and French imperial power in the Middle East, but it took years to reach that inevitable end. American primacy will not disappear immediately, either, but long-building doubts about American power and purpose have passed their tipping point. The revelations of the Iran war and of the Israeli war in Gaza before it have already changed the calculations of U.S. allies and adversaries. Another round of fighting or the election of a different American president will not repair the rupture.

The years ahead promise further discord. Israel and Iran have a shared interest in keeping the Middle East in a state of lawlessness and violence, and the United States has few means of holding back either of them. Israel hopes to expand its de facto borders, including by annexing as much as possible of historic Palestine, and to impose its writ by force across vast swaths of the region. And assuming that the Iranian regime does not collapse any time soon—which it appears highly unlikely to do—an emboldened Tehran will hope to defend and expand its regional influence by bogging Washington down in the kinds of endless, borderless "gray zone" conflicts in which it has always thrived.

If the United States is finally willing to abandon its failed strategy, however, the collapse of one order could still be an opportunity to build a new and better one. The conditions, admittedly, are far from ideal. Although most of the region's leaders and publics desperately want a respite from military strikes and economic disruption, they also deeply resent Washington for dragging them into a disaster. But discarding its policy of support for autocrats, impunity for allies, and militarized containment of enemies might enable the United States to engage with the region in a healthier way—one that eventually could yield the

durable stability Washington has claimed to want all along.

CRACKS IN THE FOUNDATION

For many decades after World War II, American ambitions in the Middle East were defined by its global competition with the Soviet Union, which gave Washington an outsize interest in regional politics but made it wary of overt military intervention. The current Middle East order, established by the George H. W. Bush administration after the collapse of the Soviet Union and the liberation of Kuwait from Iraqi occupation in the Gulf War of 1990–91, has been defined by American primacy. Presented with a historic opportunity to secure uncontested dominance over a long-contested region, Washington made itself indispensable by setting up military bases and security arrangements to contain Iraq and Iran. Its military and political support underpinned the survival of nearly every regime in the region.

To legitimize its role as something more than predatory domination, Washington launched the Arab-Israeli peace process in hopes of integrating its Arab allies and Israel into a common security framework. The result was a region divided between an American-led bloc that included Israel, Turkey, and almost every Arab state, and an opposing, less formal bloc that included Iran, Syria under the Assad dynasty, and nonstate actors such as Hamas, Hezbollah, and the Houthis. This structure remained remarkably unchanged through three decades of dramatic changes in global, regional, and American politics.

In the American telling, this order has provided a degree of stability while protecting core U.S. interests such as the oil trade, Israeli security, and counterterrorism. And in many ways, that has been true. Israel has not faced a state-level threat or fought a war against a peer competitor since 1973, which perhaps led it to underestimate the challenge of attacking Iran. Arab countries have worked with Israel against their common enemies despite the lack of a just solution to the Israeli-Palestinian conflict. For the most part, oil has flowed consistently at reasonable prices. No rival great power has seriously challenged American primacy—not even China, which has been content to sit back and take advantage of the economic opportunities made possible by the American provision of security.

For Washington, the strategic benefits accrued from this order seemed to justify the costs of the wars required to sustain it. But the price was much higher for those who live in the region. The past 35 years have seen Israel enter numerous smaller wars against its much weaker neighbors, the Israeli-Palestinian peace process completely fall apart, Hamas attack Israel on October 7, and Israel subsequently embark on the destruction of Gaza. In Iraq, the United States inflicted a dozen years of punishing sanctions, intermittent bombing, and failed regime change and counterproliferation efforts, followed by the disastrous 2003 invasion and occupation, all at tremendous human cost. Under American stewardship, catastrophic wars have shattered Lebanon, Libya, Sudan, Syria, and Yemen.

The regional order rested on American security guarantees not only to Arab states but also, critically, to the autocrats who sat atop them. Keeping democratic aspirations at bay was as vital to this bargain as protection against Iranian military attack. For a brief moment during the 2010–11 Arab uprisings, the drive for change seemed unstoppable, but otherwise the arrangement worked. Nearly all regimes within the American alliance system held on to power; most tightened their grip in the protests' wake. American support for neoliberal economic reforms encouraged those regimes to pursue privatization schemes that turbocharged elite corruption while impoverishing the majority of the population. And Washington's campaign against terrorism encouraged its allies to embrace intrusive forms of surveillance and repress potential opposition in the name of security. Although the wealthy Gulf oil states and small slivers of Arab elites flourished within this

system, for most people the American order meant only violence, hopelessness, and deprivation. By nearly every economic, political, and developmental indicator, the Middle East under American domination has performed far worse than any other region.

Ironically, American security guarantees encouraged allies to disregard Washington's policy interests. Most felt safe from external invasion or attack, creating a moral hazard: they could pursue their own ideological and political projects without fear of meaningful consequences. Washington's preoccupation with its own domestic politics, inattention to the region's nuances, and inflated fears of Chinese and Russian advances all made the United States an easy mark for manipulative local powers. As a result, it repeatedly failed over the decades to meaningfully restrain Israel or to prevent Arab allies from adopting policies that undermined stated U.S. goals. Those ostensible allies shrugged off criticism of their destructive interventions in Libya, Sudan, Syria, and Yemen. Nearly all actively opposed the 2015 nuclear agreement with Iran, which the Obama administration hoped would help stabilize the region. And in 2017, the blockade of Qatar led by the United Arab Emirates (UAE) and Saudi Arabia badly undermined the united front against Iran that Trump's "maximum pressure" campaign required.

The 2010–11 uprisings pushed Arab governments into new forms of interventionism, in part because they lost confidence in the United States' ability and willingness to respond to what they considered to be urgent threats. Autocratic allies that already feared potential coups and popular revolts now saw them as imminent realities as they faced down challenges from Iranian-backed Shiite groups, Islamist and jihadist movements, and young liberal democratic activists. Watching the lightning-fast spread of the protests, these regimes learned that the threat at home could begin anywhere, even beyond their borders. And when they saw the overthrow of Egypt's Hosni Mubarak in 2011, they concluded that they could not count on the United States to save them from internal challenges. If they wanted to ensure their own survival, they would have to go out and contain the danger themselves. Their meddling repeatedly yielded devastating outcomes, however, contributing to a military coup in Egypt and several civil wars.

The order encouraged Iran and Israel to pursue destabilizing policies, too, but each in different ways. The Iranian regime took external hostility as a given and designed its survival strategy accordingly. The government was largely unbothered by U.S. and international sanctions that immiserated the public while strengthening the regime insiders who controlled black markets. Over the decades, Iran assembled and armed a network of nonstate allies that thrived in the wreckage of American, Israeli, and Saudi wars. With its access to American and European military technology cut off, Iran invested in low-cost production, developing drones and cheap ballistic missiles that could counter its rivals' technologically sophisticated and extremely expensive systems. Like most others in the region, Iran's leaders were swift to crush protests, fearful that a hidden foreign hand lay behind what were in fact authentic eruptions of popular discontent.

Israel, for its part, enjoyed the most ironclad of American security guarantees. Although it is a democracy, at least for Jewish citizens, the country's prime ministers have often fallen into a trap akin to the one ensnaring the United States' autocratic allies. Israel's military superiority and confidence in American support enabled its leaders to prioritize maintaining their governing coalitions and fending off domestic political threats over seriously addressing the Palestinian issue or easing regional instability. But when the October 7 attacks shattered that complacency, Israel's response was to go all-in on military escalation. It displayed ever greater excess in its use of force across the region and entrenched its military occupation in the

Gaza Strip, in the West Bank, and even in parts of Lebanon and Syria.

Part of the reason the American order lasted as long as it did was that the security bargains at its core were never truly tested. The region's leaders complained endlessly of feeling abandoned but never behaved as if abandonment were a significant possibility. For years, interstate war was not a particularly salient threat, either. Israel bombed Gaza and Lebanon with some frequency, but no Arab state aligned with the United States was overly worried about an Israeli attack. Iran loomed larger among their concerns, but even a direct Iranian attack seemed extremely unlikely. Indirect attacks by Iranian proxies only reinforced the core belief that American military primacy was so obvious and overwhelming that Iran would not challenge it. That confidence began to waver in 2019, when the United States did not respond to an attack on Saudi oil refineries attributed to Iran, and again when Houthi drone strikes hit the UAE in 2022. The regional security architecture remained intact, but cracks were beginning to show.

At the same time, the United States was trying to institutionalize its Middle East order by brokering open military and political cooperation between its Arab allies and Israel. The goal was not new. Fostering an anti-Iranian coalition under American leadership had been an objective of every American government since 1991. Trump diverged from his predecessors, however, in pushing it forward without tying steps toward Arab-Israeli normalization to progress on the Palestinian issue. In 2020, his administration brokered the Abraham Accords between Israel and, originally, Bahrain and the UAE. Morocco joined soon after, and Sudan signed an initial agreement that has not been formalized. But when the Biden administration tried to cajole Saudi Arabia into signing on, it misjudged the importance of the Palestinian cause to the Saudi public and the rising competitiveness between Riyadh and Abu Dhabi. It failed to see the growing popular hostility to normalization—or to anticipate the looming catastrophe in Gaza.

ONE-TWO PUNCH

The United States' regional order has been shaken up before, including during the disastrous 2003 invasion of Iraq and the popular uprisings of 2011, but it has always reconstituted itself. U.S. policymakers were as trapped by the structure they designed as were the regional powers embedded in it. Every president since Bill Clinton came to office vowing to reduce American involvement in the Middle East, and every president has found himself dragged back into the same policies and the same wars.

The dual crisis of Israel's destruction of Gaza and the U.S.-Israeli war in Iran may seem like just another episode in this cycle. But in truth, these events together have dealt a death blow to the American Middle East. American support for Israel's assault on Gaza, particularly under President Joe Biden, swept away any residual moral authority the United States could claim. Trump's debacle in Iran has shattered the illusion of American military omnipotence. Both incidents have demonstrated to Arab states their lack of meaningful influence within the regional order and the diminishing returns of American security guarantees.

American officials under Biden and Trump failed to appreciate the seismic effects of the Israeli war in Gaza. They shared a view that regional leaders' opinions were the only ones that mattered, that those leaders had long forgotten about the Palestinians, and that they were eager for closer relations with a capable Israel and for the stronger security guarantees the United States offered as incentives. Few things better exemplified this myopia than Biden's quixotic pursuit of brokering a normalization of relations between Israel and Saudi Arabia even after the rising death toll in Gaza had rendered such cooperation politically toxic among the Arab publics that Riyadh aspired to lead.

Washington's unceasing push for Arab cooperation with Israel created further divides. As one of the first two signatories of the Abraham Accords, the UAE continued working with Israel during the Israeli campaign in Gaza and as Israel carried out military strikes in Iraq, Lebanon, Syria, Yemen, and even Qatar. During the war with Iran, according to *The Wall Street Journal,* the UAE has coordinated with Israel and the United States to launch strikes on Iranian targets. Saudi Arabia, meanwhile, has watched the Emirati-Israeli alignment with unease. Riyadh and Abu Dhabi were already at loggerheads over Syria, with Saudi Arabia backing the post-Assad regime and the UAE sharing Israel's hostility to it, and Yemen, where Saudi Arabia had just driven out Emirati proxies. Saudi Arabia complained that the UAE was promoting secessionist movements that undermined regional stability, and it broadly saw a partnership between Israel and the UAE as a threat to its own regional leadership. The rift greatly complicated any chance Washington may have had of lining up the region's heavyweights behind its campaign to defeat Iran.

If the war in Gaza left the future of American regional leadership in doubt, the war with Iran was confirmation of the end of the order. Gulf leaders were furious that the United States and Israel started the war without consulting them, while knowing they opposed it, and in the middle of Omani-brokered negotiations with Iran. A war they had no say in exposed them to direct Iranian retaliation. Although American missile defense systems protected the Gulf from the worst of the barrage, enough Iranian strikes got through to do substantial harm and to disrupt the patina of stability on which the region's social and economic model rested. Iran targeted all Gulf states, including friendlier ones such as Oman and Qatar, but focused its fire on those that had signed the Abraham Accords: Bahrain and, even more so, the UAE. Within a few weeks, Iran managed to damage, destroy, or render irrelevant large parts of the archipelago of military bases that had underwritten American primacy in the Middle East.

Gulf allies' confidence in Washington eroded further when the U.S.-Israeli campaign proved unable to dislodge the Iranian regime. For decades, advocates of bombing Iran argued that such an attack might be messy but would ultimately remove the Iranian threat. Yet the United States and Israel, with all their military might, simply failed. On top of that, the United States sat by helplessly as Iran closed the Strait of Hormuz, endangering the entire Gulf economy. Once again, Gulf leaders were shocked not just by American disregard for their preferences but also by the revelation of American impotence. And their shock turned to anger when the United States bombed Iranian water storage facilities and Israel struck Iranian oil depots. Washington was gambling with its partners' futures; had Tehran responded by striking Gulf water facilities or nuclear power sites, the resulting cycle of escalation could have ended with Gulf states' facing economic catastrophe and enough environmental destruction to render them uninhabitable.

What the Gulf took away from all this was that American security guarantees, the heart of the regional bargain, were no longer reliable. The region had already learned in 2011 that Washington could not protect it from domestic threats. If Washington could not even be counted on to consult its allies, defeat its adversaries, or protect its partners from the fallout of its regional misadventures, then what good were its promises? The fundamental bargain the United States offered has crumbled, and it will not be easily rebuilt.

THIS TIME IS DIFFERENT

It has become commonplace to refer to the Iran war as Washington's Suez moment. There are indeed similarities between today's catastrophe and the failed British-French-Israeli scheme to take the Suez Canal from Egypt in 1956, which delivered a stunning political victory to Egyptian

President Gamal Abdel Nasser. Suez became a shorthand for the demise of the European empires and the passage from a multipolar world to the bipolar Cold War–era system. But the Suez crisis did not immediately end the British and French empires in the Middle East. France would continue its war to hold on to Algeria for another six years, and the United Kingdom remained the dominant power in the Gulf for a decade and a half, fighting insurgencies in Oman and present-day Yemen before finally withdrawing from the region in 1971. It takes time for events to play out fully.

The full effects of the U.S. disaster in Iran will similarly take time to materialize. In the short term, the American-led regional order is not going anywhere. The United States may retreat from the military bases Iran destroyed, but it will still play a major role in regional defense. Gulf states are unlikely to break from Washington right away. Fearful for their future and seeing no obvious alternatives, they may even enhance their ties—as Saudi Arabia tried to do by finalizing a long-sought nuclear agreement, only to have Trump change its terms the next day, leaving the deal in limbo. They are also unlikely to pose any military threat to Israel or move closer than necessary to Iran. The U.S. rift with Israel, although real and likely generational in scale, will not soon fracture that alliance. Arab states, too, will maintain working relations with Israel and continue to avail themselves of Israeli military and surveillance technology.

The small adjustments that regional actors begin to make may not look like much at first, either. Countries have always pursued their own agendas, including at the peak of American primacy. Even the most dependent of the United States' allies have mastered the arts of foot-dragging, leash-slipping, and lobbying Washington. They will continue to engage in local rivalries, prioritize the survival of their regimes, and try to ensure their security. Sometimes that will mean working with Washington; sometimes it will not.

Walking past an anti-U.S. billboard in Tehran, Iran, August 2026 Majid Asgaripour / West Asia News Agency / Reuters

Yet what looks like short-term continuity should not be mistaken for long-term sustainability. By the time of the Suez crisis, the dissolution of the European empires was inevitable—not because of one policy fiasco, but because of the rise of nationalism and anticolonialism as well as the economic and political exhaustion of the European imperial model. The United States' Middle East order, too, had been decaying for years as policy and political failures accumulated, culminating in the loss of shared purpose and the military impotence revealed by the latest crises.

Washington will be tempted to stand by the policies that have defined its Middle East approach for decades, leaning on its relationships with the brutal, insecure, and repressive leaders who populate the landscape it designed. If American leaders stick to the same path, they should expect the same result: a region beset by constant instability, economic and political failure, and repeated eruptions of violent conflict. These

conflicts may only occasionally draw in American military forces, but the chaos will consistently demand attention and pointlessly consume resources. The forever wars will continue.

That outcome may seem acceptable to American policymakers who have become accustomed to managing conflicts and maintaining relationships with bad actors. But Washington cannot stave off a transition to a new regional order by simply pretending that nothing has changed. Arab allies that have lost faith in the United States will increasingly exercise their autonomy. At times, that could mean pursuing diplomacy with Iran and expanding relations with China and Russia against American wishes. At others, it might mean meddling in Libya, Sudan, and the Horn of Africa or reigniting violent conflict in Iraq, Lebanon, Syria, and Yemen.

Forces largely beyond American control will shape this emergent order. For one, Israel is determined to carry on with military interventionism regardless of American preferences. It continued its war with Hezbollah in defiance of the U.S.-Iranian memorandum of understanding reached in June, and it indicated no willingness to withdraw its military from southern Lebanon. Israeli officials insist that the country will maintain a troop presence in Syria as well. And with no serious domestic pressure to adopt more dovish policies, there is little standing in the way of Israel's annexation of the West Bank and its complete destruction of Gaza.

Iran, like Israel, has every incentive to pursue policies that perpetuate instability. Incessant conflict helps the regime shift blame for hard times and justify its strategy of resistance to the Iranian public. And Iran has retained the ability to stir up violence. Although the country has been badly damaged by war, the regime remains intact, and its regional power has grown. Iran has demonstrated its ability to effectively control the Strait of Hormuz and to strike American allies in the region, and setbacks to allies such as Hezbollah are unlikely to permanently end Tehran's ability to project power through proxies. American pressure on weak governments in Iraq and Lebanon to disarm pro-Iranian militias could trigger additional conflict in which Iranian allies would hold the upper hand.

Regional alignments will drift further away from the anti-Iranian coalition that American officials envision. Instead of relying on American protection, many Gulf states could pursue side deals with Iran to keep themselves off Tehran's target list. And instead of following Washington's lead, regional politics will likely revolve around a deepening competition for primacy between the Emiratis and the Saudis. Before the Iran war began at the end of February, Riyadh had started to mobilize a coalition that included Egypt, Pakistan, Qatar, and Turkey to counter the U.S.-backed Emirati-Israeli alliance. This contest will resume after the fighting simmers down, likely destabilizing already beleaguered states, stretching across the wider region, and generating endless new crises that a distracted Washington will struggle to navigate.

Finally, most regimes will face ever greater pressures from below as the fallout of the Iran war ripples through the region's struggling economies. It is not only countries whose infrastructure has been damaged by Iranian strikes that will feel those effects. In Egypt, for example, steep hikes in fuel and food prices and enormous losses of Suez Canal revenues as the war disrupts global shipping are compounding existing fiscal and unemployment crises. Many countries already hurt by cuts in U.S. aid may lose another critical source of external investment as the wealthy Gulf states grapple with their own economic problems. Domestic grievances and outrage over Gaza make for a potent mix, and a wave of protest comparable to the uprisings of 15 years ago could again be on the horizon.

LAST CHANCE

The violent demise of the old regional order could disrupt or even foreclose

any attempt to establish a functional new one. But this moment could also be an opportunity for the United States to recast the core bargains that have produced such destructive results. Getting a new Middle East policy right requires rethinking the decision to prioritize relations with autocratic and lawless allies in the name of pragmatism. For decades, Washington assumed that it did not need to worry much about Arab public opinion because it could count on Arab rulers to crush any dissent. It similarly assumed that mouthing empty words about supporting a two-state solution, all while Israel continued its creeping annexation of Palestinian lands and avoided genuine peace negotiations, would be enough to keep its Arab allies on board. That meant the United States never considered adopting policies that would command the consent, or even the support, of the peoples of the region. And it meant Washington could never seriously engage in the promotion of democracy or the defense of human rights, because its strategy depended on their absence.

The Trump administration, contemptuous of democracy and the rule of law at home and abroad, is not going to change that. It is difficult to imagine Trump, who vacillates wildly between strategies, designing a new regional order of any kind. But his successor will have a real chance to break with the status quo and craft a more coherent and more effective Middle East strategy. That starts with renouncing the use of military intervention as a first resort and ending the practice of diplomacy by airstrike. Washington's priority should be defense, not offense. One way to make that intention clear is to forgo the restoration of damaged or destroyed U.S. military bases across the Gulf and focus instead on investments in intelligence sharing, missile defense systems for Gulf partners, and the preservation of freedom of navigation through the Strait of Hormuz.

The United States must pursue stability in the Middle East through diplomacy and collective defense, not militarized containment. The Iran fiasco has thoroughly exposed the hollowness of hawkish calls for war and promises of decisive action. It is time for Washington to commit to a diplomatic process that can bring Iran into the regional security system as an invested partner. The Gulf states may be open to such an approach despite their fury over Iran's latest attacks; after all, Saudi Arabia and Iran reached a rapprochement in 2023 after an earlier bout of Iranian aggression. The Obama administration evoked a similar vision when it was negotiating the 2015 Iran nuclear deal, and even Vice President JD Vance has spoken of a willingness to "fundamentally transform" the U.S. relationship with Iran following a new agreement. The aspiration is there, but a new administration will have to demonstrate quickly and decisively that it intends to see it through.

The reset in U.S. policy must also extend to the way Washington treats its allies. This includes Israel. Conditions are ripe for a rethinking of the U.S.-Israeli relationship: according to a Quinnipiac poll released in June, nearly two-thirds of Democrats and more than half of independents think the United States is too supportive of Israel. In mid-July, more than half the Democrats in the House of Representatives voted for a bill to cut off U.S. military aid to Israel. The next administration should use this momentum to put the kind of pressure on Israel that U.S. governments have long shied away from. Washington need not abandon its ally, but it should demand that Israel respect human rights within all the territories it controls, stop the creeping annexation of the West Bank, and end its destabilizing interventions in Lebanon and Syria.

More broadly, stability at the regional level requires that the United States recommit to international human rights norms, oppose secessionist movements in countries such as Syria and Yemen, deter partners' military interventions and proxy wars in places such as Sudan and Libya, and stop urging the Iraqi and Lebanese governments to

disarm the Iraqi militias and Hezbollah before they are fully prepared to do so. Stability at the domestic level requires democratic change. For the United States, that means encouraging reform, including human rights protections, and calling off the bargain that has allowed autocratic allies to get away with grievous repression. This message will not be welcome in Cairo, in Riyadh, or indeed in many other capitals. But no real transformation of the regional order will be possible without addressing the pathologies of its regimes.

New American policies would not create a stable, peaceful Middle East overnight. At first, they would win little public applause from a region that has grown accustomed to American hypocrisy and abuse. Later on, the rise of more democratically responsive governments in the region would likely cause considerable headaches as ambitious politicians competed to condemn and denounce the United States. But in the long run, a Middle East populated by regimes that are less willing to follow Washington's lead on unpopular policies or to suppress public opposition would likely be more stable than the region of today. Washington struggles to conceive of a Middle East it does not dominate and to imagine real alternatives to the present regional order no matter how badly it has failed. But that order is ending, and this may be U.S. leaders' last chance to change course. If they cannot, they will watch the American Middle East fade away like the European empires that came before.

Marc Lynch is Professor of Political Science and International Affairs at George Washington University, where he is the director of the Project on Middle East Political Science and Co-Director of the Program on African Social Research. He is the author of *The New Arab Wars: Uprisings and Anarchy in the Middle East* and a co-editor of *The One State Reality: What Is Israel/Palestine?*

Accused 9/11 mastermind Khalid Sheikh Mohammed, 3 co-defendants set for 2028 trial

Source: https://www.foxnews.com/us/accused-9-11-mastermind-khalid-sheikh-mohammed-3-co-defendants-set-2028-trial

Aug 26 – Khalid Sheikh Mohammed, the accused mastermind of the Sept. 11 terror attacks, and three alleged co-conspirators will stand trial in 2028, a military judge ruled Wednesday. Lt. Col. Michael Schrama set the trial for June 5, 2028, rejecting prosecutors' request to begin proceedings in January 2027. Mohammed and the three other defendants have been held at Guantánamo Bay since 2003 in the long-delayed case stemming from the attacks that killed nearly 3,000 people.

Stopped at the Border, Dangerous at Home: Europe's New Islamic State Problem

By Giorgia Valente

Source: https://themedialine.org/top-stories/stopped-at-the-border-dangerous-at-home-europes-new-islamic-state-problem/

Aug 27 – Failed journeys to foreign conflict zones can redirect radicalized individuals toward targets in their own countries. The July 25 attack near Berlin's Pride celebrations brought Europe's changing Islamic State threat into sharp focus. German authorities said 21-year-old Abdul Ballout

drove a van into a crowd and attacked people with a bladed weapon, killing one person and injuring 29 others before police fatally shot him the following day.

Investigators said they found a video on Ballout's phone in which a masked person appeared to pledge allegiance to Islamic State (IS). Authorities believed the person in the video was Ballout, who had previously been convicted over attempts to travel abroad to join the organization, including unsuccessful journeys in 2025.

The case raised a familiar but increasingly complicated counterterrorism question: What happens when a person attracted to an extremist organization fails to reach the conflict zone?

For Kiria Borak, a security analyst focused on West Africa and the Sahel, preventing the journey does not necessarily remove the underlying risk.

"I think the Berlin attack follows a pattern we keep seeing: an individual tries to reach a conflict zone, gets stopped before they arrive, but that does not mean the threat disappears or is necessarily well managed. In some cases, the focus just shifts closer to home," Borak told The Media Line.

She said the expansion of IS theaters and the links between them can become a European security issue even when those drawn to the organization never reach the battlefield.

Europol's latest terrorism assessment, released in July, recorded 45 terrorist attacks across 10 European Union member states during 2025, including 24 classified as jihadist. Of the 486 suspects arrested for terrorism-related offenses, 347 were linked to jihadism. Europol also warned that online environments increasingly allow dispersed networks, lone actors, and self-initiated cells to radicalize and mobilize without the large organizational infrastructure once associated with terrorist groups.

European authorities are also confronting networks whose operational roots lie far beyond the continent.

Between June 1 and 5, Europol coordinated a counterterrorism operation with eight European law enforcement agencies and the FBI targeting Islamic State Khorasan Province (ISKP) and its support networks in Europe. Europol said the operation resulted in several arrests but did not disclose a precise number. It focused particularly on individuals of Chechen and Central Asian origin and examined travel routes extending through Europe, South America, and the US.

Lucas Webber, a senior research fellow at The Soufan Center, said the operation illustrated an important distinction between pressure on ISKP inside Afghanistan and Pakistan and the branch's continued international reach. Webber's research focuses in part on Western domestic terrorism, extremist propaganda, and violent nonstate actors in South and Central Asia.

"I think the Europol-FBI joint efforts against ISKP are quite significant due to the branch's activity declining in Afghanistan and Pakistan, where it primarily operates. The new UN monitoring report notes the decrease in activity in the actual conflict theater, but these arrests show that there are still robust international networks," Webber told The Media Line.

"The branch still has external operations capabilities, propaganda production, financing, fundraising, and influence networks outside of its actual area of provincial operations," he added.

That assessment broadly corresponds with the UN Security Council's Thirty-Eighth Report of the Analytical Support and Sanctions Monitoring Team, published Aug. 10, 2026, and covering developments through June 9. The report said counterterrorism operations by Pakistan and the Taliban had dealt ISKP serious setbacks and reduced its attacks in Afghanistan, although its attacks increased in Pakistan. It assessed that the branch remained intent on conducting operations abroad and retained the ability to carry out occasional high-profile mass-casualty attacks.

The report found that the broader threat from IS and al-Qaida had intensified in the Sahel and South Asia, with regional affiliates assuming greater importance as the organizations' senior leadership became more geographically dispersed.

Webber said that geographic dispersion makes the threat difficult to assess solely through the traditional measure of battlefield strength.

"The roll-up of this network, the arrests and so on, show that it is still a security concern. There is still an active threat posed, but the mainstream media attention or political statements made publicly don't align with, or are not proportionate with, the actual threat posed by ISKP and other groups," he said.

Africa has become another focus of concern.

The Sahel is now one of the principal areas of expansion for jihadist organizations, including IS affiliates and al-Qaida-linked Jama'at Nusrat al-Islam wal-Muslimin (JNIM, meaning "Support Group for Islam and Muslims"). The Soufan Center said in a June assessment that IS had entered a new phase in the region as it sought to consolidate its West Africa and Sahel provinces.

The implications are not confined to the territory those groups control or contest.

North Africa provides a clear example of how Sahel-based networks can extend beyond their immediate region. In February 2025, Moroccan authorities arrested 12 suspected members of an IS-linked cell across nine cities. Authorities said the group was preparing attacks inside Morocco and had links to an IS figure operating in the Sahel. Investigators found weapons, explosive materials, and other equipment.

"Morocco is probably one of the places where this has been clearest," Borak said. "Moroccan authorities have repeatedly dismantled networks with links to the Sahel that were also involved in planning or facilitating attacks closer to home."

Networks extending from the Sahel into North Africa do not automatically become operational networks in Europe. Still, the movement of people, financing, propaganda, and facilitators across those regions requires European authorities to monitor developments well beyond the EU's physical borders.

Webber said there are signs that the IS branch in the Sahel is assuming a larger role beyond its immediate battlefield.

"Islamic State in the Sahel remains largely regionally focused, of course, but it is taking on a greater external-operations role," he said.

Authorities have disrupted plot cells and support networks connected to the branch in Morocco and Spain, he said.

"You are seeing increased online chatter, for instance, about Western foreign fighters wanting to join Islamic State, and they are being referred increasingly to Islamic State in West Africa, in the Sahel, and in Somalia," Webber said.

Somalia presents a somewhat different model. The UN Security Council's Aug. 10 monitoring report estimated that IS's Somali branch had between 150 and 250 fighters, primarily concentrated in Puntland's Cal Miskaat mountains. The estimate represented a sharp decline from figures reported before Puntland began its sustained counterterrorism campaign.

The report said the movement of foreign fighters into Puntland had declined and that IS was discouraging prospective recruits from traveling there. It warned that migration routes and illicit transit networks previously used by the organization could be reactivated if counterterrorism pressure weakened.

Puntland forces have mounted a sustained offensive against IS positions in the Cal Miskaat mountains, recapturing territory and bases. The US and the United Arab Emirates have supported the campaign with airstrikes, including attacks targeting senior IS members.

Borak cautioned against treating Somalia and the Sahel as identical recruitment environments.

"I think the Somali branch of IS is a somewhat different case. Its ranks have become increasingly international," she said.

"Puntland's campaign against the group has turned up foreign fighters from multiple countries, including Ethiopia and Morocco, suggesting a recruitment network that extends beyond Somalia," she added.

"While there is some evidence of international recruitment, a lot of what we see with the Sahelian groups is still primarily local recruitment, with facilitation and support networks extending north into North Africa and Europe."

The evidence does not indicate a simple mass transfer of fighters from Africa toward Europe. Analysts instead describe a layered system in which local insurgencies, foreign fighter movements, online recruitment, financing channels, and international facilitation networks can overlap without being controlled from a single center.

Battlefield losses alone therefore provide an incomplete measure of the threat.

Webber pointed to ISKP after the Taliban returned to power in Afghanistan as an example of how parts of the IS network can assume greater international responsibilities as conditions change.

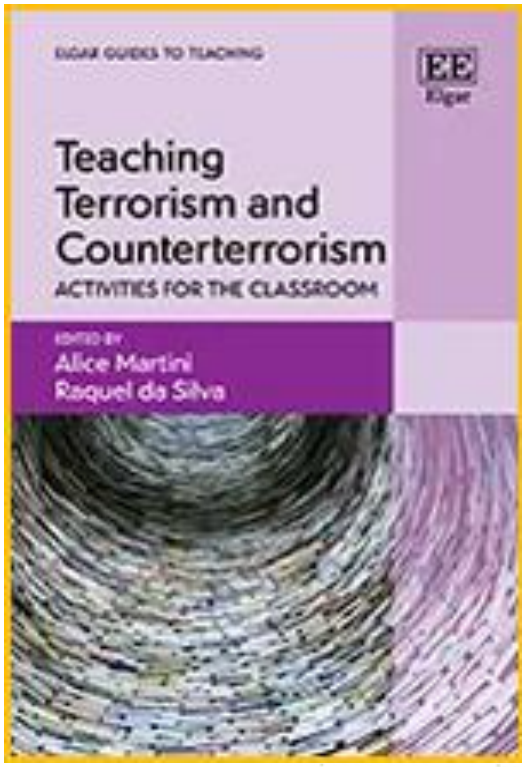
"After the Taliban takeover, ISKP took on a more prominent operational role in propaganda production, recruitment, incitement, guiding attacks, and external operations," he said. "It took a while for security coverage and preparations to catch up. And now we are seeing something similar happen with Islamic State networks in the Sahel."

For European security services, the challenge is one of simultaneity. A threat originating in Afghanistan can coexist with recruitment in Somalia, territorial expansion in the Sahel, facilitation networks in North Africa, and self-radicalized or remotely influenced individuals inside Europe.

"There is a broad range of nonstate threats that are tying up resources, and there is always a risk of security coverage gaps and resource gaps being exploited successfully by any one of these groups, or multiple," Webber said.

Teaching Terrorism and Counterterrorism

Activities for the Classroom



Edited by **Alice Martini,** Lecturer of International Relations, International Relations and Global History Department, Complutense University of Madrid, Spain and **Raquel da Silva**, Associate Professor, Faculty of Economics, University of Coimbra and Integrated Researcher, Centre for International Studies, Iscte-IUL, Portugal

Publication Date: 2026 | **Extent:** 290 pp
Source: https://www.e-elgar.com/shop/gbp/teaching-terrorism-and-counterterrorism-9781035354306.html

This timely and innovative book offers practical, classroom-tested activities for engaging students in critical learning about terrorism and counterterrorism. Bringing together leading scholars, it reimagines the classroom as a space of inquiry and experimentation, where dominant narratives are questioned and assumptions are actively challenged.

Open access Protocol

BMJ Open

Acute care for patients exposed to a chemical attack: protocol for an international multicentric observational study

Stephane Bourassa ,[1,2,3,4] Daniel Noebert,[3,5] Marc Dauphin,[3,6] Jerome Rambaud,[7] Atsushi Kawaguchi,[8,9] François Léger,[2,3] Daan Beijer,[5] Yvan Fortier,[10] Mina Dligui,[10] Hristijan Ivanovski,[11] Serge Simard,[12] Philippe Jouvet,[4,13] Jacinthe Leclerc[6,12,14]

ABSTRACT

Introduction: The use of weapons of mass destruction against civilian populations is of serious concern to public health authorities. Chemical weapons are of particular concern. A few studies have investigated medical responses in prehospital settings in the immediate aftermath of a chemical attack, and they were limited by the paucity of clinical data. This study aims to describe the acute management of patients exposed to a chemical attack from the incident site until their transfer to a medical facility.

Methods and analysis: This international multicentric observational study addresses the period from 1970 to 2036. An online electronic case report form was created to collect data; it will be hosted on the Biomedical Telematics Laboratory Platform of the Quebec Respiratory Health Research Network. Participating medical centres and their clinicians are being asked to provide contextual and clinical information, including the use of protective equipment and decontamination capabilities for the medical evacuation of the patient from the incident site of the chemical attack to the moment of admission at the medical facility. In brief, variables are categorised as follows: (1) chemical exposure (threat); (2) prehospital and hospital/medical facility capabilities (staffing, first aid, protection, decontamination, disaster plans and medical guidelines); (3) clinical interventions before hospital admission, including the use of protection and decontamination and (4) outcomes (survivability vs mortality rates). Judgement criteria focus on decontamination drills applied to any of the patient's conditions.

CTCSENTINEL

August 2026 Issue | Volume 19, Issue 8

Source: https://ctc.westpoint.edu/august-2026/

Managing the foreign fighters who remain in Syria has emerged as a defining test of the country's transition, Aaron Zelin writes in this month's cover article. It is a complicated, nuanced task, one that Zelin finds would not be made easier and could in fact be made far more difficult with a "disarmament-by-headcount framing." "Syria's foreign fighters are not a stockpile of weapons to be confiscated," he cautions. "They are a differentiated, fracturing population that

has been substantially absorbed into the state, that is drawing new arrivals, and that now sits at the center of Syria's contested reintegration into international politics."

Our interview is with Gary Greco, who served for over 40 years in the U.S. intelligence community with the Defense Intelligence Agency and the Office of the Director of National Intelligence. Ahead of the 25th anniversary of 9/11, he reflects on the events of that day and also considers future threats: "Terrorists are always going to be opportunists, but they are also technology driven, and we're always a step behind," he warns.

James Khalil, Andrew Glazzard, John Horgan, and Alastair Reed examine the utility of "Exit Comms," communication campaigns aimed at individual or group-level disengagement from violent extremist (VE) organizations or movements during active conflicts. They offer an analytical framework based on five dimensions—audience, messenger, channel, format, and content—to inform Exit Comms' design and evaluation. "Despite [a] lack of attention to date," they write, "emerging evidence from cases such as Colombia, Nigeria, and Somalia suggests that Exit Comms can provide an effective tool for increasing exit rates from VE organizations."

Terrorism After Ideology

By James Paterson

Source: https://www.irregularwarfare.org/terrorism-after-ideology/

Sep 01 – On April 29, two Jewish men were stabbed in north London in what British police declared a terrorist incident. **Harakat Ashab al-Yamin al-Islamiya** (HAYI), an "Islamic resistance" group that did not publicly exist two months earlier, immediately claimed responsibility. Since then, HAYI has claimed more than seventeen attacks across Europe.

HAYI is less a coherent terrorist organisation and more of a disposable instrument within an evolving hybrid warfare ecosystem. The group's symbolism, propaganda, and operational patterns closely resemble those of Iran's Axis of Resistance network, marking it as the latest in a series of proxy actors the Iranian regime has deployed for gray zone warfare in Europe.

Given HAYI's terrorist organizational trappings but hollow ideological affinity, it is reflective of a contemporary extremism landscape that is defined less and less by ideological boundaries. This means emerging threats are increasingly outpacing the conventional categories Western governments use to identify, prosecute, and prevent terrorism. Western counterterrorism efforts have historically been calibrated around the working assumption that ideologically committed actors organized into coherent movements are the central problem to be detected, disrupted, and prosecuted. In 2026, that assumption is now under strain. Recent expressions of violence signal a broader shift in how contemporary terrorism manifests. Terrorism is shifting from organizations with clear ideological boundaries toward fluid, transactional, and amorphous forms that the existing counterterrorism architecture was not built to recognize and therefore cannot defeat.

The Evolution of Ideology

The phenomenon of gray zone warfare, disruptive behaviour that sits below

our traditional threshold of warfare, is by no means novel. Russia, in particular, has been strongly implicated in such activities, with over 150 hybrid incidents linked to Russia across Europe since its invasion of Ukraine in 2022. As part of this threat environment, the international community has observed the emergence of a new crime-terror nexus whereby hostile actors have increasingly cultivated ties with criminal entities, including both organized crime groups as well as 'disposable' local petty criminals who may not be fully aware of their involvement in geopolitical competition. Hostile state actors have leveraged criminal partners for hybrid activities in what is sometimes described as a "violence as a service" model. The goal of such hybrid tactics is to instill fear, provoke communal anxiety, strain security resources, and generate propaganda effects, all while avoiding thresholds that would provoke unified Western retaliation.

Read against this backdrop, HAYI looks at first glance like a recognizable case study in the genre. What makes the group different is the specific way it dresses these tactics in the costume of a terrorist organisation. The ideology is a wrapper. HAYI borrows the language, symbolism, and behavioural repertoire familiar from jihadist organisational practice without committing to ideology as a genuine organizational pillar. The result sits at the intersection of two trajectories: an expression of gray zone warfare on one hand, and an expression of how terrorism can manifest without clear ideological boundaries on the other. The latter creates complexities for how terrorism should be understood and engaged by policy makers.

Conventionally, terrorism analysis and response has organized around ideological taxonomies, with acts separated by the belief systems that inspire violence. This approach assumes terrorism emerges in distinct ideological waves that produced coherent movements with their own and identifiable strategic logics, mobilization pathways, grievance narratives, and organizational structures. Counterterrorism systems across Europe and North America were built around this assumption. The conventional model treated ideology as the primary mechanism of mobilization. The radicalization pathway, from grievance through ideological exposure to operational activity, became its organizing principle across countering violent extremism programs, intelligence prioritization, and prosecutorial strategy.

However, the extent to which this view continues to hold analytical value has been increasingly questioned by both terrorism scholars and practitioners. Rather than terrorism defined by clear ideological boundaries, contemporary terrorism dynamics are characterized by greater fluidity and diversity. Driven in part by the virtualization of extremism, and of society more broadly, the current threat environment is shaped by younger lone attackers whose radicalization occurs primarily online and at accelerated speed, combining fragments of political ideas with personal grievances that defy clear ideological categorization. Coherent organizations with identifiable membership, leadership, and doctrine are no longer the central operational unit for how terrorism emerges in Western countries. They have been replaced by fluid online milieus, post-organizational networks, and individuals self-assembling worldviews from the available material. Terms such as mixed, unstable, unclear ideologies, salad-bar or pick-and-mix extremism have emerged to capture the individually assembled and ideologically promiscuous nature of contemporary radicalization.

HAYI adds a further dimension to this already heterogeneous ecosystem. The lone actor problem of the past decade described ideologically thin individuals operating without organizational backing. HAYI describes something close to the inverse. The operational signature is recognizably terrorist, including symbolic targeting of religious minorities, claim videos,

and political demands. But the recruitment infrastructure is transactional, the perpetrators are interchangeable, and the organizational form is deliberately disposable. Ideology, in this case, is not the cause but the cover.

Taken together, the most recent iterations of violent extremism highlight a terrorism landscape in which the relationship between ideology, organization, and violence has become genuinely unstable.

This is not to say ideology has ceased to matter. Ideology continues to shape, constrain, and facilitate violent behaviour, and ideologically coherent organisations continue to motivate and structure violent action across the contemporary threat landscape. The argument is not that terrorism is leaving ideology behind. It is that the relationship between ideology, organization, and violence has become more variable than the conventional model assumed, and that counterterrorism practice needs to understand how ideology interacts with the wider set of factors that produce political violence, including financial incentive, social vulnerability, online ecosystem dynamics, and state strategic interests, rather than treating ideology as a monolithic explanatory variable. The end result is an emergent terrorism environment that generates significant complexities for counter-terrorism practitioners, not that their jobs were ever simple or straightforward.

The Task Ahead

How European jurisdictions have responded to HAYI illustrates this complexity. Dutch authorities charged suspects in the Rotterdam synagogue case with arson with terrorist intent. French authorities charged the suspects in the foiled Paris Bank of America plot with criminal terrorist conspiracy and attempted destruction in connection with a terrorist enterprise. British authorities, by contrast, initially charged suspects with standard arson and criminal damage offenses, while more recently designating the Iran Revolutionary Guard Corps as a terrorist organisation. The targeting pattern, ideological framing, and external claim of responsibility are common to all three jurisdictions. Same campaign, same operational signature, three different legal frames. These divergent responses reflect the absence of any single coherent approach within the existing European legal architecture for how a campaign like HAYI's should be addressed.

Western governments and security services have not been blind to this shift. Ken McCallum, the director general of the United Kingdom's domestic counter-intelligence and security agency (MI5), publicly described "more volatile would-be terrorists with only a tenuous grasp of the ideologies they profess to follow" and named the disposable-agents model directly in his 2025 threat update. Europol's 2025 Terrorism Situation and Trend Report explicitly identifies the hybridization of ideologies and the growing involvement of minors in violent extremism. The diagnosis is increasingly shared across European security and intelligence services.

What has not yet followed is the structural translation of that diagnosis into legal frameworks, prosecutorial strategy, and prevention architecture. The divergent legal responses to HAYI across the United Kingdom, the Netherlands, and France are the most concrete evidence of this lag. Recognition at the intelligence level has not produced consistent legal treatment at the prosecutorial level. The analytical categories used to organize terrorism reporting, including the European Union's annual Terrorism Situation and Trend report, still rest on ideological taxonomies even when they are acknowledged by security practitioners as inadequate. Prevention programmes are being reformed in principle but the institutional weight of fifteen years of ideology-centered design will not shift quickly.

The task ahead is less about discovering the problem than about closing the gap between what is now recognized and what is operationally adapted. Security

institutions will either need to broaden existing concepts of terrorism and radicalization to accommodate fluid, transactional, and state-directed forms of violence, or new frameworks will need to be developed alongside those previously established. Legal frameworks that currently force ambiguous cases into single statutory categories will need to bridge across terrorism, foreign interference, and organized crime authorities. Prevention work calibrated around ideological signatures will need to extend toward the recruitment ecosystems where contemporary perpetrators are increasingly found, including encrypted platforms, financial intermediaries, and online marketplaces for low-skilled violence.

None of this is straightforward, and the structural burdens of ideology-centered design will act as a barrier. But the cost of inaction is already visible. The HAYI brand will likely be retired and replaced within months. The model it represents will not. If Western institutional response continues to lag the diagnosis, the next franchise will exploit the same gaps.

James Paterson, Ph.D., is a research associate at the Lowy Institute's Transnational Challenge program. He holds a Ph.D. from Monash University, and his research focuses on insurgent adaptability and organizational dynamics.

Why is piracy picking up off Somalia's coast again?

By Faisal Ali

Source: https://www.aljazeera.com/news/2026/8/31/why-is-piracy-picking-up-off-somalias-coast-again

Aug 31 – The Federal Government of Somalia announced on August 29 that the Turkish navy, working with Somali forces, had freed the cargo ship MV Lutuf after a 10-day pursuit, killing 14 pirates and destroying four of their boats. The vessel had been seized on August 17 off Jifle, on the coast of Puntland, Somalia's semi-autonomous northeastern region. Mogadishu's Defence Ministry credited its release to a 2024 defence pact between Somalia and Turkiye.Puntland has disputed that account. Its Ministry of Security said no military rescue had taken place and accused federal officials of securing the vessel's release through a ransom payment to the pirates. The conflicting accounts have not been independently verified. But the seizure and the military response around it mark the most dramatic episode yet in a series of pirate attacks off Somalia this year, raising fresh questions about how far a resurgence that began in the spring could go.

How serious is the return of Somali piracy?

Piracy incidents in Somali waters and the Gulf of Aden have risen sharply since the spring, after several years in which the crime had all but disappeared from the region.

An AFP analysis of International Maritime Organization data found at least 15 attacks since the start of the year, including eight in the Gulf of Aden since May.

One tanker seized off Yemen in May was later directed towards Somalia by pirates demanding $10m. Another vessel, the MV Honour 25, has been held for more than two months.

In May, a separate pirate group abandoned a hijacked Emirati dhow after running short of supplies while using it as a mother ship to attack other ships, Puntland security officials told AFP.

The Joint Maritime Information Center, which monitors threats to

shipping in the region, raised its piracy threat assessment to "severe" in response to the surge in attacks during April and May.

The increase is significant, but still far below the scale of the crisis in the early 2010s, when the International Maritime Organization, the United Nations agency responsible for shipping safety and security, recorded around 200 attacks a year.

Afyare Elmi, a Somali academic at City University in Mogadishu, told Al Jazeera there had "been an uptick, but compared with the levels seen in the early 2010s, the number of attacks is not that high".

Mostafa Elbanna of the United Nations Office on Drugs and Crime said piracy remains well below its historic peak. Speaking at a security meeting in Nairobi last week, he said countries in the region are better equipped to respond than they were last time.

Between 2005 and 2012, pirates carried out more than 1,000 attacks off Somalia, according to a World Bank study. They successfully hijacked 218 vessels and collected an estimated $315m to $385m in ransom payments.

At the peak in 2011, Somalia accounted for well over half of all piracy attacks recorded worldwide.

One Earth Future's Oceans Beyond Piracy programme, a maritime security initiative set up during the Somali piracy crisis, estimated that piracy off Somalia's coast cost the global economy between $6.6bn and $6.9bn in 2011, largely through security measures, higher fuel use, insurance and naval operations.

The crisis was eventually brought under control by a vast international security effort. NATO's Operation Ocean Shield, the European Union's Operation Atalanta and the US-led Combined Task Force 151 increased naval patrols, while shipping companies hardened vessels and changed procedures.

Between 2013 and 2023, barely a handful of hijackings succeeded off Somalia.

NATO ended its counter-piracy mission in 2016.

But the long period of relative calm did not mean the conditions that sustained piracy had disappeared. International patrols and better-protected ships made hijackings far harder and more expensive, while weak coastal governance, illegal fishing and criminal networks persisted onshore.

As early as 2013, a report by the UN secretary-general said the persistence of pirate networks reflected "the onshore rule of law and governance vacuum in which they operate", and cautioned that attacks could rise again if naval patrols were reduced or commercial vessels relaxed their defences. The resurgence is now testing how durable that earlier success was.

Why is piracy rising again now?

No single factor explains the resurgence, Abdullahi Mohamed Kulmiye, a former ports and maritime transport minister in Galmudug, a state neighbouring Puntland, told Al Jazeera. Several conditions, he said, appear to have aligned at once.

One is a shift in naval attention elsewhere in the region. The United States and Israel have been at war with Iran since late February, and Iran has at times controlled passage through the Strait of Hormuz. Naval forces that might otherwise patrol waters closer to Somalia have been drawn towards that crisis.

Abdurrahim Muhammad Ali of the Djibouti Maritime Authority told a regional security meeting in Nairobi this week that pirates were exploiting the diversion of naval forces elsewhere.

"They use this opportunity and the distraction of maritime forces globally to carry out more attacks in this area, because they know everyone is busy [looking in another direction]," he said.

Economic pressure onshore has intensified at the same time. Inflation in Somalia reached 9.2 percent in March, its highest level in years, as fuel and food prices surged.

The International Monetary Fund ranks Somalia among a handful

of countries, including Sudan, Yemen and Afghanistan, with almost no financial buffer against such shocks.
Cuts to aid from the US and United Kingdom, two of Somalia's most important humanitarian funding sources, have further deepened the country's economic pressures.
Seasonal conditions may also play a part. According to analysis from the Institute for Security Studies, a Johannesburg-based think tank, attacks typically fall during the winter monsoon, when rough seas keep small boats close to shore, before rising again as the waters calm in spring.

What role does illegal fishing play?

Somalia has the longest coastline in mainland Africa, while its exclusive economic zone covers an area larger than its landmass.
The country is still rebuilding after decades of civil war, with law enforcement stretched thin on land and no effective coastguard to patrol its waters.
The African Development Bank estimates Somalia loses about $300m a year to fishing fleets operating illegally in its waters.
Coastal communities have long accused foreign trawlers of depleting stocks on which local fishermen depend.
That grievance helped shape the first major wave of piracy attacks in the 2000s, when some fishermen took up arms to defend the waters that nobody else was protecting.
But piracy has since developed far beyond that origin story. Andrew Mwangura, a maritime security consultant who spent three decades at sea and later helped negotiate hostage releases during the earlier crisis, told Al Jazeera that the motive had changed.
"Before, the people were vigilantes mainly driven to sea because of illegal fishing in Somali waters and the dumping of toxic chemicals. Now it is more about seizing ships for ransom," he said.
Recent attacks suggest both dynamics may still be present. According to the French navy's Maritime Information Cooperation and Awareness Center (MICA Center), pirate groups operating far offshore typically use dhows disguised as fishing boats as floating bases. From them, crews launch fast skiffs capable of striking vessels as far as 600 nautical miles (1,111km) from the Somali coast. Mwangura believes at least some of those involved are trained seamen, pointing to their use of GPS navigation and long-range vessel-tracking systems.
Closer to shore, the MICA Center has identified a different pattern, with attacks launched directly from the coast and aimed at foreign fishing boats accused of stealing Somali fish rather than commercial vessels.

Who is financing the pirates?

Recent piracy operations also appear more organised than the image of impoverished fishermen taking opportunistically to sea might suggest, according to experts and Somali officials tracking the resurgence.
A former pirate speaking anonymously to Al Jazeera said that today's operations are financed by investors, often businesspeople in Yemen and Somalia, who supply crews with satellite phones, navigation equipment, weapons and provisions to head to sea.
A joint study by Interpol, the United Nations and the World Bank found that during the earlier piracy crisis, financiers behind attacks typically took 30 to 50 percent of ransom payments. The men who actually boarded ships generally received a much smaller fee.
The study found that small groups in communities near pirate anchorages also supplied crews with food, repairs and khat, a stimulant leaf widely chewed in the region.
Abdifatah Mohamed Abdinur, a state minister in Puntland's government, said the pirates were also linked to criminal networks operating across Somalia and Yemen, allowing some groups to operate closer to the Yemeni coast and with a greater hijacking success rate.
"There is definitely a connection," Abdinur told Al Jazeera, "but we have to put the pieces together to make the big picture clearer."

Can another major piracy wave be prevented?

The security landscape around Somalia has changed considerably since the last crisis.

The international response to piracy helped turn nearby Djibouti, which sits on the narrow Bab al-Mandeb Strait between the Red Sea and the Gulf of Aden, into a hub for foreign military forces. The area is now one of the world's most crowded strategic arenas. There are signs that another response is beginning to take shape, though its scope and prospects for success remain uncertain. The European Union's foreign policy chief, Kaja Kallas, signed a new basing agreement with Djibouti in July, preserving access for Operation Atalanta and a second EU mission patrolling the Red Sea. Saudi Arabia has assembled a maritime task force for the Red Sea that a growing number of countries, including Somalia, have joined. In early August, Puntland's president also signed an agreement with a visiting US military delegation to deepen maritime security cooperation around Bosaso, its main port.

Officials from Somalia, Djibouti, Ethiopia and Yemen met in Nairobi this week under a UN-backed programme aimed at strengthening intelligence-sharing on piracy and other maritime crime.

These measures could make hijackings more difficult. But the conditions that allowed piracy to survive the last international crackdown have not disappeared.

Elmi, the Somali academic, argues that naval patrols alone cannot prevent piracy from repeatedly resurfacing. "Onshore-based solutions are more sustainable when it comes to dealing with piracy on the Somali coast," he told Al Jazeera.

Did America Win the War on Terror?

It depends on where you look.

By Arthur Herman

Source: https://www.city-journal.org/article/war-on-terror-911

Sep 01 – Anyone over 40 remembers the Global War on Terror. As announced by President George W. Bush, it was a multipronged effort on five continents to eradicate the networks that had inspired and supported the attacks of September 11, 2001, along with the jihadi Muslim extremist movement that had murdered not only nearly 3,000 people that day but thousands more around the world, including in Europe and Israel, over five decades.

By one (admittedly biased) estimate, calculated 20 years after the attacks, the war on terror had cost $8 trillion, including hundreds of billions spent to bring about regime change in Iraq and Afghanistan, where over 7,000 American military personnel lost their lives and 52,143 were maimed and injured.

The war on terror also led to a radical restructuring of government under the Patriot Act, which enabled unprecedented cooperation among federal intelligence agencies and expanded federal powers of electronic surveillance to uncover terrorist networks and their supporters. It gave the Treasury Department a new global reach to find and shut down the financial networks that paid for terror.

Here we are, 25 years later, though, and some would argue that, far from having eliminated support for Islamist terrorism, we see its sympathizers embedded in our politics.

The skeptics would point not only to our failure through two "endless wars" to bring about democratic regime change as promised in Iraq and Afghanistan but also to the spread of jihadi sentiment in the streets of

American cities—and even on the campuses of our most elite colleges and universities. They would point to a popular commentator (Hasan Piker) who has declared that America "deserved 9/11," and yet shows up on the campaign trail for some Democratic politicians. In the aftermath of 9/11, University of Colorado–Boulder professor Ward Churchill was fired for saying something similar (he referred to the victims as "little Eichmanns"). Today, he'd be chair of his department or running for Congress. A skeptic can find other glaring evidence that those who wished us harm on 9/11 have found a sympathetic home here in the United States. Consider the ebbing support for Israel, whose efforts to defend itself against enemies committed to its destruction are routinely denounced as "genocide" in the same elite circles that express sympathy for Hamas and other terrorist groups whose aims are explicitly genocidal.

We've seen attacks on Jewish students at leading college campuses and in the streets of major cities, where the presence of pro-Hamas banners and Palestinian flags is no longer shocking. And we've seen the election, in the city with the country's largest Jewish population, of a mayor who has repeatedly equivocated when pressed about Hamas and anti-Israel extremism.

Even worse, the Biden administration's open-borders policy led to a flood of terrorist watch-list candidates hammering at our gates. According to data from U.S. Customs and Border Protection, border officials encountered at least 382 individuals on the federal terrorist watch list trying to cross the southwestern border illegally between fiscal years 2021 and 2024. How many more slipped through undetected is anyone's guess, but at least 99 were released after being detained—with

at least 50 still unaccounted for.

The U.S. Muslim population has more than doubled, from roughly 2 million in 2001 to more than 4 million today. It would be outrageous to claim that any beyond a small minority of American Muslims are terrorists or terrorist sympathizers. Yet there is no denying that some heavily Muslim communities—including Cedar-Riverside in Minneapolis and, more recently, Dearborn, Michigan—have emerged as centers of concern over Islamist radicalization. In Europe, the terrorists seem to have gained the upper hand. Major cities, from London and Paris to Brussels, Madrid, and Milan, regularly see masked and black-garbed Islamists flood their streets to protest and riot, while political leaders cower before the social and cultural crisis they have helped create.

It's true that America hasn't suffered another attack as catastrophic as 9/11, though not for want of trying by terrorists seeking to emulate their predecessors. Instead, we've endured a series of long-wolf attacks, from the 2009 Fort Hood shooting and the 2013 Boston Marathon bombing to attacks on synagogues and Jewish individuals. What would have seemed monstrous before 9/11 has become a recurring feature of American life.

Was the Global War on Terror worth it? When considering that the radical Islamist movement once run remotely from bases in the Middle East or Somalia is now excused or openly celebrated here at home within the ranks of the Democratic Party, a reasonable person could answer: No.

Yet strangely, in the Middle East itself, the terrorist cause has rarely been weaker.

Over the past two decades, we've seen al-Qaeda reduced to a shadow of its former self, and likewise its more savage and apocalyptic successor, ISIS. Though the Taliban remains firmly in control of Afghanistan after the U.S. withdrawal in 2021, and violence by radical Islamist groups has surged in Pakistan, the opportunities for jihadis to export terror beyond their borders have shrunk.

Over the past two years, Israel has essentially destroyed Hamas as a conventional fighting force and steadily reduced Hezbollah from a strategic threat to a diminished one, with little or no pushback from its Arab neighbors.

Iran has long occupied the center of the global terror network—yet its power and influence are at historical lows. When Donald Trump entered the White House for the second time, Iran was the dominant power in Syria, Lebanon, Iraq, and Gaza, as well as a major force in Yemen through its Houthi proxies. Tehran was also being regularly courted by Turkey and Qatar and had built a formidable alliance with both Russia and China.

Now, Iran has been mostly forced out of Syria, Iraq, and Gaza. Its proxies are in retreat both in Lebanon and the Arab peninsula, while Turkey has been aligning itself with the major new geopolitical force in the region: the Israeli–Arab Gulf state alliance that Trump has fostered. As for Russia and China, their influence in the Middle East has been reduced to cameo appearances rather than starring roles.

The biggest change of all has been in Saudi Arabia. Under Crown Prince Mohammed bin Salman, the country that spawned most of the 9/11 terrorists has moved slowly but decisively into the U.S./Israel camp—one might even say the Western camp.

As for Israel itself—now, as always, the prime target of the leftist/jihadi movement—the Jewish state has never been stronger regionally or more firmly entrenched as a U.S. ally.

If this is what losing a war on terror in the Middle East looks like, it's hard to imagine what winning might resemble.

So why the disconnect with what has happened here at home?

In the end, we must conclude that the success of America's jihadi enemies domestically has less to do with their intrinsic strength and more to do with us—specifically, with a lack of confidence in our own values and civilization, especially the Judeo-Christian values on which our civilization is built. This is particularly true among our college-

educated elite today, but its roots go back to the days and months after 9/11 itself. We saw it first in the Left's swift change of heart when it came to standing up to terrorism following the massacre of Americans on that day. After some initial enthusiasm for taking the fight to the enemy by stamping out al-Qaeda in Afghanistan and then seizing weapons of mass destruction in Iraq, it didn't take much—a few photos from the rogue prison at Abu Ghraib—to convince the Left that a robust response to Islamist terrorism "wasn't who we were." The Left soon decided that U.S. efforts were only creating more terrorists than we captured or killed—or fueling Islamophobia. The best way to defeat terrorism, the argument seemed to go, was to admit that we were in the wrong, as we had been since at least 1948.

That's why it's no good blaming the Bush administration alone for serial policy failures in Iraq, or Afghanistan, or anywhere else. The Left was primed for defeat from the start, as epitomized by the Obama administration's decision to cultivate closer relations with the Islamic Republic of Iran while distancing ourselves from Israel.

American support of Israel, or lack of it, has always been a barometer of how we feel about ourselves. During the Six-Day War in 1967, Americans never felt stronger, and support for Israel cut across the political spectrum. Today, elites are down on America and about their own future prospects. Support for Israel has paid the price.

Soul-searching about the war on terror has an earlier analogue in questions that lingered after the end of the Cold War in 1989. Two decades later, some of us asked: "Who won the Cold War?" We wondered because we saw leftist academics enthralled by Communism and socialism more firmly entrenched in our colleges and universities than ever before. Now their students are out in the world, with their deeply distorted views of the U.S. and the West. That view, in turn, resonates in today's politics, shaping an equally skewed view of the Middle East and Israel and of America's global responsibilities.

Objectively, America as leader of the West has rarely been stronger. It is the sole superpower; the builder of a grand alliance between Israel and the Arab Middle East; the world's biggest producer of oil and gas; the leader in AI compute and innovation, the decisive door to the future. The United States dominates the globe. And yet.

Rarely have political perceptions been more out of step with empirical reality. After the massacre of 9/11, we avenged our countrymen and defeated evil where it truly lived. What we didn't know then was that we would have to defeat it here, as well.

Arthur Herman is the CEO of Freedom's Forge Solutions LLC and author, most recently, of *Founder's Fire: From 1776 to the Age of Trump*.

The Shifting Landscape of Islamist Terror Since 2001

By Bruce Hoffman

Source: https://www.city-journal.org/article/war-on-terror-taliban-al-qaeda-islam

Sep 02 – Twenty-five years after 9/11, the United States faces a disquieting paradox. On the one hand, the country has largely been spared another major terrorist attack. Only one lethal incident directed by a foreign terrorist organization has succeeded on American soil since 9/11: the 2019 shooting at Naval Air Station Pensacola by a Saudi al-Qaeda operative, which killed three sailors and wounded eight others. This record is a towering achievement. In the dark and fearful days after 9/11 and during the early years of the war on terror, such an outcome was a matter of hope rather than certainty. The horrific attacks in Madrid in 2004,

London in 2005, Mumbai in 2008, Paris in 2015, Sri Lanka on Easter Sunday in 2019, and Moscow in 2024 underscore the importance of the 9/11 Commission's recommendations and the Intelligence Reform and Terrorism Prevention Act of 2004 in keeping the United States safe from another catastrophic attack.


Photo by Ibrahim Khader/Pacific Press/LightRocket via Getty Images

On the other hand, the broader war on terror has produced a more troubling, and still unresolved, outcome. Al-Qaeda survived, spawning a global network of franchises, allies, and even more lethal offshoots. A decade ago, its Iraqi affiliate, rebranded as the Islamic State, resurrected the long-defunct but deeply venerated Muslim caliphate: the supranational political-religious authority governed by Islamic law (Sharia). At its peak, the Islamic State controlled some 40,000 square miles and ruled nearly 8 million people across Iraq and Syria. After a five-year campaign involving some 90 countries, the group was ultimately defeated. But the ideology—and divinely ordained narrative—that sustained it, and has long guided al-Qaeda, remains a force driving both organizations.

The situation today therefore remains worrisome. The Taliban again rules Afghanistan, with al-Qaeda reportedly having recently reestablished its pre-9/11 terrorist training camp at Tarnak Farm. Al-Qaeda's affiliate in the Sahel, JNIM (Jama'at Nusrat al-Islam wal-Muslimin, or the Group for the Support of Islam and Muslims), has besieged Mali's capital and threatens to overrun the country. In East Africa, al-Shabaab continues to undermine the stability of the Somali government, while the Islamic State's network of branches wages violent campaigns across Africa, the Middle East, and Asia. In recent years, its adherents have carried out attacks in countries as diverse as Iran, Turkey, Russia, and the United States.

Two factors explain the resilience of the Salafi-jihadi terrorist movement. The first is ideology. Both al-Qaeda and ISIS draw from the same intellectual tradition, rooted in the conviction that Muslims are under siege from foreign infidels, corrupt apostate regimes, and a Western liberal order fundamentally hostile to Islam. That worldview was most powerfully articulated by Abdullah Azzam, the Palestinian-Jordanian cleric who became Osama bin Laden's mentor. Building on the medieval theologian Ibn Taymiyyah's treatise *The Religious and Moral Doctrine of Jihad* and the writings of his own mentor, the Egyptian Islamist thinker Sayyid Qutb—especially his seminal work *Milestones*—Azzam transformed the concept of *fard ayn*, the individual Muslim's obligation to defend the faith wherever it is threatened, into a universal call to arms. Azzam was assassinated in 1989, but the clash-of-civilizations framework that he advanced remains the ideological bedrock of both organizations.

The second factor is organizational adaptation. After al-Qaeda's core leadership was decimated following 9/11, the group devolved authority to regional franchises. Within eight years, for example, its affiliate in Yemen, AQAP (al-Qaeda in the Arabian Peninsula), had surpassed the parent organization as the most serious terrorist threat to the United States and its allies. ISIS replicated that model less than a decade later, dispersing into 33 formal "provinces" across nearly a dozen countries. This decentralized structure has enabled both groups to absorb repeated military setbacks

while continuing to marshal fighters and resources to prosecute the war that bin Laden declared 30 years ago.

The differences between al-Qaeda and ISIS have always been more tactical and hence stylistic than strategic or substantive—matters of tone, not ideology or outcome. Both reject democracy as incompatible with Islamic governance, both seek the restoration of a caliphate under strict Sharia law, and both frame Western influence and intervention in Muslim lands as necessitating violent resistance. When the Islamic State's founder and leader, Abu Bakr al-Baghdadi, announced the caliphate in June 2014 and declared himself caliph, he was not departing from bin Laden's vision but accelerating it.

Taliban security personnel stand guard near the Torkham border crossing between Afghanistan and Pakistan (Photo by Aimal Zahir / AFP via Getty Images)

With this bold move, al-Baghdadi dramatically upstaged al-Qaeda. His aim was to achieve what bin Laden had only promised: nothing less than redrawing the map of the Middle East, erasing the artificial states and borders created by the Western powers after World War I, and laying the foundation for the resurrection of a Muslim empire stretching from Spain across North Africa, through the Middle East and the Caucasus, into South and Southeast Asia. Though the new caliphate proved short-lived and ultimately fell to the international coalition arrayed against it, the surviving remnants of the Islamic State continue to derive satisfaction from having withstood the combined power of a massive coalition led by the most technologically advanced military in history: the U.S. armed forces. In one of his last publicly released video addresses, in 2004, bin Laden similarly boasted that al-Qaeda had defeated the Red Army in Afghanistan and forced its withdrawal in 1989. He even claimed to have set in motion the chain of events that led to the collapse of the Soviet Union and the demise of Communism as a global ideology. Having survived the war on terror proclaimed by President George W. Bush, al-Qaeda, bin Laden argued, had demonstrated that the same fate would eventually befall the world's other superpower, the United States. For both ISIS and al-Qaeda, their continued existence reinforces the narrative that the ultimate triumph of Salafi-jihadism is divinely ordained. If bin Laden were alive today, he might well be pleased. The enterprise he launched in August 1988 has survived decades of sustained, international counterterrorism pressure. And it continues to inspire violence and resistance, attracting new recruits and supporters who were not even alive on September 11, 2001. This is exactly what bin Laden's chief bodyguard, Abu Jandal, said would happen. "In case of his death, I think he will be a symbol for all those who follow him," Abu Jandal told bin Laden's biographer, journalist Peter Bergen, as recounted in Bergen's *The Osama bin Laden I Know*. "His death will be a great force for stirring up everybody's emotions and enthusiasm to follow him on the path to martyrdom."

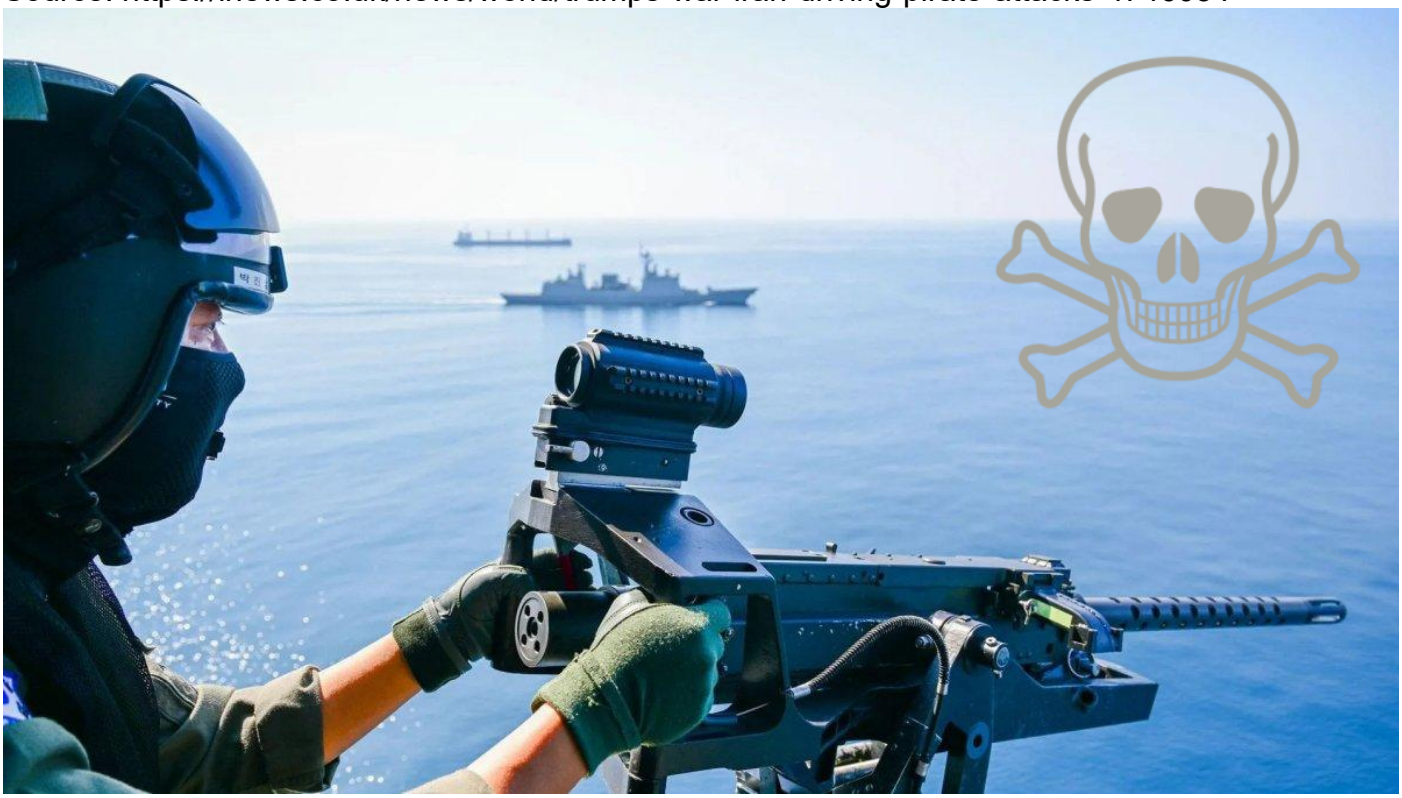
The result, a quarter-century after the epochal 9/11 attacks, is a movement that has defied predictions of its demise. It has franchised itself across continents,

recruited fighters born after 9/11, and sustained an ideology compelling enough to inspire violence from North Africa to Southeast Asia. Protecting the American homeland has been a success. Defeating the movement that made 9/11 possible has not—at least, not yet.

Bruce Hoffman is a professor in Georgetown University's School of Foreign Service and the senior fellow for counterterrorism and homeland security at the Council on Foreign Relations.

Trump's war in Iran is driving the worst wave of pirate attacks in decades

By Kieron Monks | Foreign news and feature writer
Source: https://inews.co.uk/news/world/trumps-war-iran-driving-pirate-attacks-4746034



Sep 06 – The *MV Lutuf* was lightly protected when it was boarded on 17 August. Just two security guards were present on the Turkish cargo ship as it sailed off the coast of Somalia, and they were overwhelmed by six gunmen.

The pirates took 10 hostages and demanded a multi-million dollar ransom for their release. But a bloody Turkish-Somali assault last week freed the prisoners and left many of their captors dead.

The incident set off alarms among counter-piracy forces that are facing the largest surge in attacks around the Horn of Africa in more than a decade. It marked the first known case of private security forces being overcome by pirates in the region, and – part of an emerging and concerning trend – the raid was reportedly launched from another hijacked ship.

Mohamed Jama, base commander of the Puntland Maritime Security Force, is tasked with tackling marine crime around the Somali autonomous region where many of the attacks have originated.

"The resurgence of piracy in 2026 is more dangerous," he told *The i Paper.* "When you look at the capability, the

momentum, and the ability to go to the deep sea."

Incidents have surged. According to an AFP study of UN data, there were at least 15 attacks on shipping in the region this year compared to five in 2025, and more than any whole year since 2013. The Royal Navy, which recently completed a spell leading a multinational Combined Maritime Forces in the region, reported 25 pirate-related incidents in six months to late August.

The figures include a series of successful hijackings, including two in four days last month. Five vessels and 87 crew members are being held by pirates after the *Lutuf* was freed, according to the UN, with millions sought in ransoms.

Experts and officials point to new groups with new methods and new alliances, and a powerful set of drivers for the rise of piracy, including factors linked to the Iran war.

At least three distinct pirate groups are now operating off Somali coasts, according to Castor Vali, a risk management firm focused in Africa. They typically attack through high-speed approaches and gunmen armed with rocket-propelled grenades, the firm said.

Jama said the Puntland-based groups have connections to "cross regional criminal networks" that stretch as far as Yemen, and they are increasingly hijacking vessels to use as "motherships" – as with the *Lutuf* – that allow them to launch surprise raids on vessels hundreds of miles offshore.

Analysts point to anti-piracy patrol forces being redirected due to the Iran war. At the height of Somali piracy attacks, EU, Nato, and other multinational forces were deployed to the region and helped to bring piracy incidents down from a peak of 237 in 2011 to just 15 two years later.

But those missions have dwindled in recent years. Tim Walker, who has studied piracy in the region for 15 years at the Institute for Security Studies, said the reduction of naval forces in the region is "very visible".

The EU's Operation Atalanta lists just "one to three surface vessels" to cover an area of around three million square miles. The mission commander warned in May that anti-piracy efforts have been weakened by a reduced presence of the 47-nation Combined Maritime Forces, whose base in Bahrain has come under heavy attack by Iran.

The Indian navy, which has played a significant role in suppressing piracy, has also redeployed assets to protect shipping around Hormuz. But the loss of American resources may be most damaging.

"The US has been completely pulled into its conflict with Iran," said Walker. "The US was the main provider of maritime security, and ships and support to other countries who wanted to patrol the area as well. Now they have been cut off." The US State Department declined to comment.

Mostafa Elbanna, head of the Somalia branch of the UN Office on Drugs and Crime, said the reduced security presence was offering encouragement to pirate groups.

"For sure the Iran conflict is a distraction for international naval forces, so the pirates know that the response (to attacks) will be a little bit less compared to what they were facing before, which gives them more motivation," he said.

Elbanna added that successful hijacking and ransom attempts led to more attacks, as groups were able to use the money to plan further raids. Their success can also inspire other groups. The Somalian government has asked foreign governments and companies not to pay ransoms to avoid encouraging attacks.

Another by-product of the Iran war is that ships were directed away from the Strait of Hormuz onto other routes, sometimes bringing them closer to Somali waters.

Dr Alessio Patalano, a naval expert at King's College London, said one factor in increasing piracy is the slow circulation of shipping around the Gulf of Aden between Yemen and Somalia, adjacent to the Bab al-Mandab route, which is being used as an alternative to the Strait of Hormuz.

"As a result you have a context that is more favourable to conduct attacks… it's surprising that it's taken this long for pirates to take the opportunities presented to them," he said.

A senior officer of an oil tanker who was

trapped in the Persian Gulf for months during the blockade of Hormuz before recently passing the Strait, said security advisors warned of a growing threat of piracy, with many ships holding valuable cargo but not moving.

"Our security briefings indicated a probability of a resurgence of piracy," said the officer, who was granted anonymity to speak freely. "The sheer amount of vessels idling in the Indian ocean, or close to Bab al-Mandab, or close to Oman, was too much of an opportunity [for pirates] to pass on. And I'm pretty sure that most of those vessels did not even have security guards on board because they were just drifting or waiting for orders."

Experts pointed to other factors driving the surge of piracy. The International Maritime Bureau lifted the Indian Ocean High Risk Area designation in 2023, which led to weakened adherence to security protocols and reduced spending on security, according to Castor Vali analysis.

Elbanna also noted rising economic insecurity in coastal parts of Somalia, with rampant inflation driving up food prices. He said this is exacerbated by illegal and unregulated fishing by international companies, which has undermined the livelihoods of local fishing communities, adding that this has been a major driver of privacy in the area since the 1990s.

"When you have economic pressure, it's easier to be recruited by organised crime," he said.

Local gang leaders are assembling teams of young people and planning attacks for them to carry out, the UN official said, before taking most of the money they generate.

Illegal fishing by international firms that threatens the livelihoods of Somali fishing communities is seen as a driver of piracy (Photo: Abukar Mohamed Muhudin/Anadolu/Getty)

Connections between pirates and criminal groups now extend to Yemen, a launch site for several recent attacks.

Recent reports citing Puntland officials claim the Iran-allied Houthis have supplied equipment and small arms to pirates. The UN has investigated possible coordination but is yet to find strong evidence back the claim.

Jama said the pirate attacks are "complementary" to the Houthis' goal of disrupting shipping in the area, and suggests the militant group could be providing indirect support for pirates through criminal networks. But he believes the pirates' backers in Yemen are "criminal gangs that are not extremists, that are not the Houthis".

Officials and analysts fear the piracy surge is likely to escalate in the coming months. The longer the war in Iran drags on, "the more general maritime security will decrease in the area", Walker said. Countries that supply anti-piracy forces will increasingly look to safeguard their own interests in an increasingly fractious and threatening geopolitical environment, he predicted.

Walker added that cases of successful hijackings and ransom claims this year have shown potential pirates that security can be breached and rewards are possible. "The incentives

have increased and the risks have decreased," he said. Elbanna also points to another factor: the weather: "Right now we are in monsoon season, which is the toughest sea conditions. When the sea is getting better, from October onwards, we are expecting more cases."

What We Have Forgotten About 9/11

By Tal Fortgang

Source: https://www.city-journal.org/article/911-islam-terror-enemies

Sep 08 – Twenty-five years after 9/11, the Islamist war against the liberal, democratic West still shapes our daily lives. Most Americans recognize that certain people and groups around the world want to destroy us—sometimes for reasons we can comprehend, sometimes not. Remembering 9/11 stands, in part, for the proposition that we will not allow the terrorists to win. Our laws, at least as written, have codified that remembrance. They reflect our national conclusion that foreign terrorist organizations are among the most depraved criminal enterprises imaginable. It was once commonplace to hear President George W. Bush declare that you were either part of the free world or aligned with the terrorists. Yet 25 years later, that ultimatum seems far less self-evident.

Consider the axis of leftism and Islamism—the Red–Green alliance, whose cultural and political prominence has grown in recent years. Dalliance with foreign terrorist organizations is part of its organizing ethos. The shocking proliferation of terrorist paraphernalia at post–October 7 protests in 2023 testifies to the rallying power of symbolism—in this case, a symbolism emphasizing sacrificial moral purity and conscientious opposition to decadent Western policies. In the Red–Green worldview, 9/11 signifies the moment

Americans were forced to confront the consequences of their own evil, now visited upon them. Noam Chomsky often advanced versions of this argument on behalf of the Third-Worldist Left; clerics around the world (including some in the United States) have, unsurprisingly, echoed the Islamist account of America's misdeeds.

What has changed today is where expressing such sentiments might get you. In articulating the inescapable conclusion of this line of thinking—"America deserved 9/11," as he put it—Hasan Piker has entered today's Democratic mainstream, not the pariahdom that would have resulted in the early years after 9/11. (To leave no doubt about his views, he recently moved a framed copy of the *New York Times* cover page from September 12, 2001, to be visible over his shoulder while streaming.) Several Democratic Socialists of America candidates have displayed oddly conciliatory instincts toward al Qaeda and 9/11. Drawing a moral equivalence between the U.S. and its enemies has become an important signal in progressive politics, with 9/11 equivocation as its touchstone.

In our mimetic culture, a transgressive message delivered under the guise of forbidden truth can influence millions of susceptible minds. That is what happened in late 2023, shortly after Israel began its counteroffensive in Gaza, when Osama bin Laden's 2002 "Letter to America" went viral on TikTok. As the *New York Times* reported, the letter prefigured our Red–Green moment perfectly: One video with nearly 100,000 likes showed a TikTok user at her kitchen sink with the caption: "Trying to go back to life as normal after reading Osama bin Laden's 'Letter to America' and realizing everything we learned about the Middle East, 9/11, and 'terrorism' was a lie." In a video with more than 60,000 views, another user said the letter showed her that America was a "plague on the entire world."

Such messaging, amplified by algorithms, feeds young Americans' worst instincts while advancing the Chinese Communist Party's broader efforts to sow division in the West. But that explains only half the equation. Exposure to bin Laden's justifications for murdering innocents is one thing—but why would anyone find those justifications compelling? And why did they resonate in November 2023?

To be sure, some of the initial videos were likely inorganic, scripted to create the impression that freethinking young people were reclaiming Islamism from its paranoid American critics. But at least some young Americans proved receptive to the idea that suicide attacks targeting civilians were an understandable, if extreme, response to America's actions abroad and its support for Israel. Our revulsion toward terror, rooted in a tradition of morally constrained violence, has been eroding. Replacing it is an alien, Manichean morality preoccupied with heroes and villains, in which the good are licensed to do whatever they deem necessary to liberate themselves from the evil.

Complementing the new morality is the contention that the United States is a force for evil, perhaps uniquely so in world history. How could such a notion catch on? Here the thesis offered by critic Paul Berman in *Terror and Liberalism*, analyzing the world's rush of sympathy to the perpetrators of suicide bombings in Israel during the opening years of the 2000s—what might be called the era of High Islamist Terror—becomes inescapable:

There was, in short, an idea that each new act of murder and suicide testified to how oppressive were the Israelis. Palestinian terror, in this view, was the measure of Israeli guilt. The more grotesque the terror, the deeper the guilt. And, if unfathomable motives appeared to drive the suicide bombers forward, the oppressiveness of Israel was likewise deemed to be, by logical inference, unfathomable—a bottomless oppression, which had given rise to the maximum of violence, which is suicide murder.

So, too, with 9/11—and, years later, the macabre spectacle of October 7. If others launch such attacks against us,

the assumption must be that they are responding to something intolerable in our own conduct. The alternative—that their violence is irrational and unjustifiable, compelled by some condemnable approach to solving our differences—would require admitting that Western ways of governing and ordering society are, in key respects, superior to those of our rivals. Better, then, to concede the opposite: we made them do it, and we had it coming.

Ironically, this conclusion follows from the liberal pretension of universal rationality advancing toward the future, which leaves no room for fanatic theocrats lashing out with hatred for the West. Yet by turning the accusatory finger inward, it systematically undermines the liberal project to the point of inevitable collapse. It is little wonder that progressives have offered so little resistance to the Red–Green march through their institutions. Until they can say that America and its allies are better than their enemies and deserve to prevail, they will keep ceding ground to those who equivocate about 9/11—if not worse.

George W. Bush, much maligned, was actually right: you are either with us or against us. Our terrorism laws are designed to force institutions around the world to choose between affiliating with the United States—its markets, citizens, and institutions—or aligning with groups we have designated as a uniquely dangerous class of adversary. Congress has prohibited all forms of support for foreign terrorist organizations, which "are so tainted by their criminal conduct that any contribution to such an organization facilitates that conduct." In upholding that principle, the Supreme Court has ruled that even some forms of speech may constitute prosecutable material support if they confer a benefit on a terrorist group.

Our enforcement of these laws, however, lags behind their apparent implications. Expressions of support for terrorist organizations abound, from city streets to conferences where some American lawmakers voice enthusiastic backing. Some of this activity may be protected by the First Amendment. But some of it—from conspiring to disrupt American military supply chains to stealing and burning American flags—is surely not. Yet investigations and prosecutions remain rare.

There is at least one reason for this. As I argue in the forthcoming autumn issue of *City Journal*, courts have been reluctant to hold defendants liable for supporting terrorist organizations, inventing new requirements of knowledge and coordination that the law itself does not impose. This is the legal, highly technical expression of a broader shift over the past 25 years. We have not forgotten 9/11, but we have forgotten that a real difference exists between us and our enemies—and that Americans are right to insist that their nation belongs to those who believe in Americanism, not those who aid and abet its enemies.

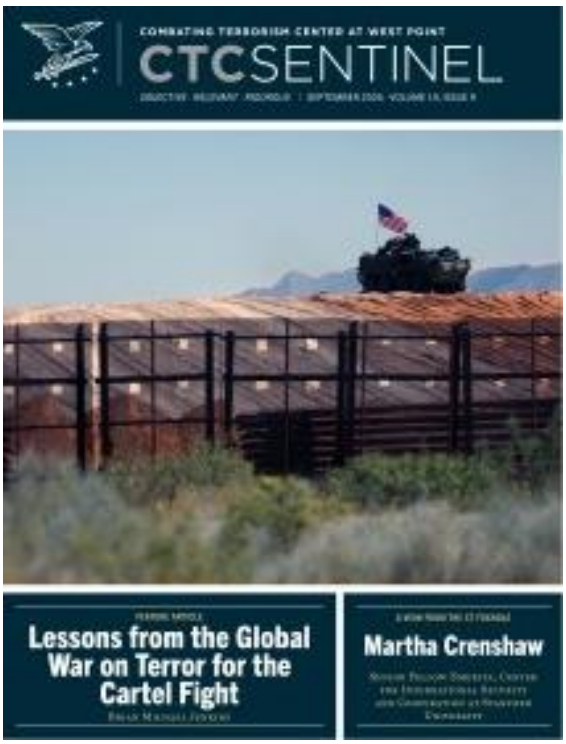
Tal Fortgang is a Legal Policy Fellow at the Manhattan Institute.

CTCSENTINEL

September 2026 Issue | Volume 19, Issue 9
Source: https://ctc.westpoint.edu/september-2026/

This month, the United States will mark 25 years since the terrorist attacks of September 11, 2001. That tragic day set into motion a long and arduous Global War on Terrorism, the impacts of which are still being felt today. To reflect on the lessons learned from the GWOT and how they might apply to the United States' current fight against cartels, we turned to terrorism expert Brian Michael Jenkins who has been studying the phenomenon for more than 50

years. “While the circumstances differ significantly,” he writes, “the campaigns against al-Qa`ida and its Taliban allies, its affiliates, and its successors are instructive. They also offer some cautionary notes.” We also sought insights from leading terrorism scholar Dr. Martha Crenshaw, whose academic career spans more than five decades. She discusses the evolution of the terrorism studies field since 9/11 and reflects on its current focus. “Over the intervening years, we have, if not eliminated, at least severely diminished, the particular threats from al-Qa`ida and ISIS. At the same time, we can always be taken by surprise,” she explains. “It’s critical to avoid complacency.”



Peter Bergen examines the long history of concern surrounding terrorist use of weapons of mass destruction in the post-9/11 years and considers whether, given the current accessibility of extraordinary technologies and capabilities, that concern is more justified today than ever before. “History suggests that terrorists could not deploy true weapons of mass destruction because the barriers to entry were so high,” he writes. “But will those barriers be lowered now that we are in the age of AI and synthetic biology?”

Sandra Pellegrini provides a data-driven overview of the shifting criminal landscape in Mexico. She finds that “between January and August 2026, non-state armed group violence decreased by 19 percent nationwide compared to the same period in 2025.” But she cautions that security operations have corresponded with uneven shifts in patterns of violence in the country, and “in some states, they have likely contributed to violence spreading or even intensified criminal competition. Elsewhere, reduction in violence likely reflects criminal adaptation rather that the dismantling of criminal organizations and networks.”

On a final note, we wish to dedicate this issue of *CTC Sentinel* to the memory of those we lost on September 11, 2001, and in the months and years that followed in the Global War on Terrorism. We dedicate it as well to the professionals who work daily—in a variety of capacities, in ways known and unknown—to keep us safe from terrorism.

Don Rassler and Kristina Hummel, *Editors-in-Chief*

In This Issue

25 Years After 9/11: Lessons for Securing the Homeland

Source: https://www.rand.org/pubs/commentary/2026/09/25-years-after-911-lessons-for-securing-the-homeland.html

The Tribute in Light rises above the New York skyline from the Brooklyn waterfront across the East River in New York, on September 9, 2025 | Photo by Gordon Donovan/NurPhoto via Reuters

Sep 08 – Friday marks 25 years since the September 11 terror attacks. Americans are spending the week remembering those who lost their lives and honoring the first responders and others who sprang into action to help. The attacks cast a long shadow, stretching beyond Ground Zero, the Pentagon, and Flight 93 to transform not just the United States but the world.

RAND experts are reflecting on one of the most enduring aspects of this transformation: what we've learned about homeland security in the quarter-century since the attacks. Below, our researchers answer questions about protecting soft targets, mitigating risks from emerging technologies, and more.

What has stayed with you most about September 11, 2001? How did that day shape the way you think about protecting the homeland?

Heather Williams My professional trajectory has been shaped by many events, but it was set in motion by September 11. The attacks led me to focus on the Middle East and to join the U.S. Intelligence Community. That day stays with me as a reminder that solidarity is interwoven into the American fabric. This is comforting as we grapple with the current national divisions.

My thoughts on September 11 as a policy expert are more nuanced. Policymaking is so difficult because bureaucracy is complex and people are naturally resistant to change. September 11 allowed leaders to overcome much of the resistance, and I lived the positive effects of the Intelligence Reform and Terrorism Prevention Act. At

the same time, the reactionary nature of those changes created a patchwork of organizations working on homeland security, largely focused on terrorism as the threat.
That enterprise is now reorienting toward today's multi-hazard environment but without the catalyst that September 11 provided. Like many others, I'm motivated to build the necessary protective institutions before another tragedy strikes.
Ryan Consaul I think back to the tremendous sense of patriotism and unity born from the great tragedy of 9/11. Sadly, that unity has given way to controversy and division. Congressional oversight remains diffuse, and past bipartisan efforts to enact meaningful legislation to protect the homeland have given way to more-partisan priorities. Given the multitude of threats we continue to face, we need to stand together to tackle ongoing and emergent homeland security challenges.
Given the multitude of threats we continue to face, we need to stand together to tackle ongoing and emergent homeland security challenges.

What have we learned in the years since 9/11 about how best to protect soft targets? What does the evidence say about safeguarding communities from mass attacks by nonstate actors and others?
Brian Jackson For protecting soft targets, we often think first about technology: cameras, weapon-detection systems, or other physical protection measures. But some of the most effective protection comes from the community working together to identify and respond to potential threats. This is called behavioral threat assessment and management, or BTAM, and it's now one of the ways that the majority of K–12 schools, many workplaces, and some police departments or community safety efforts protect themselves. Teams respond when someone's behavior suggests they may become violent. Much of what the teams using this approach do doesn't look like security. For example, they might get the people referred to them into counseling or other programs to redirect them from whatever is moving them toward violence.
BTAM is effective, but it relies on everyone buying in. You can't intervene with a kid who's reading violent websites or making threats if their classmate doesn't let the teacher know what's happening or if the kid's parent refuses to let the child work with a counselor. Building and maintaining trust is tough. We tried to use this approach in the years after 9/11; it was a central part of efforts to respond to radicalization to violent extremism. But because many of the other counterterrorism approaches undermined trust with key communities, the strategy was never able to strengthen homeland security as much as it could have.
John Hollywood The evidence supports starting with layered security strategies in which multiple measures work together to improve the chance that an attack will be stopped or at least mitigated.
These security layers start with prevention. Tips from the public to police or on-site security have often helped to foil plots. Look for warning signs that incorporate a strong motivation to attack with concrete actions to prepare. Things like creating attack plans; researching how to attack; seeking to learn from extremists (including traveling to receive paramilitary training); accumulating large quantities of weapons or materials used in the construction of improvised explosives; and probing or breaching potential attack sites. Be aware that most motivations for mass attacks have been personal rather than ideological or partisan.
For on-site security, focus on the basics. Cases where attackers had direct access to a large crowd have tended to have the highest lethality, so consider how to put distance, barriers, and crowd movement between would-be attackers and crowds. Access-control systems—notably exterior and interior door locks, secured windows, and securable entryways—have all been effective and efficient. However, all require training and maintenance.
Be aware that most motivations for mass attacks have been personal rather than ideological or partisan.

Bystanders and security have stopped attacks. Groups of bystanders tackling shooters has been extremely effective. Again, training can make responses even more effective. That said, training needs to be low-stress and empowering without causing psychological injuries.
For communities, use interagency teams to support prevention, security training, and response planning. We need to establish and fund teams responsible for both educating the public about what to report and conducting diligent follow-up on reported cases. (Brian mentioned an approach for doing so, BTAM, above.) We then need to ensure advance planning and joint training with those agencies that will respond locally to a mass attack.

For many Americans, the creation of the Transportation Security Administration (TSA) and changes to airport screening remain among the most visible legacies of 9/11. What has research found about the TSA?

Kelly Klima Research over the past 25 years suggests that TSA has played a vital role in reducing the risk of terrorist attacks against U.S. aviation. Since 9/11, there has been no successful terrorist attack on a U.S. commercial flight that passed through TSA screening. This record reflects a layered defense-in-depth approach to screening passengers, baggage, and cargo, alongside intelligence, law-enforcement, and industry partners.
TSA has also balanced security with the need to move millions of travelers and large volumes of cargo efficiently and at reasonable cost. The passenger fee is less than $6 per flight, and the total TSA budget (which includes the development and procurement of screening technology) is about $8 billion in 2026.
That balance of security and reasonable cost continues to improve through better physical and chemical screening technologies, changes in checkpoint design and procedures, and risk-based approaches that focus attention where it's needed most.
But the threat continues to evolve. Terrorists and insiders may seek to conceal firearms, explosives, or other weapons in new ways. Emerging cyber and other nontraditional threats require constant assessment. Continued investment in advanced detection technologies, process redesign, and responsibly developed AI can help TSA identify threats more accurately and quickly, strengthen aviation security, and improve the passenger experience.
Continued investment in advanced detection technologies, process redesign, and responsibly developed AI can help TSA identify threats more accurately and quickly.
Williams Americans associate TSA with the blue shirts they encounter at the security checkpoint, but the organization has a broader mandate than many realize. One of the other programs TSA manages is the Security Threat Assessment for multiple security credentials, including the Transportation Worker Identification Credential (TWIC) and Hazardous Materials Endorsement for commercial driver's licenses. RAND research has found that TSA generally executes these programs effectively, at cost, and with timely resolution, in a way that reduces internal threats. For example, TWIC applicants who have no flags for possible disqualifying factors could find a physical card in their mailbox less than six days later.

Many anti-terrorism technologies and capabilities require collaborations between government and the private sector. What have we learned about how to effectively navigate those partnerships?

Thao Liz Nguyen One of the enduring lessons is that the development, maturation, and operational adoption of anti-terrorism technologies can proliferate in well-structured public-private collaboration. After 9/11, the Support Anti-terrorism by Fostering Effective Technologies Act of 2002, enacted as part of the Homeland Security Act of 2002, established the Office of SAFETY Act Implementation and created a statutory framework for

evaluating and incentivizing anti-terrorism technologies. From a technology-evaluation perspective, the SAFETY Act not only encourages innovation in the abstract but applies a rigorous process to assessing technical performance, operational utility, and real-world deployment considerations of mature technologies to emerging capabilities.
Designation and Certification protections under the SAFETY Act have helped mature the market for proven security technologies and services by reducing liability uncertainty and signaling that a capability has undergone meaningful DHS review. At the same time, the Developmental Testing and Evaluation Designation protection has been especially important for emerging technologies, because it allows developers to generate operational evidence, refine concepts of use, and test performance in relevant environments before a capability is fully fielded.
What we've learned is that effective public-private partnership requires more than funding or policy encouragement; it requires credible evaluation pathways, clear incentives for participation, and mechanisms that help bridge the gap between innovation, validation, and scalable adoption for anti-terrorism technologies.
The development, maturation, and operational adoption of anti-terrorism technologies can proliferate in well-structured public-private collaboration.

Of course, new technologies have also transformed the threat landscape. Let's start with unmanned aerial systems, commonly known as drones. How have drones emerged as a potential threat to people and infrastructure, and what do we know about how to mitigate that threat?

Brendan Toland Drones have rapidly emerged as a threat because these systems have become more capable and more available. Parallel advances in a series of technologies (batteries, electric motors, precision manufacturing, optics) have shrunk the airframe for drones, increased their speed and endurance, and lowered their cost. Additionally, improvements in lightweight cameras, guidance via GPS waypoints, and wire-guided control have made it more difficult to detect and take over hostile drones. Finally, drones come in various forms. This lets bad actors select a drone that is optimal for the intended objective, whether that's maintaining an eye in the sky or delivering compact items (contraband, bombs) virtually anywhere at speed.
As part of RAND's work operating the Homeland Security Operational Analysis Center, we evaluated the capabilities of commercially available drones. We found that these systems continue to lower in cost while improving on operationally relevant metrics, such as speed, flight time, and payload capacity. We also developed several high-threat scenarios in which bad actors could use drones to threaten the homeland, including bombing a federal building or delivering a chemical agent outside a major sporting event. Looking across the market, we found more than 500 systems capable of conducting at least one of our high-threat scenarios. This number has only grown in the six years since our research was conducted.
The speed of drones and the ability to launch these systems from virtually anywhere constrains the response time for those working to defend the homeland. In our more recent simulation modeling, we found that defenders had only seconds to a few minutes to detect and defeat incoming drones, depending on the situation. If the adversary uses a drone to provide aerial surveillance, then in many cases the onboard camera enables a stand-off range that undermines detection. Any effective defense requires deploying layered mitigation capabilities in advance, putting these capabilities in the hands of trained personnel, sharing detection information across the homeland security enterprise, and empowering defenders on the ground to make quick decisions.
Christopher Scott Adams Advances in drone technology have made the threat more salient, but the homeland security enterprise has some tools to help mitigate that threat. The Preventing Emerging Threats Act and the SAFER

SKIES Act have given key counter-drone authorities to federal and state/local/tribal/territorial law enforcement, respectively. These include permissions, under certain circumstances, to intercept communications between drones and their operators, track and monitor drone flights, and disable, down, or destroy potential threats.
These authorities have allowed DHS and its partners to invest in counter-drone technologies. At RAND, we've advised our DHS sponsors on the requirements for effective counter-drone capabilities and the right technology mix. This analysis has informed ongoing counter-drone investments at the border and in defense of major events, such as the World Cup and the Olympics.
Advances in drone technology have made the threat more salient, but the homeland security enterprise has some tools to help mitigate that threat.
Across these assessments, we've found a few consistent effective practices to mitigate, though not eliminate, the threat. First, defense-in-depth is key; having multiple types of sensors and effectors (kinetic and non-kinetic) in the same location gives the best chance of detecting and defeating a variety of drone threats. Second, defenders need to plan ahead. This includes resolving authorities issues, developing rules of engagement that are well understood by all operators, and creating information-sharing agreements across responsible agencies. Third, employing automation in defense can provide the speed to respond to a similarly automated threat.

What about artificial intelligence? For example, concerns are rising that AI could enable biological attacks. What do we know about this emerging risk and how best to mitigate it?
Steph Guerra Historically, biological attacks have been rare, unsuccessful, and difficult to execute. That's because of the technical, operational, and motivational barriers that bad actors face. But AI is increasingly able to lower these barriers by democratizing biological expertise, driving laboratory workflows, raising the ceiling of biological novelty, and circumventing existing biosecurity controls like gene synthesis screening. At RAND, we seek to assess these capabilities to help inform policy action that reduces the risk of misuse while still enabling beneficial scientific innovation.
Our team recently published a biosecurity strategy for the AI era to prevent AI-enabled biological attacks. The strategy is deliberately layered, because different mitigations stop different threat actors. For example, access controls like gene synthesis screening may stop a lone terrorist, but they probably can't stop a state bioweapons program. But a state program might be deterred from developing bioweapons by credible attribution and rapid response capabilities. Each layer is critical, but only having one is insufficient.
We know AI capabilities in biology are advancing fast, but thankfully the most hazardous thresholds haven't yet been crossed. That gives us a narrow window to build protective infrastructure before misuse becomes demonstrably easy.
Nguyen Detection technology is being pushed to do more than it was originally built for. This is true for any emerging unforeseen threat. As AI lowers the barrier to entry of designing novel biological agents or even modifying existing ones, screening systems must improve at spotting unusual patterns, not just known signatures stored in their static reference libraries. In practice, that means detection equipment needs to keep pace with new compounds, new delivery methods, and changes in how material may be packaged or concealed.
The challenge is that detection is only as good as the data, calibration, and reference libraries it relies on, so if the libraries are outdated, then the equipment can miss something that doesn't look like the “expected” threat. That's why DHS and other stakeholders should continue investing in research, development, testing, and evaluation; field testing; and recalibration of sensors and screening tools. We also need to think about how these systems are integrated across layers of screening, because no single device is going to catch

everything. We need to invest in innovative detection systems and the algorithms behind them so they can stay adaptive and agile as threats evolve.

David Luckey The convergence of AI with advances in biotechnology and chemistry represents one of the most significant emerging risks to homeland security since 9/11. AI is rapidly lowering technical barriers in synthetic biology, genomics, and chemical engineering. This means that malicious actors could potentially leverage AI tools to design, synthesize, or optimize biological or chemical agents with unprecedented speed and precision.

This risk is not hypothetical. AI-driven platforms can already assist in protein folding, gene editing, and even the design of novel chemical compounds. Used by a bad actor, these capabilities could be repurposed to engineer pathogens or toxins that evade current detection and mitigation strategies. The dual-use nature of AI in life sciences poses unique governance and oversight challenges; the same tools that accelerate medical breakthroughs can also facilitate weaponization.

Mitigating this risk almost certainly requires a multi-layered approach that includes strengthening oversight, promoting responsible innovation, enhancing detection and response, and building cross-sector partnerships. Effective mitigation will likely depend on seamless collaboration between government, industry, and the research community. Proactive risk assessment, horizon scanning, and anticipatory governance are essential to stay ahead of adversaries who might exploit AI for catastrophic ends.

Proactive risk assessment, horizon scanning, and anticipatory governance are essential to stay ahead of adversaries who might exploit AI for catastrophic ends.

Twenty-five years later, what lesson from 9/11 feels most urgent in your work today?

Jackson Responding to threats requires thinking about how we will maintain defenses in the long term, even when the need to respond is most urgent.

The human and financial costs of 9/11 were catastrophic, and so there was pressure to do everything possible to make sure that such a tragedy couldn't happen again. As time passed, it became clear that the costs of all the security and other measures added up over time—and that one of the most effective responses to that specific threat (reinforcing airplane cockpit doors) was one of the cheapest. While government needs to spend to protect the nation, the more expensive security measures are, the harder they are to maintain over time.

Though thinking about the cost-effectiveness of security may seem odd when we're concerned about the risk of disasters like 9/11, doing so is critical, particularly since it's often much cheaper for attackers to try something new than it is for defenders to update protections.

Hollywood We need to stay vigilant but not overreactive.

This means maintaining a focus between overreaction to what have been extremely rare events and inattention to ongoing threats. Similarly, we must avoid getting distracted by a single part of the threat (e.g., focusing on a specific ideology when most attacks are personally motivated) or by a single security technology. Instead, what's needed is a strategic, layered approach that counters the full range of violent threats. Perhaps most importantly, vigilance means maintaining and developing partnerships between the public, security groups, and local, state, and federal agencies to provide ongoing prevention and protection.

Luckey It's imperative to have imagination and adaptability in the face of evolving threats.

9/11 exposed the dangers of “failure of imagination,” specifically the inability to anticipate how adversaries might exploit emerging or unexplored vulnerabilities. Today, as we confront the intersection of AI and biological or chemical weapons, that lesson is more urgent than ever.

Our adversaries are agile, opportunistic, and increasingly technologically sophisticated. The tools of mass disruption are no longer confined to nation-states or well-resourced groups; they're becoming accessible to a broader

spectrum of actors. This reality demands that we continually reassess our assumptions, update our risk models, and foster a culture of innovation and vigilance across the homeland security enterprise. I'm reminded daily that security is a dynamic process, not a static end state. The post-9/11 era amplified the value of intelligence sharing, public-private partnerships, and resilience. But it also illuminated that the next threat might not look like the last. Our greatest asset is the ability to anticipate, adapt, and act—before the unimaginable becomes reality.

Heather Williams is director of research strategy and a senior policy researcher at RAND, and a professor of policy analysis at the RAND School of Public Policy.
Ryan Consaul is a senior policy researcher at RAND.
Brian Jackson is a senior physical scientist at RAND.
John Hollywood is a senior operations researcher at RAND.
Kelly Klima is a senior engineer at RAND and a professor of policy analysis at the RAND School of Public Policy.
Thao Liz Nguyen is associate director of the Infrastructure, Immigration, and Security Operations Program in the RAND Homeland Security Research Division, a professor of policy analysis at the RAND School of Public Policy, and a senior physical scientist at RAND.
Brendan Toland is director of the Navy and Marine Forces Program in the RAND National Security Research Division and a senior operations researcher at RAND.
Christopher Scott Adams is a senior policy analyst at RAND.
Steph Guerra is a biosecurity resident and head of AI x Bio at RAND.
David Luckey is a senior policy researcher at RAND and a professor of policy analysis at the RAND School of Public Policy.

The Failure to Stop 9/11 Was a Catastrophe. But Even Bigger Mistakes Were Made in Its Aftermath

By Greg Barton

Source: https://www.homelandsecuritynewswire.com/dr20260909-the-failure-to-stop-9-11-was-a-catastrophe-but-even-bigger-mistakes-were-made-in-its-aftermath

Sep 09 – The September 11 2001 terrorist attacks were unlike anything the world had seen before. For America, and the watching world, September 11 (or 9/11) seemed most like a Pearl Harbour moment – a devastating surprise attack by a distant enemy that demanded a response. But here the distant enemy was not a nation state in the middle of war, it was a ragtag collection of rebels living in mountain hideouts, long underestimated and widely misunderstood.

It took Hollywood movies to convey the horror of Pearl Harbour. But hundreds of millions around the world watched, via live satellite TV feeds, in disbelieving horror as a fully laden commercial aircraft slammed into the first World Trade Centre tower in New York. Hundreds of millions more saw the second tower hit, then witnessed both massive skyscrapers collapsing faster and more completely than seemed possible.

At the time, this felt like a moment that changed everything – a hinge point in history on which so much would turn. Twenty-five years later, that devastating intuition has been confirmed through a cascading series of grim events and tragic mistakes.

Could the September 11 Attacks Have Been Prevented?

In September 2026 we live in a world of uncertainty and change. Geopolitics, technology and the

physical world are experiencing rapid transformation that fascinates and terrifies in equal measure. Much of this would have occurred without September 11, but there is a sense in which that day changed all these things. The collapse of 80 years of global order cannot be said to have simply resulted from the world's biggest terror attack, but it certainly played a role in triggering a series of responses that has changed all the nations involved. Could the September 11 attacks have been foreseen and prevented? Absolutely. Counterterrorism intelligence has evolved massively over the past 25 years. But international terrorism was not new in 2001, nor was al-Qaeda – the terrorist group responsible – completely unknown and operating without scrutiny.

Well before the 9/11 Commission report was published, it was clear there were multiple "if only" moments that may have prevented the attack. If only those sounding the alarm had been listened to. If only the FBI and the CIA had put aside their rivalries to trust each other, fully share what they knew, and act on it. If only the threat posed by al-Qaeda was taken more seriously. At all of these points, the attacks could have been stopped.

The September 11 attacks were audaciously ambitious, involving global orchestration of planning, training and execution on a scale never seen before. In the decades that followed, there have been dozens of mass-casualty terrorist attacks, first by al-Qaeda and then by its spinoff, Islamic State.

The biggest and most effective have been in conflict zones where explosive material is readily available and the tempo of violence makes stopping every attack impossible. But in stable states there have been multiple massive attacks that have killed hundreds at a time. One year after 9/11, in 2002, the October 12 bomb attacks in Bali took 202 lives, 88 of them from Australia.

Lessons Have Been Learned

One area of lasting success in the past 25 years is the development of police lead intelligence. Police forces are now cooperating effectively across international agencies, which have developed remarkable capacity to intercept communications and disrupt planned terror attacks involving cells and networks.

In our region we have witnessed the remarkable results of close cooperation between the Indonesian police and the Australian Federal Police (AFP).

Thankfully, the ratio between attempted large-scale attacks that were detected and disrupted and those that have succeeded is large. Increasingly, the vast majority of terror plots are being thwarted at the planning stage.

The flip side of this is that lone actor attacks, with one or two gunmen acting alone without a cell or a network, remain a constant threat that is not easily countered. Australians were reminded of the horror of such attacks in the Bondi Beach shootings of December 2025.

Were it not for this welcome international cooperation and fast-evolving capacity, the past 25 years would have seen many thousands more lives lost.

However, this does not mean the threat posed by terrorist organizations seeking to inflict a mass casualty attack has been eliminated. Thankfully, it's highly unlikely an attack of the scale and nature of September 11 could be repeated. But it is not impossible. The best intelligence systems in the world are only as good as the political frameworks in which they exist, and the leaders they serve.

A terrible recent reminder of this occurred on October 7 2023, when the al-Qaeda aligned Hamas terror group, based in the Gaza Strip and supported by Iran, succeeded in a mass attack on Israel.

Even more than was the case with the 2001 attacks, there were multiple intelligence reports and warnings given ahead of October 7. The attacks succeeded not so much because of an intelligence failure as a failure by Israeli leadership to listen to the intelligence.

Almost three years on, there has yet to be a proper reckoning of how

Hamas managed to succeed beyond what anyone had dared think possible. Hubris and misplaced confidence in modern technology, a structural unwillingness to listen to junior intelligence officers, particularly women, and a complex web of political interests and cynical manipulation came together to defeat some of the world's best counterterrorist intelligence.

The years since the October 7 attack by Hamas have shown the true potential of terrorism to provoke an angry, vengeful response that involves striking out without any plan, with catastrophic consequences.

The devastating impact of the response to the Hamas attacks, not just on the two million plus people living in the Gaza Strip but more broadly on Israel, the West Bank, Lebanon and the wider Middle East, is the topic for another discussion.

But it is that vengeful, angry response of understandable outrage that is causing the greatest lasting damage.

How the Response to Terrorism Creates More Terror

One clear way the September 11 attacks changed the world was as a catalyst for a decades-long global "War on Terror". This war never had a clear strategic plan or an agreed endpoint. Instead, it saw first Afghanistan, then Iraq, drawn into destructive conflict that amplified threats and gave new opportunities to terrorist groups. Al-Qaeda had never been as effective as when the occupation of Iraq gave rise to Islamic State.

Incredibly, 20 years after a relentless military campaign by a global coalition fighting the Taliban in Afghanistan, the al-Qaeda aligned terror group is now running a cruel authoritarian state repressing tens of millions, particularly women and children. It presents a growing threat not just to its immediate neighbors but also to the wider world.

The great mistake made was not the failure to stop the September 11 attacks in the first place, although that should have been achieved. It was the failure to understand how terrorism can amplify its impact through our response to outrage.

To properly understand the way in which September 11 functions as a hinge point in history, we need to look back 50 years before 2001 to see the coalescing of the forces that gave rise to al-Qaeda.

Al-Qaeda's origin story stems from the imprisoning and persecution of Muslim Brotherhood leaders in Egypt in the 1950s. The 1966 prison execution of visionary brotherhood leader Sayyid Qutb saw his brother and remaining Brotherhood leaders flee to Saudi Arabia, where their revolutionary political vision was fused with state-sponsored Wahhabi fundamentalism and the support of Osama bin-Laden. It fueled the global resistance movement in Afghanistan and gave rise to groups such as Jemaah Islamiyah, the Southeast Asian terror network behind the Bali bombings.

Twenty-five years after September 11, the Salafi jihadi terrorist ideas first sketched out by Sayyid Qutb, then realized by al-Qaeda, remain an enduring threat.

Their impact in Afghanistan and central Asia continues to be underestimated. But it is in Africa where both al-Qaeda and Islamic State continue to expand and evolve, inflicting devastating violence across a dozen conflict zones.

Given the September 11 attacks were 50 years in the making, there's every reason to believe the threat unleashed through the rise of al-Qaeda presents an enduring problem.

Sadly, the mistakes of the past 25 years seem set to produce more generations of angry young men drawn to the siren song of revolutionary jihad.

Greg Barton is Chair in Global Islamic Politics, Alfred Deakin Institute for Citizenship and Globalization, Deakin University.

The terrorism threat to Singapore remains high. The ongoing conflicts in the Middle East have contributed to a volatile global security environment and elevated the terrorism threat worldwide. Terrorist and extremist groups have exploited the Israeli-Palestinian conflict and the United States (US) / Israel-Iran conflict tospread propaganda, deepen grievances and incite their supporters to mount attacks against their perceived enemies. These tensions have also contributed towards growing hostility between communities. Anti-Semitism has surged in many parts of the world, while anti-Muslim rhetoric and Islamophobia have also intensified, fuelled by developments in the Middle East and far-right extremist narratives. In some cases, such hatred has translated into violence.

The state of terrorism, 25 years after 9/11

By Atlantic Council experts
Source: https://www.atlanticcouncil.org/dispatches/the-state-of-terrorism-25-years-after-9-11/

Sep 10 – Twenty-five years ago, the United States suffered the deadliest terrorist attack in its history. The September 11, 2001, attacks killed nearly three thousand people and inflicted a collective trauma on an entire nation, fundamentally altering the US national security apparatus, ushering in the “war on terror,” and leading to overhauls of US intelligence and homeland security. But the core problem of terrorism itself—which has existed for centuries—didn’t go away.

As the world reflects on the twenty-fifth anniversary of 9/11, we asked Atlantic Council experts to answer twenty-five pressing questions about how terrorism continues to shape the present era.

1. Was the war on terror successful?

The answer resists a simple *yes* or *no*, and for good reason. Counterterrorism ought to be conducted with grand-strategic discipline, which requires one thing the United States has so far not produced: a stated theory of victory. Twenty-five years after 9/11, no administration has told the American public what the end of this effort looks like or what conditions would permit it to close. "Disrupt, dismantle, and defeat," which US President Barack Obama presented early in his first term, is a task list. The 2001 authorization for the use of military force was stretched across two decades and multiple continents without much congressional pushback. Over those same years, nonstate actors and their state sponsors pushed aggressively into high-tech domains, where cyber operations, artificial intelligence (AI), and cryptocurrency financing now grant asymmetric threats a global reach that the al-Qaeda of 2001 could scarcely have imagined.

Any honest verdict must begin with the human ledger. More than 900,000 people died in direct violence across the post-9/11 wars, including over seven thousand American service members. Their families deserve a candid answer on whether those sacrifices were in vain. National security practitioners delivered two decades of superb tactical execution, proving the ethos I was taught as a young infantry officer: "Lieutenants and sergeants win battles." The shortfall was not with those at the pointy end of the spear. Instead, it lay in statecraft, where four successive administrations resourced the campaign lavishly, institutionalized it across the bureaucracy, and never once defined the end state those tactical triumphs were meant to secure.

Alongside that strategic vacancy ran a failure of basic decency. The United States repeatedly betrayed partner trust, the one element of counterterrorism that no amount of technological or economic power can replace. From the Kurds to the Afghans, the United States abandoned allies who bled beside US soldiers once national interests shifted. I watched the cost of that habit firsthand on the ground in Kabul during the August 2021 evacuation, as Afghanistan returned to the same tyrannical regime whose sanctuary for al-Qaeda had triggered the war.

This legacy of broken trust arrives as the wider strategic environment grows more combustible. As of 2025, conflict data show that state-based conflicts are at their highest level since 1946. That instability directly feeds terrorist networks, providing recruits, sanctuary, and revenue with every political order that collapses. A record of abandoning trusted allies will make the next necessary coalition harder to assemble.

Was the "war on terror" successful? It produced tactical excellence that strategic drift and broken faith squandered. The threat has splintered into forms harder to detect and, in several key domains, more lethal. Naming what victory requires, and keeping faith with those who fight for it, remains unfinished business.

—Omer Rafiq is a nonresident senior fellow with the Atlantic Council's Rafik Hariri Center and Middle East programs.

2. What was the long-term impact of the Iraq and Afghanistan wars on US national security?

Twenty-five years after 9/11 and five years after the fall of Kabul, the United States has not become isolationist—but it has become more realist.

The disappointing ends to the wars in Afghanistan and Iraq soured the American public on "intervention." What exactly that means is still evolving. It has never been a terribly useful unit of analysis. After all, what counts as an intervention? But much of the public debate about foreign policy takes place in those terms anyway.

It seems to mean that the United States will continue to be active in the world, but not for the sake of democracy, human rights, or alliance solidarity. That is exactly what President Donald Trump campaigned on, after all, and his foreign policy has followed his campaign rhetoric. Yet even some of President Joe Biden's policies followed the same logic.

Neither president has led the United States to embrace isolationism. Nothing in Trump's foreign policy, from saber-rattling against North Korea in 2017, assassinating an Iranian general in 2020, capturing the president of Venezuela in January, or going to war against Iran this year, suggests isolationism.

Biden, similarly, assembled and led an impressive coalition to support Ukraine's defense against Russia's aggression. He maintained strong support for Israel's war against Hamas against considerable opposition within his own party and among the United States' traditional allies.

But both presidents have deemphasized the idealistic side of America's role in the world. Trump openly campaigned against it as early as 2016, mocking the idea of democratization and routinely deriding "nation building." While Biden spoke more positively about democracy, he, too, rejected "nation building" and sought to limit America's liability by completing the withdrawal from Afghanistan.

The change is evident in how US officials talk about their purpose. Trump has successfully popularized his "America First" slogan, falsely implying that the old foreign policy consensus did not prioritize American interests. That has percolated into a new vocabulary in which US officials routinely criticize "globalism" and play up supposed conflicts between American interests and global order.

The net result is that the United States has a much more short-sighted approach to the world. It is still active and engaged, but it is now more transactional, less relational; more material, less idealistic; more nationalist, less cooperative.

Yet in some ways, Trump has been arguing against a straw man. The traditional view was not that the United States should invest in the liberal international order in spite of American interests, but because of them. US foreign policy used to be premised on the idea that the liberal international order was the outer perimeter of American security, the engine of American prosperity, and a tool of American influence. Losing that belief is the biggest change and worst defeat in US foreign policy.

—Paul D. Miller, PhD, is a nonresident senior fellow with the Atlantic Council's Scowcroft Center for Strategy and Security.

3. How does the global terrorism landscape today compare with that of 2001?

It's easy to attempt neat analytic delineations on matters that are neither neat nor linear. Still, there is value in comparing September 11, 2001 to today, not so much for any coherence it might illuminate, but to reflect on how much the structure, concept, and category of terrorism has changed.

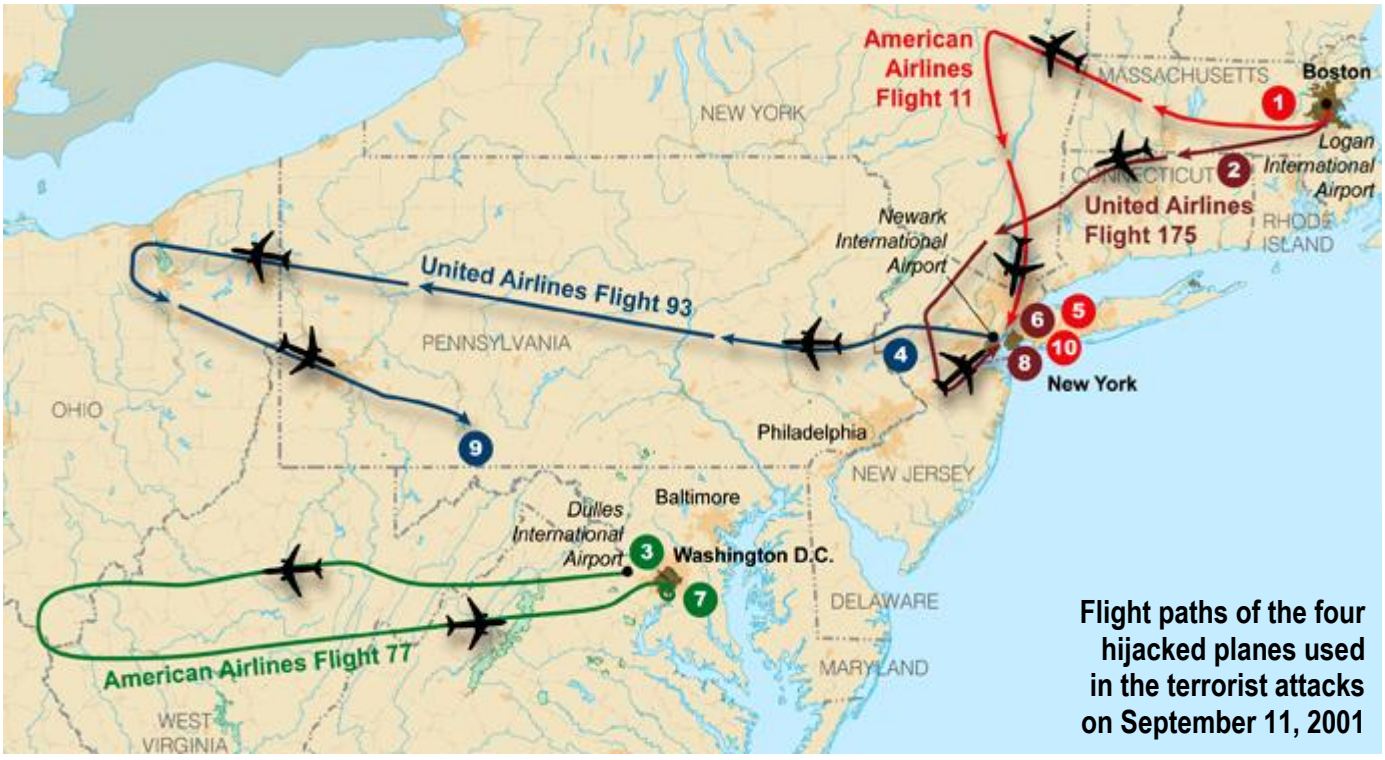
Terrorism, perhaps counterintuitively, is historically contingent. The pre-9/11 terrorism landscape was heterogeneous. Existing groups encompassed a range of forms, including separatist, nationalist, revolutionary, and religious organizations. Although state-sponsored terrorism never circumscribed that era in whole, state sponsorship as a prism supplied a distinctive framework through which governments understood the terrorist threats they faced.

Al-Qaeda represented a mutation: a transnational, nonstate actor operating from ungoverned spaces, with hierarchical leadership, directing complex attacks against a "far enemy." After 9/11, this new model became the dominant paradigm for understanding "modern" terrorism. Global counterterrorism efforts then rapidly organized themselves around finding, fixing, and finishing this new center of gravity.

Today, terrorism has mutated further, giving way to a more dispersed ecosystem. A rough parallel might be made with the move from broadcast television, which was dominated by the major, identifiable networks, to a digital environment with a seemingly infinite plane of platforms, niche communities, influencers, and other content publishers. Al-Qaeda and the Islamic State remain influential brands. But they no longer project exclusive command and control. They do not communicate with or even inspire every potential adherent of their ideas and methods of generating violence. Today's terrorists embed themselves within local conflicts that have local effects, combining terrorism with insurgency, territorial control, and contested governance. Legacy terrorist brands lay claim to still being global, but their grievances, recruitment, and objectives are frequently local. Digitalization has further allowed this atomized polity to radicalize more easily and act with little formal direction and more dispersion.

What then is 9/11's lesson for today? That it is never a clean transition from one kind of terrorism to another. It's a change in form that organizes an understanding of the threat. For the United States following 9/11, the central challenge was to dismantle an organization capable of strategic, spectacular surprise. Today, it is to understand a fragmented and adaptive system in which transnational networks, local grievances, self-mobilization, criminal economies, and state interests overlap.

—Edward Bogan is an adviser to the Atlantic Council's Counterterrorism Project and a retired Central Intelligence Agency operations officer with twenty-four years of experience in national security and intelligence operations and policy.



Flight paths of the four hijacked planes used in the terrorist attacks on September 11, 2001

4. What threat do al-Qaeda and ISIS pose today?

Al-Qaeda and the Islamic State of Iraq and al-Sham (ISIS) no longer resemble the major, bureaucratic, lethal terror organizations they once were. However, both organizations have remodeled themselves and now support networks of splinter groups across the developing world. In Africa, for example, an al-Qaeda–affiliated group controls significant territory in Mali, while ISIS almost certainly manages its global

operations from its hub in Somalia. ISIS and al-Qaeda retain significant influence as terror groups. They have developed broad networks of affiliates and subgroups. And they continue to inspire terror attacks and plots worldwide.

ISIS and al-Qaeda are not resurgent organizations, but they have remodeled in response to the shifting terror landscape. Both groups have spawned extensive networks of affiliates, which aim to spread their ideology, terrorize civilians, and seize territory. Furthermore, ISIS affiliates have long attracted foreign fighters, a trend that has only continued in recent months. As these affiliated terror networks attract fighters and consolidate territorial control, they demonstrate the enduring—if localized—threat these groups pose to weak states.

More importantly, both ISIS and al-Qaeda have adapted their propaganda and influence techniques to the digital age. They can rapidly reach global audiences, radicalizing individuals anywhere with an internet connection and inspiring terror attacks in the West. Their responsive, flexible propaganda machines are the most challenging—and enduring—threat posed by ISIS and al-Qaeda today. Both groups consistently adapt their practices to avoid content restrictions, ensuring that their extreme messages can reach their audiences. This content has inspired individuals to travel to terrorist-held territory and to plot and conduct attacks in Europe and the United States.

ISIS and al-Qaeda still pose a threat, even though the face of the organizations has changed over the past two decades. Their ability to spread propaganda and recruit and radicalize vulnerable individuals underpins their enduring presence as major terror organizations, a presence that is only bolstered by their networks of affiliates. Both groups have demonstrated a remarkable ability to adapt, and they will likely continue to do so in the coming years.

—Morgan Tadych is a nonresident senior fellow with the Scowcroft Middle East Security Initiative at the Atlantic Council's Middle East programs.

5. What is the state of foreign terror threats to the US homeland?

The United States's global war on terror was largely won in the twenty-five years after the attacks of September 11, 2001. It was not a war on terror, in truth, but largely a campaign against a single type of violent Sunni extremism, to which groups such as al-Qaeda and the Islamic State adhered. As a political movement, that type of Salafist politics is dead.

This is not to say that the United States won the wars in Iraq and Afghanistan. The outcomes of those conflicts were different: mixed in Iraq and a resounding defeat in Afghanistan. But as an attractive ideology—as a political idea that can pull adherents and recruits from an ocean away—there is no longer much gas left in the tank. The violence perpetrated against Salafist political projects over the past twenty years has devastated their attraction, particularly in Iraq and Syria. The nascent civil war between Shia paramilitaries and the government in Iraq in the 2000s, followed by the international campaign against ISIS in the 2010s joined by those same Shia paramilitaries, has left the Sunni cities of the northern Levant in ruins. In the heart of the Sunni Levant, few want to try for a third time, and even fewer want to join them.

The threat from violent Salafists still exists, of course. Radical Sunni groups in North Africa, Central Asia, and the Sahel are still a threat, and lone-wolf actors still conduct attacks in the United States and Europe, sometimes professing allegiance to ISIS or al-Qaeda. But their attraction, and their threat to the US homeland, has diminished.

Instead, the looming terror threat to Americans comes from state-directed actors, above all Iran. On the one hand, these are easier to counter: Washington knows where they come from and can interdict various points of the terror supply chain. In contrast, the diffusion and unpredictability of Sunni Salafist terrorism was a constant challenge. It has often been more opportunistic, willing to strike a disco or shopping mall than a more politically meaningful target. On the other hand, Shia militants with state support may be

more capable. It is more likely that a Shia militant would have access to a surface-to-air missile in Turkey that might threaten Air Force One than would a member of ISIS, for example. As a result, modern terrorism, and the modern threat to the homeland, will come from less spastically violent actions and more careful, strategic planning.

—Andrew L. Peek is the director of the Adrienne Arsht National Security Resilience Initiative at the Scowcroft Center for Strategy and Security. He previously served as the deputy assistant secretary for Iran and Iraq at the US Department of State's Bureau of Near Eastern Affairs.

6. What is the future of terrorism in Central Asia?

Extremist groups, including Islamic State–Khorasan Province (IS-K), are likely to continue to exploit weak governance and social issues in Afghanistan and Central Asia to conduct external operations in the near future. At present, the largest counterterrorism challenge in the region is the Taliban's inability to deter or prevent terror groups from operating inside Afghanistan.

The Taliban struggles to maintain security and prevent threats within Afghanistan, and it faces significant challenges from both IS-K and the East Turkestan Islamic Movement (ETIM). The ETIM, an al-Qaeda-aligned militant group that aims to establish a caliphate in what it calls Turkestan (an area including Central Asia, Afghanistan, and parts of Western China), claims to defend oppressed Uyghur Muslims. In Afghanistan, the group is distinct from ISIS, though both have targeted Chinese interests in the region

Similarly, IS-K conducts operations within Afghanistan, while simultaneously recruiting young men to travel to and train in ungoverned portions of the country. Many of these individuals come from other Central Asian nations, as IS-K steps up its propaganda and recruitment efforts across the region. Tajikistani IS-K recruits have been implicated in attacks and plots across the globe, including in Europe, the Philippines, and the United States, highlighting the central role they play in IS-K's external operations.

Looking forward, Afghanistan will likely continue to be a permissive environment for terror groups. The Taliban has proven itself incapable of managing emerging terrorism threats in Afghanistan, and other Central Asian states now face a crisis on their borders. Furthermore, IS-K remains poised to exploit the poor economic and social conditions in the region to continue its recruitment campaign. These new recruits are likely to continue to conduct, plot, and inspire attacks across the globe over the near to medium term.

—Morgan Tadych is a nonresident senior fellow with the Scowcroft Middle East Security Initiative at the Atlantic Council's Middle East programs.

7. What is the future of terrorism in Southeast Asia?

A quarter-century after 9/11, Southeast Asia's counterterrorism landscape faces a structural evolution. While traditional violent extremist organizations have been strategically degraded by sustained security pressure, underlying socio-political grievances, archipelagic safe havens, and radical networks remain intact.

Over the next decade, the primary threat to regional stability will not stem from large-scale territorial insurgencies, but from low-resourced, highly ideological nonstate actors leveraging agentic AI to project state-level asymmetric power.

Autonomous AI frameworks—capable of multi-step reasoning, tool use, and task coordination—can lower the organizational barriers facing violent nonstate actors. Unlike static language models, agentic workflows can help small or fragmented cells carry out more sophisticated operations across multiple domains:

- Amplifying and legitimizing grievances: Artificial persona swarms can autonomously generate hyper-localized, multilingual propaganda in

regional dialects, reframing local grievances as existential causes and accelerating radicalization across digital platforms.

- Precision maritime targeting: Multi-agent loops can combine live Automatic Identification System (AIS) ship tracking, satellite feeds, and port schedules to produce real-time targeting packages against commercial vessels.
- Synchronizing strikes across domains: AI orchestration can automate cyber-reconnaissance against port authority infrastructure and locate optimal launch points for commercial first-person-view aerial drones, explosive surface craft, and low-cost submersibles.

Singapore and its littoral partners maintain world-class maritime security through the Malacca Straits Patrols and autonomous defense assets. However, nonstate actors do not need to defeat state militaries to achieve strategic disruption. By exploiting micro blind spots, short reaction windows, and jurisdictional seams in narrow passages such as the Phillips Channel, nonstate actors can use even low-cost harassment strikes to trigger global market volatility, gain global attention, and spike shipping insurance costs.

To preserve a free, open, and secure Indo-Pacific, Washington and its regional allies must shift toward proactive cross-domain deterrence, integrating counter-unmanned systems, point-defense electronic warfare, and AI-driven maritime anomaly detection.

—Colonel Gittipong "Eddie" Paruchabutr, USA (ret.), is a nonresident senior fellow in the Indo-Pacific Security Initiative at the Atlantic Council's Scowcroft Center for Strategy and Security.

8. What is the future of terrorism in the Sahel?

The future of terrorism in the Sahel may be determined as much by what we cannot see as by what we can.

Across Mali, Burkina Faso, and Niger, terrorist organizations are operating across an enormous geographic space where state authority is frequently weak or absent. Jama'at Nusrat al-Islam wal-Muslimin (JNIM), affiliated with al-Qaeda, and the Islamic State in the Greater Sahara are exploiting porous borders, local grievances, illicit economies, and ungoverned territory to move, recruit, generate revenue, and establish influence. Increasingly, they are not simply conducting terrorist attacks. They are functioning as insurgencies, controlling access to territory and economic activity while competing with governments for authority.

The scale is difficult to overstate. The militant Islamist threat now stretches more than 1,200 kilometers across the Sahel, while violence continues to expand southward and westward toward the more densely populated states of coastal West Africa. The Sahel remains the deadliest theater of militant Islamist violence in Africa, accounting for around nearly ten thousand deaths in 2025, or 41 percent of fatalities on the continent linked to militant groups that year.

At the same time that the threat has expanded, US visibility has contracted.

Following the 2023 coup in Niger, the United States suspended counterterrorism operations and ultimately withdrew its forces, completing its departure from Air Base 201 at Agadez in August 2024. The base had supported regional counterterrorism efforts, while the broader US presence in Niger provided an important platform for intelligence, surveillance, and reconnaissance across the region. Its loss did not make the United States blind to the Sahel, but it removed a persistent collection and operational platform positioned inside an enormous and increasingly difficult operating environment.

That combination, expanding terrorist freedom of action and diminishing US visibility, is what makes the future particularly concerning.

There is an uncomfortable parallel to Afghanistan before September 11, 2001. The Sahel is not Afghanistan, and history rarely repeats itself cleanly. But Afghanistan demonstrated what can happen when terrorist organizations are

afforded sanctuary, time, resources, and sufficient freedom from sustained external pressure. The danger was not simply what al-Qaeda was when it arrived. It was what the organization was able to become.

That should frame how US policymakers think about the Sahel today. JNIM and Islamic State elements remain overwhelmingly focused on regional objectives. A local insurgency does not inevitably become a transnational terrorist threat to the United States.

But the problem is precisely that the United States may have a decreasing ability to observe that transition if it occurs.

The future threat from the Sahel, therefore, is not simply terrorism expanding across Africa. It is the possibility that across an increasingly lawless expanse, terrorist organizations have the time and space to evolve faster than our ability to understand what they are becoming.

—Alex Plitsas is a nonresident senior fellow with the Scowcroft Middle East Security Initiative and leads the Initiative's Counterterrorism Project. He previously served as the chief of sensitive activities for special operations and combating terrorism in the Office of the Secretary of Defense.

9. What is the future of terrorism in the Horn of Africa?

Terrorist threats in the Horn of Africa are becoming more interconnected, technologically capable, and global in impact, requiring creative responses that combine political, military, and economic tools. The Islamic State's presence in Somalia illustrates this evolution. Although smaller than al-Shabaab, the Islamic State in Somalia plays a financial facilitation role for the broader Islamic State network, raising and transferring funds that support operations beyond Somalia. Meanwhile, cooperation between al-Shabaab and the Houthis in Yemen is increasing despite their ideological differences. The relationship represents a dangerous marriage of convenience: al-Shabaab can offer financial resources, smuggling networks, and access on the African side of the Gulf of Aden, while the Houthis possess increasingly sophisticated drone, missile, and maritime-warfare capabilities.

The Horn of Africa will not be exempt from intensifying pressure on global maritime chokepoints. Its centrality in the Bab el-Mandeb, Red Sea, and Gulf of Aden means that terrorist and insurgent activity can threaten shipping, ports, energy supplies, and global supply chains. Addressing this danger should not be treated solely as an Iran or Houthi problem. Governments and other actors on both sides of the Red Sea have equal roles in disrupting illicit finance, weapons transfers, smuggling routes, and operational cooperation among militant groups.

Yet military operations alone will not resolve the threat. In many areas, communities have seen few benefits from their governments. Where the state cannot provide security, justice, services, or economic opportunity, residents may tolerate or passively support terrorist organizations, because the consequences of resisting them are greater than anything the government can offer. Without stronger governance and legitimate economic alternatives, this dynamic is likely to continue.

The long-term answer therefore lies in political solutions, supported by economic programs and by sustained counterterrorism pressure. Negotiations with elements of al-Shabaab should not be ruled out, and diplomatic engagement with the Houthis might form part of a wider regional approach. These tracks should proceed in parallel alongside credible military pressure.

The future of counterterrorism in the Horn must consequently be multipronged: political and diplomatic negotiation, economic growth that offers communities viable alternatives, more legitimate and capable governance, coordinated action across both shores of the Red Sea, and targeted military pressure against irreconcilable actors. As we have argued before, Washington must move beyond viewing the Horn principally through a counterterrorism lens. The threat is becoming transregional and the response must become equally integrated.

—Maureen Farrell is a nonresident senior fellow at the Atlantic Council's Scowcroft Center for Strategy and Security and previously served as US deputy assistant secretary of defense for African affairs.
—Rose Keravuori is a nonresident senior fellow at the Atlantic Council's Africa Center and previously served as the director of intelligence at US Africa Command.

10. What is the future of terrorism in South Asia?

At first blush, terrorism's current trajectory in South Asia appears much less troubling than it was in the years leading to 9/11. Legacy groups like al-Qaeda have grown old and weak. Most of the dozen-plus terrorist organizations operating in the Afghanistan-Pakistan region are relatively inactive. Attacks by IS-K, the South Asia affiliate of the Islamic State and one of the few truly potent groups in the region, have come down in recent years.

But it would be a mistake to downplay the continued threat of terrorism in the region. The Taliban—which has alliances with most of the terror groups in the Afghanistan-Pakistan region, from Central Asian jihadists to Pakistani outfits focused on India—has been back in power for five years, with no foreseeable threat to its political survival. This ensures the presence of sanctuaries for terrorist actors, and it creates space for weakened groups—including al-Qaeda—to focus on rebooting. One of the Taliban's most dangerous allies, Tehreek-e-Taliban Pakistan (TTP), is using bases in Afghanistan and Pakistan to carry out attacks in Pakistan. Most TTP attacks have targeted security forces in Pakistan, but more than a decade ago—before Pakistani counterterrorism operations temporarily weakened the group—it carried out waves of attacks on Pakistani civilians and trained a fighter to attempt an attack on New York's Times Square.

The one group with which the Taliban is not allied is IS-K. The Taliban has carried out ground offensives against IS-K that likely account for the reduction in IS-K attacks (and even prompted grudging praise from Biden administration officials). But IS-K is famously resilient, having withstood years of NATO airstrikes and even the "Mother of All Bombs" deployed against its cave sanctuaries in Afghanistan in 2017. Indeed, over the past few years, even while getting hit hard in Afghanistan by the Taliban, IS-K has developed a growing capacity to project a threat beyond South Asia.

The future of terrorism in South Asia is concerning. The region may not be the global hub for international terrorist plots that it was in the past, and the number of attacks may not be as great. But terrorism will continue to be a reality, thanks to potent and resilient groups such as IS-K and TTP, and thanks to the rule of the Taliban, which provides an enabling environment for militant organizations of many stripes.

—Michael Kugelman is a resident senior fellow for South Asia at the Atlantic Council.

11. What is the future of Iran's terrorist proxies in the Middle East?

Should the current Iranian regime remain the country's governing force at the end of the current conflict, expect its proxies—Hamas, Palestinian Islamic Jihad (PIJ), Hezbollah, the Houthis, and the Iraqi Shia militias—to remain core to the regime's strategic goals of survival, forward defense, and asymmetric warfare. This is a likely outcome given that current negotiations do not appear to include any demands for a cessation of Iranian support to its proxy network. The extent to which Iran will continue to fund and provide material support to its proxies will largely depend on economic concessions, cash infusions, and the easing or elimination of sanctions that Iran garners in a final peace settlement.

Moreover, even a diminished Iranian regime will not lead to its proxy network's demise. It will instead force the network into transitional phases of survival and regeneration. Facing no existential threat to its belief structure, the network will continue even with less financial and military support from a weakened Iranian state.

The proxies will also endure sustained pressure on their operations from both internal and external forces that will shape but not eliminate their influence and impact. Hamas and PIJ's ability to pose a significant terrorist threat to Israel has been significantly reduced for now, but Hamas will likely remain a significant ideological and political movement committed to Israel's destruction. Likewise, Hezbollah's recent setbacks are substantial, but it is unlikely to be disarmed. It will continue to influence Lebanese politics and society and destabilize Lebanon's pursuit of a lasting peace treaty with Israel. In addition, the Houthis can be counted on to pursue their political objectives in Yemen. With a reduction in material support from Iran, the group may more frequently try to hold shipping through the Bab el-Mandeb hostage to counter Saudi and Emirati pressure.

Regardless of Iranian support, the Shia militias in Iraq, including the Popular Mobilization Forces and the Islamic Resistance in Iraq—much like Hezbollah in Lebanon—remain fixtures of Iraq's society and polity. At a minimum, these groups' anti-US, anti-Saudi, and anti-Israel positions hinder Iraq's economic growth and the Gulf's stability.

Iran's proxies have a hydra-like ability to regenerate, especially when fed with new funding and materiel. For the foreseeable future, expect them to contribute to instability in the Middle East.

—Joe Zacks is a nonresident senior fellow with the Scowcroft Middle East Security Initiative at the Atlantic Council's Middle East programs. He previously served as deputy assistant director of the Central Intelligence Agency for counterterrorism.

12. What is the future of terrorism in Latin America?

The global security environment is at its most unsettled in decades, and arguably since the end of World War II. With conventional conflicts underway in Eastern Europe and the Middle East, positive global and regional security trends are in short supply.

Yet in Latin America, one long-standing challenge is showing signs of improvement: terrorism. Since the end of the Cold War, the Castro regime in Cuba and the Chavista regime in Venezuela have been particularly pernicious in incubating and even using terrorist proxies against the United States and its partners. With the Cuban regime under sustained pressure from Washington and Hugo Chávez's successor Nicolás Maduro ousted in Caracas, the primary state sponsors of terrorism in Latin America are either deposed or on the run.

Cuba has long supported leftist militants and terrorists across the Western Hemisphere. Havana has also sheltered fugitives from the US legal system. For Havana's actions, the US State Department has designated Cuba as a state sponsor of terrorism. The Trump administration's mounting pressure on the Castro regime is likely to restrict its operating environment for the foreseeable future.

In Venezuela, the removal of the Chavez-Maduro regime deprives Hezbollah of its principal base of Latin American operations. Having executed successful attacks in Argentina during the 1990s and operated in the tri-border area of Brazil, Argentina, and Paraguay, Hezbollah's support from the Venezuelan regime has provided it with staying power. Washington's successful operation against Maduro in January is likely to substantially degrade Hezbollah's capacity for Latin American operations.

Despite the positive momentum of recent months, terrorism in the region will undoubtedly persist, albeit without immediate state hosts and sponsors. Transnational criminal organizations and narcotics traffickers pose a threat more analogous to traditional terrorist organizations in many instances, including in Mexico and Ecuador. These organizations remain exceptionally dangerous in a region often defined by limited state capacity and unstable political institutions. Additionally, as the Trump administration outlined in its 2025 National Security Strategy, such organizations are capable of directly threatening the US homeland while trafficking deadly narcotics across borders.

Overall, however, Latin America has made progress in reducing the threat of terrorism, particularly as Washington has applied pressure on regimes with longstanding records of sponsoring terrorism. To build on this momentum and fortify the region against terrorism-like violence from cartels and other criminal organizations, Washington must deepen security cooperation and training programs with like-minded governments in Latin America. Recent elections that have brought more compatible governments to power across the region open the possibility of a shared security agenda in the hemisphere.

—Alexander B. Gray is a nonresident senior fellow with the GeoStrategy Initiative at the Atlantic Council's Scowcroft Center for Strategy and Security. He previously served as deputy assistant to the president and chief of staff of the White House National Security Council.

13. What is the future of state-sponsored terrorism?

The future of state-sponsored terrorism is likely to feature more covert, deniable support to diverse violent actors, increasingly enabled by technology and shaped by great-power competition rather than by ideologically driven proxy wars alone. Classic patterns, such as states training, arming, and sheltering militant groups, will persist, but sponsorship is already shifting toward more ambiguous arrangements. Analysts note that governments increasingly rely on criminal networks, loosely affiliated operatives, and low-profile proxies instead of clearly branded militias, making attribution harder and complicating legal and diplomatic responses. This trend blurs the line between terrorism, organized crime, and covert action, and it allows states to exploit violence while avoiding formal designation as "state sponsors of terrorism" under US law.

State sponsorship is likely to grow alongside intensifying geopolitical rivalries. Research on terrorism suggests that in regions such as the Middle East, Africa, and Eurasia, states are likely to keep using nonstate violence to pressure adversaries, shape battlefields, and circumvent conventional deterrence. Debates over designating Russia as a state sponsor of terrorism highlight how sponsorship can involve both direct attacks and enabling third parties, from separatist movements to private military companies. At the same time, some governments, such as in the discussions around Syria, may seek removal from terrorism lists without necessarily abandoning clandestine support, underscoring the political nature of designation processes.

AI and cheap commercial drones will amplify the impact of state-backed actors. AI tools can enhance targeting, surveillance, propaganda, and recruitment, while also strengthening states' counterterrorism capabilities by creating a dynamic of mutual escalation. Assessments for 2026 foresee terrorist and proxy actors adopting drones for attacks on critical infrastructure, a pattern that state sponsors can quietly subsidize or enable through training and technology transfer.

Several analyses warn that global intelligence-sharing and counterterrorism cooperation are degrading, even as the threat landscape becomes more fragmented and ideologically diffuse. Without renewed multilateral agreements on what constitutes "state sponsorship," including both active support and permissive environments for financing and recruitment, sanctions and legal tools will remain partial and uneven. The future of state-sponsored terrorism will therefore hinge less on whether states use terror-linked proxies, which seems inevitable, and more on whether international institutions can adapt fast enough to identify, attribute, and impose real costs on these evolving forms of sponsorship.

—Doug Livermore is the national vice president for the Special Operations Association of America, senior vice president for solution engineering at the CenCore Group, and the deputy commander for Special Operations Detachment–Joint Special Operations Command in the North Carolina Army National Guard.

14. What makes narcoterrorism different?

While cartels certainly employ tactics of terror, such as public executions and mass killings, they lack the ideological ambition to unseat political governance structures that often defines terrorism. Whereas ISIS and other terrorist groups sought to eradicate existing governance structures and impose their own, cartels are often driven by profits, which hinge on commercial and logistical networks operated by their national governments.

Despite this general pattern, however, the Trump administration's designation of cartels as foreign terrorist organizations in 2025 was not unfounded. Recent years have seen cartels increasingly tread on the state's legitimacy, both by fomenting lawlessness and by attempting to cultivate the population's support through infrastructure and aid projects. This, coupled with the growing pervasiveness of *narcocultura*, or the veneration of narcoviolence in popular culture, has imbued cartels with a politico-ideological dimension that increasingly warrants treating them as terrorist organizations.

Despite some skepticism of the Trump administration's embrace of narcoterrorism as a conceptual reality, it remains unlikely that subsequent US presidents, regardless of political leanings, will undo the cartel foreign terrorist organization designations. At its height, the cartel-fueled opioid epidemic killed more Americans in a single year than during the entire Vietnam War. Reversing the designations seems like a politically untenable sword to die on.

Ultimately, as I have argued, the United States needs a counter narcoterrorism strategy tailored to the market realities in which cartels operate. While the US has pursued decapitation strategies, history has shown that removing cartel leaders often fragments criminal organizations, increasing violence and allowing smaller successor groups to proliferate because the underlying drug market remains intact. Recent findings further indicate that the Trump administration's strikes on suspected drug boats in the Caribbean and Eastern Pacific have failed to reduce seaborne drug smuggling into the United States.

Instead, Washington should take several steps. It should puncture cartel transport networks by hardening the Southern border. It should weaken cartels by working to cut their access to US firearms. And it should work alongside regional governments to deepen intelligence and law enforcement partnerships. The ultimate blow to narcoterrorism, however, would be to reduce US demand for narcotics—an ambitious but necessary public health objective all Americans should support.

—*Charlotte Bertrand is a program assistant for the GeoStrategy Initiative in the Atlantic Council's Scowcroft Center for Strategy and Security.*

15. What is the future of bioterrorism?

The anthrax events of 2001 began shortly after 9/11, with the first letter containing weaponized, powdered anthrax received on September 18. Over the past two and a half decades, the United States and other countries took steps to address the threat of bioterrorism, but those efforts have waned in recent years. The underlying threat did not go away, and it will not in the future.

Al-Qaeda and ISIS have issued statements encouraging their followers to use biological weapons in acts of terrorism. These and other terrorist organizations will continue to do so. However, as more time goes by, it will become easier to obtain biological material and learn to weaponize it due to the evolution of biological sciences. The technology needed to synthesize and modify organisms or toxins will likely continue to spread throughout the world and enable terrorist organizations to produce what they cannot otherwise obtain. For example, recent field research indicates that Boko Haram and its offshoots are already using AI for attack

planning and weapons troubleshooting, raising concern that such tools could lower the expertise barriers to developing biological weapons.

Russia and North Korea possess active biological weapons programs today. Nation-state sponsorship of bioterrorism will remain an option for these and other countries suspected of possessing biological weapons. Working through proxies could provide states with plausible deniability while giving terrorist organizations access to biological agents or weapons already in their inventories. Uncertainty about the disposition of biological agents and materials associated with Iran's suspected biological weapons program is likely a long-term risk for US and allied warfighters and civilians.

Domestically, ricin events continue throughout the United States. Letters containing ricin have appeared and been sent to government officials, including Obama and Trump. Attempts at and successful execution of bioterrorist events in the United States should be expected for decades to come.

Greater investment in public health security is needed. The United States must remain vigilant both to prevent biological terrorism and to detect and attribute an attack rapidly if prevention fails. In order to do that, the United States and its allies must gather information and data from throughout the world and analyze them to produce both classified and unclassified assessments of bioterrorist threats, as well as vulnerabilities to and consequences from acts of bioterrorism. The central challenges for the next quarter century will be to transform data and information into early warning systems and scientific advances into biodefense, before adversaries can turn those same advances into weapons.

—Asha M. George, DrPH, is the director of the Bipartisan Commission on Biodefense at the Atlantic Council's Scowcroft Center for Strategy and Security.

—John (J.T.) O'Brien is the associate director of research for the Bipartisan Commission on Biodefense at the Atlantic Council's Scowcroft Center for Strategy and Security.

16. What is the future of cyberterrorism?

For twenty-five years, policymakers have warned that terrorists might launch a "cyber 9/11"—remotely crashing an airliner, poisoning a water system, or blacking out a major city. October 7, 2023, was not that attack. It was among the most consequential terrorist attacks of the post-9/11 era, but its effects came from physical reconnaissance, deception, drones, explosives, communications, and armed teams; not an integrated cyber strike. Google's Threat Analysis Group found no evidence that Hamas used cyber operations to tactically support the assault, even though Hamas-linked actors had previously engaged in cyberespionage and information operations.

That distinction clarifies the gap between the cyberterrorism long feared and the cyber-enabled terrorism more likely to emerge. Terrorist organizations have used the internet extensively for propaganda, recruitment, surveillance, fundraising, and coordination, but they have not yet consistently fused offensive cyber operations with complex physical attacks. Many ideologically and politically motivated cyberattacks have been linked to nation-states rather than terrorist organizations. Still, October 7 demonstrates both how much damage a capable organization can cause without cyber integration and how much more disruptive a future attack could become if that remaining seam is closed.

Terrorists may not need to develop elite hacking units to close it. The 2021 Colonial Pipeline ransomware attack offers a useful preview. DarkSide was a criminal enterprise, not a terrorist organization, yet its intrusion caused the operator to take portions of a major fuel pipeline out of service. The capability already existed within a commercialized criminal ecosystem. United Nations research has similarly warned that cybercrime-as-a-service could allow extremist actors to acquire tools and expertise they cannot produce internally.

The next phase of cyberterrorism will therefore be less cinematic and more operational. Attackers could buy stolen credentials to map a facility, disable cameras before an assault, disrupt dispatch systems as bombs detonate, publish responders' personal information, or circulate convincing false evacuation instructions. Cyber tools would not replace firearms, explosives, drones, or insiders. They would make each one more effective.

A cyber 9/11 scenario has not yet come to pass. The more plausible danger is that the next major physical attack begins with a password and that attackers learn to treat surveillance, communications, emergency response, public information, and weapons as parts of one integrated system.

—Stephen Honan is a fellow with the Atlantic Council's Counterterrorism Project, a senior consultant for BVG and Company, and a former explosive ordnance disposal officer for the US Navy.

17. How might terrorist groups adopt emerging unmanned technologies?

This September 11 anniversary reminds us of the grave consequences when leaders fail to anticipate a highly unconventional threat. This generation's "failure of imagination" could be the threat posed by drones. Unmanned systems are the great democratizer of weaponry—incredibly accessible, inexpensive, easy to use, and capable of gaining an advantage over larger conventional forces. Their capabilities are largely limited only by a user's intent and imagination, offering terrorist groups immense opportunities to induce fear and advance their ideological goals. Some terrorists have already begun using unmanned aircraft systems, including in a January 2024 attack by Kataib Hezbollah with a drone in Jordan, which represented the first time US soldiers were killed in a drone strike.

The next target may be the US homeland, offering terrorists opportunities to trigger large-scale violence in crowded venues and symbolic places, deny access and use of critical infrastructure, and terrorize Americans. The future of unmanned systems is being revealed in Russia's war on Ukraine, such as Russia's horrific "human safari" fear campaign. It should serve as a warning that terrorists have access to not just a new toolkit but an entirely new way of pursuing their goals.

The United States has begun to take the right steps on defending against drones, but it has more work to do. Leaders must accelerate actions to achieve broad airspace awareness, improve interagency coordination, train and equip law enforcement, and invest in technology that counters unmanned systems to protect people and critical infrastructure. Crucially, experts must imagine the unimaginable, preparing to counter the new ways that terrorist groups could use drones to devastating effect in the homeland.

—Vice Admiral Peter Gautier (ret.) is a nonresident senior fellow at the Adrienne Arsht National Security Resilience Initiative in the Atlantic Council's Scowcroft Center for Strategy and Security.

—Sydney Sherry is an assistant director with the Adrienne Arsht National Security Resilience Initiative in the Atlantic Council's Scowcroft Center for Strategy and Security.

18. How might terrorist groups target and attack critical infrastructure?

Sixteen sectors of critical infrastructure fuel daily life and economies for billions around the world. They provide water, energy, agriculture, transportation, manufacturing, communications, public health, and emergency and government services. Because these systems are often interconnected and poorly protected, they are vulnerable and strategic targets that terrorists will likely try to attack to create widespread chaos.

Between 1970 and 2015, a study of two thousand terrorist incidents targeting US critical infrastructure noted a decline in annual attack frequency. Yet after 9/11, the public profile and scale of global terrorism grew. Today, attacks on infrastructure

are spiking, disrupting livelihoods, societal resilience and cohesion, and trust in government.
Historically, terrorist groups have deployed conventional methods, such as bombs, missiles, or other explosives to damage physical structures and networks. Yet "gray zone" tactics, like drones and increased cyber capabilities are extending the reach and magnitude of potential disruption.
In July, Iranian-linked cyberhackers attacked thirty water infrastructure plants across twelve US states, halting signal operations, remote-access capabilities, and automated monitoring for water services. Those same attacks shut down a power plant in the UK. In 2023, similar groups linked to Iran's Islamic Revolutionary Guard Corps manipulated data for water and wastewater services. In 2013, they accessed flood control systems of a New York dam and three US financial companies. In the future, terrorists could expand their cyber targeting to exploit systems managing pollution and alter levels of contaminants and chemical treatments.
Weak digital security, like firewalls and default passwords, as well as dated technology used by infrastructure providers, makes remote attacks cheaper and lower risk for malicious actors. The risk of terrorists weaponizing ransomware, GPS spoofing, or AI could make protection even more difficult to develop and implement at scale. But it isn't all cyber. Another avenue may mean carrying out less-sophisticated attacks that do not require advanced equipment. In 2013, for example, Egyptian authorities arrested three divers who used underwater explosives to cut shallow telecommunications cables in the Mediterranean. Recently, too, the Houthis revealed a map of subsea cables in Middle Eastern waters on a Telegram channel, in what was widely seen as a threat.
Attacks on the input or output networks of critical infrastructure pose even more opportunities for terrorist groups to exploit. Terrorists might, for example, adapt pollution tactics such as pumping oil into bodies of water. When Iraqi forces did this during the Gulf War in 1991, they contaminated seawater and shut down desalination plants critical for supplying drinking water in Kuwait.
The ability to easily, indirectly, and remotely sabotage critical infrastructure, frequently without official condemnation or retaliation, allows terrorist groups and other state and nonstate actors to seed instability and wield geopolitical influence. A terrorist attack on one system will certainly have consequential spillover for resiliency and recovery efforts. As the US government retracts support for the Cybersecurity and Infrastructure Security Agency, critical infrastructure must become a more serious national security priority backed by more protection measures and investment.
—Ginger Matchett is an assistant director with the GeoStrategy Initiative in the Atlantic Council's Scowcroft Center for Strategy and Security.

19. How might terrorists use artificial intelligence?

Twenty-five years ago, aspiring terrorists seeking specialized training often needed direct access to knowledge networks, camps, and equipment. Today, they can turn to a large language model to achieve unimaginable results.
Terror groups today still seek to inflict damage and create shock at scale, but the AI age makes access much easier. Former Boko Haram members have described militants using AI to troubleshoot equipment, assess battlefield problems, and brainstorm attack options. Former members also described dedicated AI teams and internal training, suggesting that AI use is becoming embedded in organizational routines rather than remaining isolated experimentation. But what happens as those capabilities and sustained investments become more powerful? This question should concern counterterrorism officials and publics alike.
AI is already reshaping the terrorist threat landscape by making a familiar playbook easier, cheaper, and faster to execute. Propaganda and recruitment are obvious starting points. ISIS-linked networks have used AI to translate propaganda into multiple languages and to create AI-generated media that amplifies the group's messaging. Generative and agentic

AI could allow terrorist groups to tailor content to vulnerable audiences and produce radicalizing material at unprecedented scale.

More concerning possibilities may still lie ahead. Terrorist groups have long sought chemical, biological, and other malicious capabilities. Advanced AI models may help terrorists synthesize scientific information and identify gaps in their technical knowledge thus lowering barriers to an attack. In the biological domain, AI developers are already testing whether models could assist non-experts with weaponizing biological agents. AI will not remove every practical barrier to an attack, but it can help users work through technical problems.

AI systems are already directing experiments through remotely operated, automated laboratories. These developments could lower some hands-on skill requirements, making access controls and safeguards at the laboratory level increasingly important but also difficult to control across academic, industrial, and government contexts. Safeguards do exist. AI developers use a variety of tools to prevent models from aiding terrorism or other dangerous activities. But defenses are not impermeable. Researchers continue to identify "jailbreaks" that circumvent safeguards. The challenge becomes greater with open-weight models, which can be downloaded and used outside the monitoring and controls of their original developers. Governments and industry face a moving target where safety measures must evolve alongside both increasingly capable models and malicious users.

AI does not need to reinvent terrorism to make it more dangerous, but policymakers should not assume its effects will remain incremental as capabilities advance. The next lone actor could be radicalized by AI-generated propaganda, interact with automated extremist personas, and turn to AI when technical problems arise. If that individual is using a downloadable model outside a provider's monitoring systems, those interactions may be far harder to detect. AI will not erase every barrier to an attack, but it could lower enough of them to matter. Governments will struggle to keep up with the rapid adaptability of terror groups, and more specialized expertise and legal structures are needed now for intelligence, counterterrorism, and law enforcement agencies to create credible preventative capabilities.

—Tressa Guenov is the senior director for programs and operations and a senior fellow at the Atlantic Council's Scowcroft Center for Strategy and Security.

—Bailey Galicia is assistant director for strategy and operations with the Atlantic Council's Scowcroft Center for Strategy and Security.

20. How is cryptocurrency changing terrorist financing?

Cryptocurrency is not the primary engine of terrorist financing, but it is a useful lens through which to understand how the threat has evolved since 9/11. While cash, state sponsorship, and informal networks remain dominant, cryptocurrency is part of a broader technological shift that allows funds, communications, and operations to bypass the institutions that counterterrorism efforts are designed to monitor.

The September 11 attacks reportedly cost their plotters around half a million dollars to reap trillions in economic consequences through direct losses, war expenditures, and the architecture built in their aftermath. That asymmetry frames the enduring logic of countering terrorist financing: sanctions, financial reporting, and targeted action against key intermediaries impose real costs on terrorist networks. Those networks have evolved in response, as has the challenge.

The 9/11 Commission outlined a hybrid financial architecture mixing formal and informal channels, including donor networks, charitable fronts, hawala, and bank accounts mundane enough to disappear into legitimate flows. The post–9/11 regime was built around the obligated intermediaries and human facilitators those channels required.

Two mutually reinforcing catalysts reshaped what followed. Sustained counterterrorism pressure helped push networks toward decentralization, from al-Qaeda's hierarchy to ISIS's territorial model and toward the increasingly autonomous structures of IS-K. Technology expanded what decentralized structures could achieve, building on pre-existing informal shadow economies that made distributed operations formidable.

Financing adapted across the full spectrum. Crowdfunding made small-value global giving easier to aggregate, exploited through humanitarian fronts by ISIS, al-Qaeda, and Palestinian groups well before cryptocurrency existed. Encrypted messaging became infrastructure for propaganda, recruitment, and coordination, extending the functional logic of hawala into digital channels that cross jurisdictions without accountable intermediaries. Mobile money with limited verification has also been used to launder money across Africa, the Middle East, and Southeast Asia. Generative AI now lowers the human cost of propaganda, recruitment, and fundraising at scale.

Cryptocurrency fits this pattern because some architectures shift financial activity away from the accountable intermediaries on which the post–9/11 regime depends, distributing across protocols and node operators rather than custodial institutions. While cash and state sponsorship remain dominant, digital assets supplement terrorism financing efforts. Hamas and PIJ shifted toward dollar-pegged stablecoins after enforcement disrupted earlier wallet infrastructure; IS-K began publicly soliciting Monero, a privacy-focused cryptocurrency designed to obscure transaction flows.

Blockchain analytics and the US Treasury's Office of Foreign Assets Control designation authority have disrupted real networks. But privacy coins, cross-chain bridges, and DeFi protocols can remove the intermediation points on which existing obligations depend—a problem that is compounded by persistent gaps in global implementation of virtual asset standards.

Twenty-five years on, the post-9/11 financial coercion regime faces a problem of rapid technological innovation at almost zero margin cost. Effective deterrence will depend on whether governance and enforcement adapt to reach infrastructure designed to disperse, obscure, and relocate the obligations on which that regime depends.

—Carole House is a nonresident senior fellow at the Atlantic Council GeoEconomics Center.

21. Where are the greatest risks of climate change fueling terror threats?

The linkages between climate change and terrorism are complex, multifaceted, and indirect. But they can be boiled down to a basic proposition, which is that a changing climate can deepen the ecological, social, and political stresses in which terrorism takes root and grows. Extremist groups, which use terror as a central tactic, can more easily establish themselves in places suffering from climate-driven degradation—sustained drought, say—than elsewhere. This is most true in countries with poor or absent governance, where reduced freshwater supplies, extreme heat, and dry soils undermine state capacity, helping to turn weak states into fragile ones, and fragile states into collapsed ones. The effects can spin outward from there, affecting entire regions and even beyond.

The sequence from climate change to terror-driven collapse is far from guaranteed. Rather, climate change makes instability, insecurity, and violence, including terrorism, more likely, because it deteriorates the background conditions in which stable societies function. For example, a 2024 study of farmers and pastoralists in the Sahel by the Institute for Security Studies, a South Africa–based think tank, found that climate change has driven "natural resource scarcity" in the region, contributing to localized conflict, including the emergence of armed militias, "against the backdrop of weakening conflict management by both traditional and state systems." Climate change, in other words, makes the other hard problems facing such fragile regions even harder to solve.

"Climate security" refers to the field that examines this nexus. Although its origins date to at least the 1970s if not earlier, the 9/11 attacks underscored how terrorism can take hold in poorly governed settings and spread its violent tentacles outward. Over the next decade, climate security practitioners sharpened their arguments,

formulating such ideas as the "threat multiplier" concept, which describes climate change as compounding existing sources of instability in already volatile regions.
This problem will not go away anytime soon. Why? Since 9/11, the Earth has continued to warm. It is hotter now than it was in 2001 and getting hotter nearly every year. More heat, and therefore more drought, flooding, and other resource problems, should worry everyone concerned about terrorism.
—Peter Engelke is a senior fellow with the Atlantic Council's Scowcroft Center for Strategy and Security and the Global Energy Center.

22. Is the US prepared to counter future terrorist threats?

Is the US highly capable now on counterterrorism? Yes. Should Americans worry that the US is not doing enough? Yes, as well.
The US government remains the gold standard globally in the counterterrorism framework model to "detect, deny, and disrupt" the ability of terrorist groups to attack Americans. The US counterterrorism ecosystem includes the timely integration and synchronization of the intelligence community, law enforcement, and military—all highly specialized entities with skills honed across two decades of fighting the global war on terrorism. The intelligence community maintains a global reach, with human intelligence and signals intelligence gathering capabilities that are second to none. Counterterrorism operations are also a team sport: the United States maintains robust global intelligence liaison relationships that may be among the only areas untouched by political controversies. The Federal Bureau of Investigation's Joint Terrorism Task Forces (JTTFs) around the United States allow for interagency cooperation within US borders. The Special Operations Command maintains specialized units that are battle tested. Moreover, US border and aviation security apparatuses have also proved resilient in protecting the homeland.
That said, the counterterrorism community is akin to a soccer goalie—it can be very good at times, but goals do get by. In fact, lone-wolf attacks are extremely difficult to combat, as often there is no cell for a JTTF to penetrate, complex communications for the intelligence community to intercept, or actual terrorist groups for special operations forces to take down in a raid. Complex attacks like 9/11 may not be the norm any longer, but radicalized individuals can still cause great harm. Domestic extremism is a growing (and politically toxic) issue as well—one that law enforcement may be reluctant to tackle based on the political winds of the day. And terrorists' use of technology has evolved, with encrypted communications now prevalent across the terrorist spectrum. One can only imagine how problematic the weaponization of small, inexpensive drones within US borders would be, if such a terrorist plot materialized and matured.
Finally, given the operational successes of the US counterterrorism community since 9/11 and the renewed rise of great power competition, there are fewer resources, including funding and personnel, for counterterrorism efforts than during the Global War on Terror. Counterterrorism is playing second fiddle to threats from China and Russia, for example, and the current administration's focus on the border and narcotrafficking is also shifting resources to the Americas.
There also seems to be less of an inclination to "defend forward," meaning a diminished US footprint in terrorist hotspots in South Asia and Africa, where ISIS activity is rising. A reduced official US footprint means fewer US intelligence and special operations boots on the ground. Flying blind is never a comforting thought for counterterrorism professionals.
Counterterrorism is often not seen as important until it really is. Think of the Bush administration in the run-up to 9/11. It too often takes a catastrophic event for the US political establishment to recognize that the country cannot take its foot off the gas.

—Marc Polymeropoulos is a member of the Scowcroft Middle East Security Initiative's Counterterrorism Project. He previously served for twenty-six years at the Central Intelligence Agency.

23. What does an allied strategy for counterterrorism look like?

An effective counterterrorism strategy is built on partnerships, shared intelligence, and coordinated action. Collaboration with allies and nontraditional partners has been one of the great strengths and pillars of America's post-9/11 counterterrorism strategy. Nations find combating terrorism compatible with their domestic and foreign policies, and counterterrorism partnerships serve as a force multiplier. Effective counterterrorism partnerships require governments to commit to their partners' security nearly as part of their own. In its 2026 Counterterrorism Strategy, the Trump administration continues to prioritize counterterrorism partnership, albeit more transactionally than previous presidential strategies, which focused on collective leadership. Although today it may be "America First," it is not "America Alone."

The goal of any allied counterterrorism strategy is to prevent terrorist attacks, and its foundation is the identification and disruption of terrorist threats. Success depends on relationships built on trust and shared purpose. It must involve at least bilateral if not multilateral cooperation across intelligence, diplomacy, and finance. It cannot rely solely, however, on cooperation among intelligence services. All relevant instruments of national power must play an active role in defining and implementing counterterrorism strategies. Timely information sharing and collective action are essential to disrupting terrorist plots from every angle. For less capable countries, partners with advanced tools and abilities should provide training, materiel, and financial support.

The US-sponsored Global Coalition to Defeat ISIS, established in 2014 and now comprising eighty-seven members, along with its Counter-ISIS Finance Group, is a prime example of the value of multilateral efforts to tackle global terrorism capabilities and threats. The Global Counterterrorism Forum and the Financial Action Task Force are other examples of multilateral approaches to counterterrorism doctrine and financial enforcement.

In the future, terrorism emanating from inspired individuals, lone-wolf actors, and violent domestic extremist groups is likely to rise. Many countries may shy away from multilateral solutions to homegrown problems. Nevertheless, collective efforts will remain essential, especially as they relate to governing social media and cryptocurrency platforms that enable terrorist, nihilist, and anarchist activity to propagate.

A counterterrorism strategy heavily dependent on alliances and partnerships has served the United States and the world well for the twenty-five years since 9/11. It will continue to do so, even as the nature of terrorism evolves.

—Joe Zacks is a nonresident senior fellow with the Scowcroft Middle East Security Initiative at the Atlantic Council's Middle East programs.

24. What should an effective domestic counterterror strategy to defend the homeland look like?

It would match intelligence, cyber, political, and law enforcement resources to the most serious threats. Twenty-five years after 9/11, the threats from al-Qaeda and ISIS and their respective franchises and affiliates have diminished but not ended. However, the threat from Iranian state-sponsored terrorism has increased. Cyberattacks against US water infrastructure and threats against Iranian dissidents and Trump administration officials represent the most serious terrorist threat against the US homeland. Even if the most recent Iranian plot to shoot down Trump's plane was thinly sourced, Iranian officials' thirst for revenge for

the killing of Supreme Leader Ali Khamenei is not going away. Even a ceasefire is unlikely to end Iranian plots against Trump and the homeland.

Serious state-sponsored terrorist threats against the United States are an entirely different order of magnitude from what the United States has faced since 9/11. The annual budget for al-Qaeda at its peak, around $30 million a year, was a fraction of the $700 million to $1 billion or more that Iran spends every year to support Lebanese Hezbollah. The United States has not faced a determined state-sponsored terrorist threat like the one Iran poses today in decades, if ever.

The Trump administration's 2026 counterterrorism strategy acknowledges that "the greatest threat to the United States emanating from the Middle East comes specifically from Iran." The strategy also states that the United States will "continue to focus our kinetic, intelligence, and cyber operations against Iranian-backed terror proxies who plot against Americans, and we will take decisive action against regime actors who plot attacks against Americans in the homeland, as well as Iranian dissidents and Israelis in our country." Other administrations had essentially the same policy.

However, the loss of a thousand employees at the Cybersecurity and Infrastructure Security Agency since January 2025 raises questions about matching the policy with resources. The Trump administration is also in a bind of its own making, trying to justify increased security spending after starting a war of choice using tactics that significantly increased the terrorist threat against the homeland. Perhaps most troubling is the administration's apparent unwillingness to compromise with congressional Democrats to reallocate or increase funding to protect against Iranian terrorism. The administration needs to work with appropriators of both parties, not just Republicans, to make sure the United States has the resources and personnel to address today's greatest terrorist threat.

—Thomas S. Warrick is a nonresident senior fellow with the Adrienne Arsht National Security Resilience Initiative in the Scowcroft Center for Strategy and Security and the Scowcroft Middle East Security Initiative in the Middle East programs at the Atlantic Council.

25. How does China approach global terrorism?

In the immediate aftermath of 9/11, the United States praised China for its close cooperation on counterterrorism issues, with the topic even helping to stabilize the relationship. But by 2005, Washington was raising concerns about how sincere China's efforts were. In the years since, Beijing has focused on terrorism as a domestic threat, but as it seeks to expand its global footprint, it will increasingly face the threat of transnational terrorism.

Beijing has long worried that members of the Uyghur ethnic group hold extremist ideas that present a threat to the Chinese Communist Party (CCP). It has labeled the East Turkestan Islamic Movement, a militant separatist group founded by Uyghurs, as a terrorist group (though the United States removed the group from its list of terrorist organizations in 2020), and views it as part of a growing terrorism threat facing China. Part of this concern has also been driven by a worry that terrorist groups operating abroad would spread into Xinjiang province. Some Uyghurs have fought alongside militant organizations in Southeast Asia and the Middle East, but experts doubt that Uyghur militancy in Xinjiang is imminent or even possible. In response, China has carried out a campaign of arbitrary detention against the Uyghur population, which the United States has labeled a "genocide."

The CCP views terrorism as posing a significant threat to Beijing's ability to achieve its interests and maintain internal security. Now, as China has expanded its global presence, it must also contend with terrorism abroad.

Beijing's flagship Belt and Road Initiative, an infrastructure and development strategy, extends across many countries that face active terrorism threats. In Afghanistan, the Islamic State – Khorasan Province has targeted China in its

propaganda and has threatened Belt and Road projects in the country. Next door, in Pakistan, the Balochistan Liberation Army attacked China's consulate in Karachi in 2018, and in 2021, the TTP organized an attack on the hotel housing China's ambassador to Pakistan. Since 2021, terrorist attacks have killed at least nineteen Chinese nationals in Pakistan.

China's hostility toward its Uyghur population has also caught the attention of terrorist groups, with the leader of al-Qaeda in the Arabian Peninsula saying that China's treatment of Uyghur Muslims justified future attacks. Earlier this year in Kabul, an IS-K bombing killed seven people at a Chinese restaurant, with the group pointing to China's treatment of Uyghurs as justification.

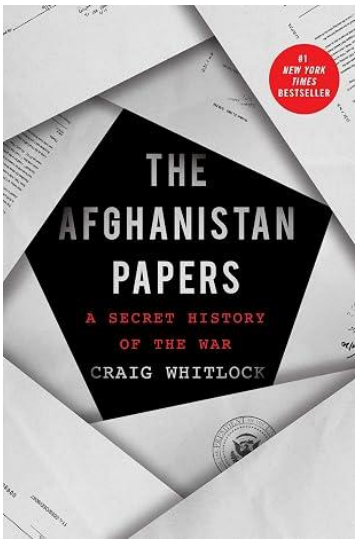
These kinds of attacks are likely to continue as China maintains a visible global footprint. Chinese nationals, infrastructure investments, and diplomatic missions will remain targets.

—Imran Bayoumi is a deputy director and resident fellow with the GeoStrategy Initiative in the Atlantic Council's Scowcroft Center for Strategy and Security.

The Afghanistan Papers: A Secret History of the War

By Craig Whitlock (Author), **The Washington Post** (Author)
Source: https://www.amazon.co.uk/dp/1982159006

The groundbreaking investigative story of how three successive presidents and their military commanders deceived the public year after year about America's longest war, foreshadowing the Taliban's recapture of Afghanistan, by Washington Post reporter and three-time Pulitzer Prize finalist Craig Whitlock. Unlike the wars in Vietnam and Iraq, the US invasion of Afghanistan in 2001 had near-unanimous public support. At first, the goals were straightforward and clear: to defeat al-Qaeda and prevent a repeat of 9/11. Yet soon after the United States and its allies removed the Taliban from power, the mission veered off course and US officials lost sight of their original objectives.



Distracted by the war in Iraq, the US military became mired in an unwinnable guerrilla conflict in a country it did not understand. But no president wanted to admit failure, especially in a war that began as a just cause. Instead, the Bush, Obama, and Trump administrations sent more and more troops to Afghanistan and repeatedly said they were making progress, even though they knew there was no realistic prospect for an outright victory. Just as the Pentagon Papers changed the public's understanding of Vietnam, The Afghanistan Papers contains startling revelation after revelation from people who played a direct role in the war, from leaders in the White House and the Pentagon to soldiers and aid workers on the front lines. In unvarnished language, they admit that the US government's strategies were a mess, that the nation-building project was a colossal failure, and that drugs and corruption gained a stranglehold over their allies in the Afghan government. All told, the account is based on interviews with more than 1,000 people who knew that the US government was presenting a distorted, and sometimes entirely fabricated, version of the facts on the ground.

Documents unearthed by The Washington Post reveal that President Bush didn't know the name of his Afghanistan war commander—and didn't want to make time to meet with him. Secretary of Defense Donald Rumsfeld admitted he had "no visibility into who the bad guys are." His successor, Robert Gates, said: "We didn't know jack shit about al-Qaeda." The Afghanistan Papers is a shocking account that will supercharge a long overdue reckoning over what went wrong and forever change the way the conflict is remembered.

People have the leaders they deserve . . .

AOC and Mamdani were seen laughing together as the names of 9/11 victims were read at Ground Zero.

I Was Surprised 9/11 Wasn't Vastly Worse

By Tom Cantlon

Source: https://www.dcreport.org/2026/09/11/9-11-bioterrorism-threat/

It Still Might Be

Sep 11 – When I first heard that Middle-Eastern terrorists had flown jets into the New York Twin Towers causing them to collapse my first reaction was relief. Of course this was a horrible thing to have happened, but I had been anticipating much worse. When the attack made clear that the worst they could accomplish was to fly planes into a few buildings killing a few thousand people, that seemed tiny compared to the hundreds of thousands of deaths I had feared could happen. The three thousand deaths we suffered that day were bad enough. A different kind of attack could have been much worse. Being someone who has always enjoyed following science news I had long been aware that scientists were able to genetically modify organisms. That potentially included the ability to modify pathogens to be more deadly or more unstoppable than they naturally are. This seemed like just the kind of technology terrorists would jump on. I'm not sure when I became aware of this, probably in the 1980s in some science news about the wonderful potential for creating cures for diseases. The science of it goes back to 1971 when a scientist, Paul Berg, at a university spliced DNA from one virus into another virus making it a new and different, and potentially worse, virus. This was the start of recombinant DNA technology.

It is now remembered as a breakthrough and Berg later received a Nobel prize. But at the time he didn't tell anyone about this for a while. When eventually another scientist in New York who studies viruses, Robert Pollack, learned of it he was immediately appalled at the danger of such work. So the fact that the technology existed,

and that knowledgeable people knew how horribly dangerous it could be, was known back then. In fact how to deal with the technology in a safe way was such a hotly debated issue that they had a conference in 1975 on how to set safety standards. It was attended by most of the great minds of the time on the topic, and was a publicly reported event. That terrorists might try to use pathogens to do great harm was known even further back. There was an attempt to put Typhoid into a water supply in 1972. In the following decades there were various attempts in the U.S. and Japan to attack the public with anthrax, botulism, salmonella, and bubonic plague. So the general method was known, and this new potentially devastating technology was known. The whole technical field is wonderful. It has of course advanced in enormous ways since then. The odds are good that you or someone you know has had significant health benefits, directly or indirectly, from all the health science that has developed from that start. But that's with scientists carefully attempting to make specific useful advances. My fear at that time was that some terrorist group with money would find some smart but sick terrorist/biochemistry student, buy supplies for a lab, and let them hack away at it. A terrorist just trying to kill people wouldn't care which virus they modify, or how it becomes more deadly or harder to stop. They could pretty much just experiment away almost randomly and see what results they get. Stumble upon something that's deadly and that spreads quickly and is hard to stop, release it in New York and Los Angeles, and there would be an attack many times worse than what we had.

With the news of the planes being flown into buildings it was immediately clear that the terrorists focused on us were not up to that kind of attack. That was an immediate and enormous relief. A terrible thing had happened, but not nearly as bad as it could have been.

Technology has of course greatly advanced. Editing the genes of viruses is much easier, and AI can be used to try to predict exactly which changes would make a virus deadlier, quicker to spread, and harder to stop. That worse level of anxiety is back.

We can try to stop plots before they happen but that's risky and better if we can be more proactive.

We can try to be ready for surprise outbreaks, if we fund such research. One of the best things we can do is try to make the world more peaceful and more cooperatively interdependent. With fewer impoverished or abused groups, particularly lessening or helping whole groups who become refugees into their neighboring countries because of war, or drought or other disasters of nature.

Hmm. Doesn't seem like that's the direction we're going on any of that. Maybe we need a change.

Tom Cantlon is an author and business owner. For most of 20 years he has provided the leftward view in columns for a right leaning daily paper in a right leaning area.

Al-Qaeda regroups in Afghanistan, 25 years after 9/11

By Greg Miller

Source: https://www.washingtonpost.com/world/2026/09/12/25-years-after-911-al-qaeda-regroups-afghanistan/

Sep 12 – Al-Qaeda's plans for the Sept. 11, 2001, attacks took root in dusty, mud-walled compounds in Afghanistan that served for years as terrorist training camps.

A quarter-century later — despite decades of U.S. military and counterterrorism operations aimed at

eradicating those strongholds — al-Qaeda is again operating training camps in Afghanistan, according to U.S. and Western intelligence officials and a United Nations organization responsible for monitoring terror networks.

The terror organization and its offshoots have set up at least eight training sites over the past three years, taking advantage of the Taliban's return to power in Kabul and the security void created by the 2021 U.S. military withdrawal, according to U.N. reports and security officials.

Other terror groups, including an affiliate of the Islamic State, al-Qaeda's main rival, also have set up new training sites, officials said, giving militant Islamist groups a foothold in at least 14 of Afghanistan's 34 provinces.

These officials and others in this article spoke on the condition of anonymity to discuss intelligence matters.

Because the Taliban has again provided "a permissive environment," a U.N. report said, al-Qaeda has been able "to consolidate, with the presence of safe houses and training camps across Afghanistan."

There are notable differences from the pre-9/11 period, officials and counterterrorism experts said.

The groups now training in Afghanistan seem more focused on regional fights than mounting elaborate plots against the United States or its allies. They appear to be constrained by Taliban hosts wary of again drawing the wrath of global powers. And with al-Qaeda's top leaders still believed to be hiding in Iran or elsewhere, no Osama bin Laden-like figure has emerged to galvanize followers.

Even so, the reappearance of training camps is a cause of growing concern.

"They're not following the pre-9/11 game plan of going after the far enemy," said Bruce Hoffman, a counterterrorism expert at Georgetown University. "But I think they hope that with local and regional gains they can start to rebuild momentum. They haven't forgotten us."

The U.S.'s failure to dismantle al-Qaeda's training camps in the 1990s still looms as one of the major missed opportunities to prevent the Sept. 11 attacks.Ask The Post AIDive deeper

The idea of flying hijacked planes into U.S. buildings was first proposed by 9/11 mastermind Khalid Sheikh Mohammed in 1996 at an al-Qaeda complex in Tora Bora, Afghanistan, according to the U.S.'s 9/11 Commission.

Bin Laden later approved the operation at a site near Kandahar. Before storming the cockpits of four transatlantic flights, all 19 of the hijackers had spent time at al-Qaeda camps or safe houses in Afghanistan.

U.N. and other security officials said they had recently investigated claims that al-Qaeda was seeking to re-establish a presence at Tarnak Farms, a sprawling compound near the Kandahar airport where one of the first CIA Predator drone surveillance flights caught a pre-9/11 glimpse of bin Laden. A Washington Post examination of satellite imagery found no visible sign of resumed activity at Tarnak.

The new camps are being used to train fighters on weapons, explosives and guerrilla tactics that would be familiar to the thousands of recruits who passed through al-Qaeda's camps in the 1990s, officials said. But they also cited indications of instruction on the use of encryption, artificial intelligence, drones and other technologies that were in their infancy in 2001.

The number of militants in Afghanistan considered part of core al-Qaeda, the parent group that spawned affiliates and imitators, is probably 100 or fewer, said Colin Smith, coordinator of a U.N. monitoring team that tracks the threat posed by terror groups and oversees international sanctions on them.

Instead of spearheading operations, "we've seen al-Qaeda acting as a consulting service for other groups," Smith said. "Giving them advice and training on things like covert operations and information security."

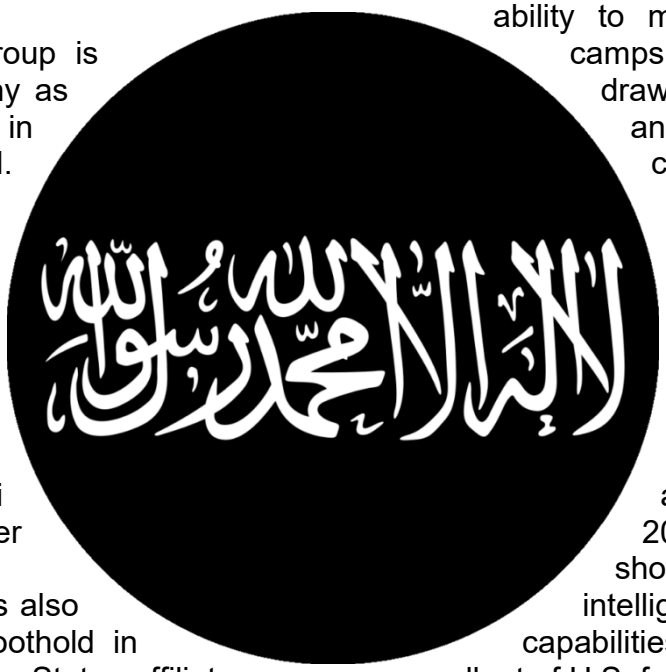
The arrangement has put core al-Qaeda in a supporting role to larger affiliates including Tehrik-e-Taliban

Pakistan, or TTP, a group that seeks to overthrow

the government in Pakistan and establish an Islamic state.

A U.N. report in 2024 said that al-Qaeda operatives in Afghanistan's Kunar province were "conducting suicide bomber training for TTP."

The Pakistan-focused group is believed to have as many as 7,000 fighters in Afghanistan, Smith said. U.N. reports said that TTP had established camps in at least four Afghan provinces "with al-Qaeda and Taliban involvement," and that the group has carried out hundreds of cross-border attacks on Pakistani military outposts and other targets.



Al-Qaeda's main rival has also worked to establish a foothold in Afghanistan. An Islamic State affiliate known as Islamic State-Khorasan, for the historical region of Khorasan, has attracted about 2,000 recruits and used northern Afghanistan as its "main hub" for training and planning operations across Central Asia, according to officials and U.N. reports.

Al-Qaeda and the Islamic State remain fierce rivals, fighting for dominance of the jihadist movement and overseeing splinter groups that compete with one another, officials said.

Both groups seem focused mainly on recruiting operatives from within Afghanistan or neighboring states, unlike in the 1990s when al-Qaeda attracted thousands of foreign fighters from Saudi Arabia — where 15 of the 19 9/11 hijackers were from — and other Middle Eastern countries.

"What I've seen from al-Qaeda media suggest that they're not really looking for foreign fighters right now," said Sara Harmouch, a terrorism expert at George Washington University who tracks the group's propaganda and social media messages. "They don't want eyes on them as they try to rebuild these capabilities."

U.S. and other security officials said that their ability to monitor the new training camps has been hampered by a drawdown in CIA personnel and other U.S. intelligence capabilities that accompanied the 2021 military withdrawal. The U.S. has since shifted resources to the war in Iran and other priorities.

Even so, the killing of Ayman al-Zawahiri, who succeeded bin Laden as al-Qaeda's leader, in a 2022 drone strike in Kabul showed that the U.S. has intelligence and strike capabilities that survived the chaotic pullout of U.S. forces.

Al-Qaeda is now led by Saif al-Adel, an Egyptian, who spent years helping to run training camps in Afghanistan after his 1988 arrival. But al-Adel is believed to remain in hiding in Iran, officials said, underscoring the organization's concern about security in its former stronghold.Ask The Post AIDive deeper Terror watch lists, travel surveillance and other security measures adopted after 9/11 would likely put any visitor to Afghanistan's training camps under intense scrutiny, officials said. Instead, al-Qaeda and the Islamic State have sought to recruit operatives online and urged sympathizers in Western countries to stay in place for "lone wolf" operations.

Many of these plots have been disrupted. In a recent case, a 35-year-old woman in Albany, New York, was arrested last month and charged by the Justice Department with pursing an "ISIS-inspired" terror plot to bomb the state capitol.

Greg Miller is an investigative foreign correspondent based in London for The Washington Post and a two-time winner of the Pulitzer Prize. He is the author

of "The Apprentice," a book on Russia's interference in the 2016 U.S. presidential race and the fallout under the Trump administration.

National Security Agency launches historic restructuring

By Zach Dorfman, Warren P. Strobel and Noah Robertson
Source: https://www.washingtonpost.com/national-security/2026/09/13/national-security-agency-launches-historic-restructuring/

Sep 13 – **The National Security Agency is set to undergo its most extensive internal restructuring in at least a decade, according to current and former officials briefed on the emerging plan.**

The new design for one of the most powerful U.S. intelligence agencies, which was announced to senior NSA leaders last week, is the brainchild of Army Gen. Joshua M. Rudd, the NSA director, these officials said.

Rudd's initiative calls for the creation at NSA's Fort Meade, Maryland, headquarters of five new organizations inside the agency, in artificial intelligence, China, cybersecurity, combat support or warfighting, and global intelligence. Each will be led by a newly elevated "mission director," according to former officials.

This new organizational configuration will better reflect NSA's current and future priorities, Rudd believes, according to current and former officials. NSA, the U.S. intelligence community's premier global eavesdropping arm, specializes in digital espionage.

The mission heads will have the "effective" authorities of an NSA deputy director, according to one former official familiar with the plan. This former official, like others in this article, spoke on the condition of anonymity to discuss sensitive information about the agency, whose operations are highly classified. The NSA did not respond to a request for comment.

It was not immediately clear if the five new organizations will replace existing divisions within NSA or be superimposed atop the agency's existing structure. The NSA is believed to employ more than 30,000 people, both military and civilian, and has a larger workforce than the CIA.

Rudd told senior NSA officials that the heads of the five new mission centers might be selected from outside the agency, unnerving NSA insiders, according to the former officials.

"They are begging people to come back, especially leaders," said the first former official, referring to NSA personnel who have left.

A second former official said Rudd is considering candidates for the new mission director posts. It is unclear whether any have been chosen yet.

The elite hacking unit known as Tailored Access Operations (TAO), reconstituted in recent months by Rudd, will fall under the purview of the mission director for global intelligence, according to a current and former official.

The TAO is set to receive a significant budget increase in the new federal fiscal year, which begins Oct. 1, the second former official said.

Founded in 1997, TAO is among the most secretive parts of the NSA, devoted to compromising — and sometimes attacking — the hardest-to-reach digital targets worldwide. The unit name was retired in 2016, and its members spread across different NSA components. Rudd, who was confirmed in March, is both director of the NSA and head of U.S. Cyber Command, one of the Pentagon's combatant commands. In his dual-hatted role, he reports to both Defense Secretary Pete Hegseth and Director of National Intelligence Jay Clayton. Before assuming the NSA directorship, Rudd's military career mostly

focused on special operations.
The NSA, generally believed to be the biggest and most-well-funded arm of the U.S. intelligence apparatus, focuses on the large-scale collection of signals intelligence, including communications and other electronic information. It also manages and secures U.S. encryption systems to prevent foreign actors from penetrating sensitive coded U.S. government communications and networks.
The timeline for the NSA restructuring is aggressive. The new mission directors will be expected to provide Rudd their organizational redesigns by the end of the month, according to a former official. Rollout is expected in mid-October, with the target for "full operating capacity" slated for mid-January 2027, said a current and former official.
Rudd "admitted that they don't know how they are going to do it, so they are going to rush into reversible decisions, in case it is wrong," said the first former official. NSA personnel are still unclear whether the new mission directors will merely be grafted atop preexisting bureaucracy or will oversee more fundamental structural shifts inside Fort Meade.
Since becoming NSA director in March, Rudd has been focused on AI-related advancements, according to former officials. The NSA has rolled out a new desktop AI tool called "Ask Mary," purportedly named for the head of the division leading the agency's AI-related integration efforts. The agency has been keenly interested in working with commercial AI labs, even circumventing a Pentagon ban against Anthropic to employ the firm's advanced Mythos model.
Rudd has been a frequent visitor to the White House, according to a former official, with AI-related issues dominating his conversations there. The administration has proposed a massive, multibillion-dollar budget increase for investments in IT and computing capability, according to former officials. Approved by Congress as part of the "black budget," NSA's funding levels are a tightly held secret.
The last major agency restructuring, known as "NSA 21," was initiated in 2016 under then-Director Mike Rogers. That effort, which divided NSA into six directorates, was given a two-year runway for its rollout and still remains unfinished, the first former official noted.

Al-Qaeda Releases Propaganda Video on 25th Anniversary of September 11 Attacks

Source: https://www.counterextremism.com/press/extremist-content-online-al-qaeda-releases-propaganda-video-25th-anniversary-september-11

An individual identified as Hamza bin Laden in an al-Qaeda Al-Sahab video memorializing the 25th anniversary of the September 11 attacks.

On September 10, al-Qaeda released an approximately 52-minute video, titled "A Quarter Century of the 11 September Raids," from the group's Al-Sahab Media Foundation, honoring the 25th anniversary of the September 11 attacks and noting the group's continued threat. The video contained previously released news footage of the attacks, news reports, and television interviews with various U.S. and European commentators, academics, and former officials discussing the long-term impact of the attacks and the continuing danger posed by al-Qaeda and jihadist terrorism. The video also included previously unseen footage of an individual identified as Hamza bin

Laden, Osama bin Laden's son, whose death was announced by the U.S. in 2019. The video did not contain information that would have identified Hamza bin Laden as having been killed. In his segments, he claimed that the enemies of Islam were waging a full-scale war on the battlefield, as well as in terms of religion, economy, and culture, and called on others to engage in the fight. Additionally, he memorialized al-Qaeda casualties.
The video also included a voiceover from senior al-Qaeda leader Saif al-Adel, who claimed that al-Qaeda was still capable of launching attacks against the U.S.

New wave of terrorism in Russia?

By Aleksander Olech
Source: https://defence24.com/geopolitics/new-wave-of-terrorism-in-russia

Sep 21 – Terrorism in Russia should be analysed not only as a threat to national security, but also as a political tool used by the Kremlin at the national, regional and international levels. The evolution of threats in the Russian Federation, from the North Caucasus and the Caucasus Emirate, through the growing significance of the so-called Islamic State, to the activities of the Islamic State – Khorasan Province and the attack at the Crocus City Hall, illustrates the many challenges facing the Russian security services. Terrorism is a term that is widely used but difficult to define unambiguously. The phenomenon is dynamic and depends on the legal and political context, as well as on the actor defining it: the state, an international organisation or a researcher. In the Russian case, this ambiguity is particularly important, because Moscow does not treat terrorism only as a security category. It also treats it as a political instrument.
It should be emphasised that extremism is not a synonym for terrorism. Extremism refers to a broader ideological, organisational and political category associated with extreme views, radicalisation, propaganda or the activities of groups regarded as a threat. It may lead to violence or terrorist activity, but it is not necessarily the same thing. Terrorism refers primarily to the use of violence or the threat of violence for political, ideological, religious or social purposes.
In the Russian legal system, extremism and terrorism are treated as related but distinct legal categories. Article 282.2 of the Criminal Code of the Russian Federation concerns extremist organisations, but explicitly excludes organisations designated as terrorist under Russian law. Terrorist organisations are covered by separate regulations, in particular Article 205.5 of the Criminal Code, which concerns the organisation of, and participation in, the activities of a terrorist organisation.
At the same time, in the practice of the Russian security apparatus, the concepts of extremism and terrorism are sometimes used in parallel as instruments of social control and for the political definition of threats. This is the core of the Russian approach. For the Moscow authorities, achieving political objectives is crucial, and for this reason they use their own, context-dependent definition of terrorism.
Russian legislation, including Article 205 of the Criminal Code, defines a terrorist act as causing an explosion, arson or other acts designed to instil fear in the population and pose a threat to life, cause significant property damage or other grave consequences, undertaken to destabilise the activities of public authorities or international organisations or influence their decisions. The provision also covers the mere threat of carrying out such actions.
The Federal Law „On Countering Terrorism" defines terrorism as an ideology of violence and the practice of influencing the decisions of government authorities or international organisations by

intimidating the population or through other forms of unlawful action involving the use of violence. The Act introduces a broad understanding of terrorist activity, including attacks, planning, financing, incitement, the creation of illegal armed structures, recruitment, training, information activity and propaganda. This broad scope gives the Russian state considerable leeway in classifying certain activities as terrorist. The National Antiterrorism Committee serves as the central body coordinating Russia's counterterrorism efforts, integrating the activities of federal, regional and local structures under the leadership of the Federal Security Service. It is responsible for planning counterterrorism operations, shaping state policy in this area and managing communication related to threats. This demonstrates the centralisation of Russia's security system and the significant role of the Kremlin in defining threats. Russia also defines international terrorism in very broad terms and in a way directly linked to its own interests. Article 361 of the Criminal Code includes not only traditional acts of violence, such as terrorist attacks or arson, but also any activities considered to be directed against the interests of the Russian Federation or to interfere with the „peaceful coexistence of states". In practice, this means that the category of terrorism can be applied much more broadly than only to domestic security threats.

From the North Caucasus to ISIS-K

After the collapse of the Soviet Union, the highest concentration of terrorist attacks on Russian territory was recorded in the North Caucasus, especially in Chechnya, Dagestan and Ingushetia. These areas have long been major centres of activity for Islamist and separatist groups. Although North Ossetia was the site of one of the most tragic terrorist attacks in Russia's history, its significance in contemporary attack statistics is smaller than that of the other Caucasian republics. As recently as 2012, before the series of attacks in Western Europe, including in France, Great Britain, Belgium and Germany, the terrorist conflict in the North Caucasus was regarded as the most brutal of its kind in Europe. During that period, around 700–800 people were killed each year in clashes between Russian forces and militants described by the Russian authorities as terrorists. Between 1992 and 2011, 1,415 terrorist attacks linked to groups operating in the North Caucasus were recorded in Russia. The highest number of incidents occurred in Chechnya, Dagestan and Ingushetia, although some attacks were also carried out in Moscow and Saint Petersburg.

Russia's experience of Islamist terrorism is long-standing and systemic. Since the war in Afghanistan, through the Chechen conflicts and later its involvement in Syria, Moscow has remained one of the main opponents of jihadist groups. As a result, Russia has been the target of numerous attacks, including those carried out at the theatre in Dubrovka in 2002, at the school in Beslan in 2004 and at the Crocus City Hall in 2024. At the same time, despite its awareness of the threat, the Russian security apparatus has limited capacity to neutralise it effectively, especially while stretched by the war against Ukraine.

Since the 1990s, Russia's „war on terrorism" in Chechnya has not been merely an internal affair. It has been part of its foreign policy strategy. After the attacks of 11 September 2001, Moscow sought to frame its actions in the Caucasus within the global narrative of the fight against terrorism. It used the temporary convergence of interests with the United States, especially in the context of Afghanistan and the American military presence in Central Asia, to legitimise its own operations.

For many years, Chechen separatists were portrayed by the Russian authorities as the most serious terrorist threat to the Russian Federation. Between 1999 and 2013, structures originating from this movement were responsible for most terrorist attacks carried out on Russian territory,

although their activity gradually decreased over time.

A new phase began on 31 October 2007, when Doku Umarov, one of the leaders of the North Caucasian insurgency, renounced his position as President of the Chechen Republic of Ichkeria and proclaimed the creation of the Caucasus Emirate. It was an Islamist, self-proclaimed organisational structure that for many years served as the principal terrorist base in the North Caucasus. Local jamaats operating in Dagestan, Ingushetia, Kabardino-Balkaria, Karachay-Cherkessia and North Ossetia became the organisational and personnel base for the Caucasus Emirate. In December 2009, the Supreme Court of the Russian Federation banned its activity, recognising it as a terrorist organisation.

The rise of the so-called Islamic State had a direct impact on the security situation in the Russian North Caucasus. Hundreds of militants left the region to join the armed conflict in Syria and Iraq. Among the foreign fighters serving in the ranks of ISIS and other jihadist organisations, a significant proportion were citizens of the Russian Federation, many of whom came from the North Caucasus. This weakened the Caucasus Emirate and reduced its recruitment opportunities.

After 2014, the structures of the Caucasus Emirate began to break down. This was the result of both intensified operations by the Russian security services and deep internal divisions within the Caucasian jihadist community. Between 2014 and 2015, some commanders and militants pledged allegiance to ISIS, which gradually assumed the role of the dominant ideological and organisational centre for radical circles from the North Caucasus.

The Islamic State Caucasus Province, established in June 2015, became a significant actor in Russia's terrorist threat landscape. It drew on part of the former Caucasus Emirate's cadre base and organisational infrastructure. During the Syrian conflict, around 2,800 fighters from the countries of the former Soviet Union joined the fighting in the ranks of ISIS, including people from the North Caucasus and Central Asian states. This led to the gradual disintegration of the Caucasus Emirate and the takeover of part of its personnel and infrastructure by ISIS structures.

Russia's military intervention in Syria in 2015 further increased the terrorist threat. When Moscow launched its military offensive in support of Bashar al-Assad, jihadist organisations began to call for attacks against Russian citizens and interests. On 31 October 2015, an explosive device detonated on board a Russian passenger aircraft flying from Sharm el-Sheikh to Saint Petersburg. A total of 224 people were killed. ISIS claimed responsibility, presenting the attack as direct retaliation for Russia's intervention in Syria.

Another example was the attack in the Saint Petersburg metro on 3 April 2017. The Imam Shamil Battalion, affiliated with Al-Qaeda and referring to itself as the „Knights of Islam", claimed responsibility. The suicide bombing between the Sennaya Ploshchad and Tekhnologichesky Institut stations killed 15 people and injured several dozen. Russian authorities detained 11 individuals from Central Asia in connection with the attack. This showed the importance of transnational jihadist networks and their ability to conduct or inspire attacks inside Russia.

Between 2015 and 2022, Russia faced terrorist threats concentrated mainly in the North Caucasus. These attacks were largely carried out by jihadist groups linked to the Islamic State Caucasus Province, which had taken over part of the personnel and structures of the former Caucasus Emirate. They most often took the form of targeted strikes against security service officers, local government representatives and religious institutions. At the same time, the Russian language became the third most popular language of ISIS propaganda after Arabic and English.

Since 2020, the Islamic State – Khorasan Province has gained increasing prominence in relation to Russia. ISIS-K, operating primarily in Afghanistan and Central

Asia, gradually took the lead in planning and instigating attacks aimed at Russia. This organisation operates differently from previous North Caucasian groups. Its recruitment relies heavily on economic migrants from Tajikistan, Uzbekistan and Kyrgyzstan, functioning on the margins of Russian society. These communities may become vulnerable to radicalisation in conditions of discrimination, repression and disinformation.

The attack at the Crocus City Hall on 22 March 2024 was the most dramatic demonstration of this threat. ISIS-K carried out the attack in the Krasnogorsk area of Moscow Oblast. A total of 144 people were killed and 551 were injured. It was not only one of the largest demonstrations of ISIS-K's capabilities in Russia, but also one of the largest terrorist attacks globally in recent years. The fact that Russia reportedly received warnings from other states, including Iran and the United States, shows that the problem was not only the absence of information. It was also the limited ability, or willingness, of the Russian system to correctly assess the threat.

The Russian response again focused on narrative management. Even immediately after the attack, the Kremlin pushed the suggestion that Ukraine and Western intelligence services were involved. This was consistent with the broader Russian approach after 2022. Terrorism in Russia has ceased to be merely one of the threats to security and has become an element of domestic and international policy, a tool used to support political and military actions.

In 2024, Russia also faced attacks in Dagestan, where armed assailants carried out coordinated attacks on Orthodox churches, synagogues and police stations in Derbent and Makhachkala. At least 20 people were killed, including security officers and clergy, and more than 40 were injured. Russian services did not confirm the identities of the perpetrators. Some information indicated cooperation with organisations associated with ISIS, including the Islamic State Caucasus Province, while ISIS-K provided media support. Once again, Russian authorities constructed a narrative alleging Western or Ukrainian involvement.

Russia, CSTO and the regional security problem

Russia is the main source of terrorist threats in the post-Soviet space among the member states of the Collective Security Treaty Organisation, and it is also a country accused of terrorist activities both domestically and abroad. The Kremlin, in order to achieve its own objectives, demonstratively resorts to measures in domestic policy that fall within the definition of terrorism. At the same time, Russia develops an anti-terrorist strategy that it uses to subjugate regions and communities and to justify military actions.

The terrorist threat to CSTO member states is connected not only with the Caucasus, but also with Central Asia and Afghanistan. There is a risk that terrorist organisations from the Caucasus will attempt to carry out attacks not only in Russia, but also in other CSTO member states. Their operations also have a criminal dimension, because terrorist organisations cooperate with criminal groups and obtain funds through international drug trafficking, kidnappings and arms sales. The use of the territories of CSTO member states to conduct illegal activities, including through a Europe–Asia trade route, poses a serious threat to regional security.

Afghanistan remains particularly important. Tajikistan, a CSTO member state bordering Afghanistan, has repeatedly reported terrorism-related threats from its southern border. This is linked to the unstable situation in Afghanistan and the lack of security at border crossings. After 2022, Central Asian states significantly changed their policy towards Kabul. They recognise the risks, but at the same time the development of Afghanistan's relations with Kazakhstan, Uzbekistan, Turkmenistan, Tajikistan and Kyrgyzstan is influenced by Russia, which seeks to oversee regional

cooperation projects and prevent Central Asian states from strengthening their independence.

The CSTO has formal structures for counterterrorism cooperation. Its Working Group on the Fight against Terrorism and Extremism prepares proposals to improve joint operations, regularly updates lists of organisations recognised as terrorist and extremist in member states, and works to improve the operational and combat training of special forces units. Between 2024 and 2025, it maintained and adapted its existing priorities to the changing security environment. Particular emphasis was placed on countering terrorist and extremist activity involving disinformation and new technologies, including propaganda and recruitment in cyberspace, combating transnational terrorist groups linked to cells in Afghanistan, protecting external borders, especially the Tajik-Afghan border, and strengthening joint exercises, IT cooperation and legal cooperation.

There are also many areas of cooperation between the CSTO and the United Nations in the field of combating terrorism. The basis for joint activity includes agreements between the CSTO Secretary General and selected UN organisational units, including the memorandum of understanding with the Counter-Terrorism Committee of the UN Security Council and the cooperation agreement between the CSTO Secretary General and the United Nations Office of Counter-Terrorism. Cooperation with the Commonwealth of Independent States and the Shanghai Cooperation Organisation is also significant.

However, Russia's war against Ukraine exposed the weakness of the CSTO as a collective security mechanism. Instead of consolidation and cooperation, there has been distancing. Most members, apart from Belarus, have avoided openly supporting Moscow. They do not want to legitimise aggression or risk losing profits in their relations with the West. At the same time, the Kremlin continues to use the narrative of the need to combat terrorism and to justify its military operation in Ukraine in order to maintain influence in the region.

The problem is that, without Russia's ability to intervene and impose resolutions on conflicts such as Armenia–Azerbaijan or Kyrgyzstan–Tajikistan, the CSTO becomes increasingly powerless. Countries in the region are seeking alternative cooperation projects with China and Turkey, as well as channels with the European Union. This weakens Russia's ability to present itself as the uncontested security guarantor in the post-Soviet space.

Africa, Syria and the internationalisation of the threat

Russia's counterterrorism narrative also has an international dimension. Moscow declares that its counterterrorism efforts are focused primarily on the Sahel states, particularly Mali, where the fight against terrorism serves as one of the main justifications for the presence of Russian military forces and mercenaries. In practice, however, this activity also serves broader political, economic and military objectives, including maintaining influence and access to natural resources.

Russia's anti-terrorist policy in Africa is presented as a response to the activities of jihadist groups operating on the continent. These include the Group for the Support of Islam and Muslims, Jama'at Nusrat al-Islam wal-Muslimin, the Islamic State Sahel Province, the Islamic State West Africa Province, Islamic State structures in Mozambique, also referred to as Ansar al-Sunna or Ahl al-Sunna, and, in Central Africa, the Allied Democratic Forces and ISIS structures in the Democratic Republic of the Congo linked to the Islamic State Central Africa Province.

In the Russian security narrative, these groups are portrayed as a threat that justifies Moscow's continued military and political presence in selected African states. Yet the data show that terrorist

threats remain strong in several countries where Russia is present or active. Mali, Burkina Faso, Niger, Mozambique, Libya, the Central African Republic and Sudan remain unstable. Russian activity does not lead to the elimination of terrorism. Instead, it often fits into a mechanism that sustains an environment of instability, enabling governments and juntas to become dependent on external support.

This is one of the most important elements of the Russian model. Russia functions as a beneficiary of prolonged chaos. Terrorism remains an element of cooperation that enables and justifies its continued presence, rather than a problem Moscow is able to resolve systemically. Russian mercenaries in Africa, who are often regular soldiers of the Russian army in practice, have repeatedly failed to effectively oppose terrorist groups. This scenario has been visible in Mozambique, the Central African Republic, Mali and Burkina Faso.

If Russia decides to build new bases, continue expanding the presence of the Wagner Group or Africa Corps, maintain infrastructure in Syria and construct additional facilities in Africa, it will have to commit more troops and resources to counterterrorism efforts both in Russia and abroad. This will require additional and significant investments, as well as a reallocation of resources, including funds currently allocated to the war in Ukraine. Russian bases in Africa would automatically become targets for terrorist groups, including jihadist organisations.

The Russian Federation therefore remains one of the countries particularly exposed to terrorist threats. In the Global Terrorism Index 2025, Russia was ranked 17th in the world, moving up 20 places compared with the 2024 report. In the Global Terrorism Index 2026, it ranked 16th. This rise was a consequence of increased terrorist activity within the country, including successful attacks with a significant impact on society. Russia, while conducting a full-scale military operation against Ukraine and engaging militarily in Africa under the slogan of combating terrorism, is simultaneously increasing its vulnerability to such threats.

The political use of counterterrorism

The authorities in Moscow portray Russia as a key actor in the international fight against terrorism. They emphasise the need to avoid double standards and to build a broad coalition against terrorism and extremism. They treat counterterrorism as a tool of state policy. They promote a narrative that prioritises eliminating existing threats rather than prevention. They control the information space and marginalise the importance of human rights. This is intended to legitimise repressive methods inside the country and increase influence abroad.

At the same time, establishing cooperation with the Taliban government or using „counterterrorism" operations instrumentally to support activities in Syria, the Sahel and Ukraine undermines the credibility of this narrative. Russia is not only trying to fight terrorism. It is trying to compete with Western countries in the way threats are defined, security narratives are constructed and its own actions are legitimised under the banner of counterterrorism.

The Russian Federation has for years argued that the fight against terrorism should be conducted without double standards, often using this issue to highlight what it presents as Western hypocrisy. This argument has become an important instrument of Russian foreign policy. Moscow opposes what it sees as selective Western treatment of actors such as Afghanistan, Iran, Syria, Hezbollah or Hamas, and uses this to undermine the credibility of the United States and its allies.

The events of 2024, including the Crocus City Hall attack and the attacks in Dagestan, showed not only the scale of challenges in the field of terrorism, but also gaps in the Russian response system, despite earlier warnings from other states. The Kremlin's response focused largely on

controlling the narrative, expanding the powers of the security services and attributing responsibility to selected terrorist groups and political opponents, in particular Ukraine and Western countries. This is consistent with the use of terrorism as an element of domestic policy and as a tool for mobilising public support.

The Crocus City Hall attack demonstrated that, despite years of pacification efforts, Russia had not eliminated the sources of the terrorist threat. The root of the problem still lies partly in the North Caucasus, where radicalisation in republics such as Chechnya, Dagestan and Ingushetia remains a persistent phenomenon, particularly among younger generations. Jihadist structures linked to the Islamic State, and also to the re-emerging Caucasus Emirate, continue to focus on operations against security services and state institutions. The conditions and threats discussed do not necessarily indicate a constant increase in the scale of terrorism in Russia, but they do indicate the existence of persistent factors that cannot be fully eliminated, even by an authoritarian security apparatus. The neglect of early signs of radicalisation, the ongoing and escalating terror, and the privileged position of Russian security services at local and regional levels have led to incorrect threat assessments and delayed state responses.

This is the key weakness of the Russian model. It is based less and less on prevention and more and more on the political definition of opponents. It allows the Kremlin to describe enemies as terrorists, to present repression as security policy and to justify foreign military action as counterterrorism. But this model does not eliminate terrorism. It distorts the perception of threats.

Russia cannot, and will not, fully eliminate terrorist threats domestically or abroad. The experience of the North Caucasus, the influence of Chechen elements, the activities of Al-Qaeda and ISIS, the emergence of ISIS-K, the attacks in Moscow and Dagestan, and the instability surrounding Russia's foreign operations all point in the same direction. Moscow may strengthen the security apparatus, expand legislation and control the narrative. But if counterterrorism is used primarily as a political tool, the state will continue to misread threats and remain vulnerable to further attacks.

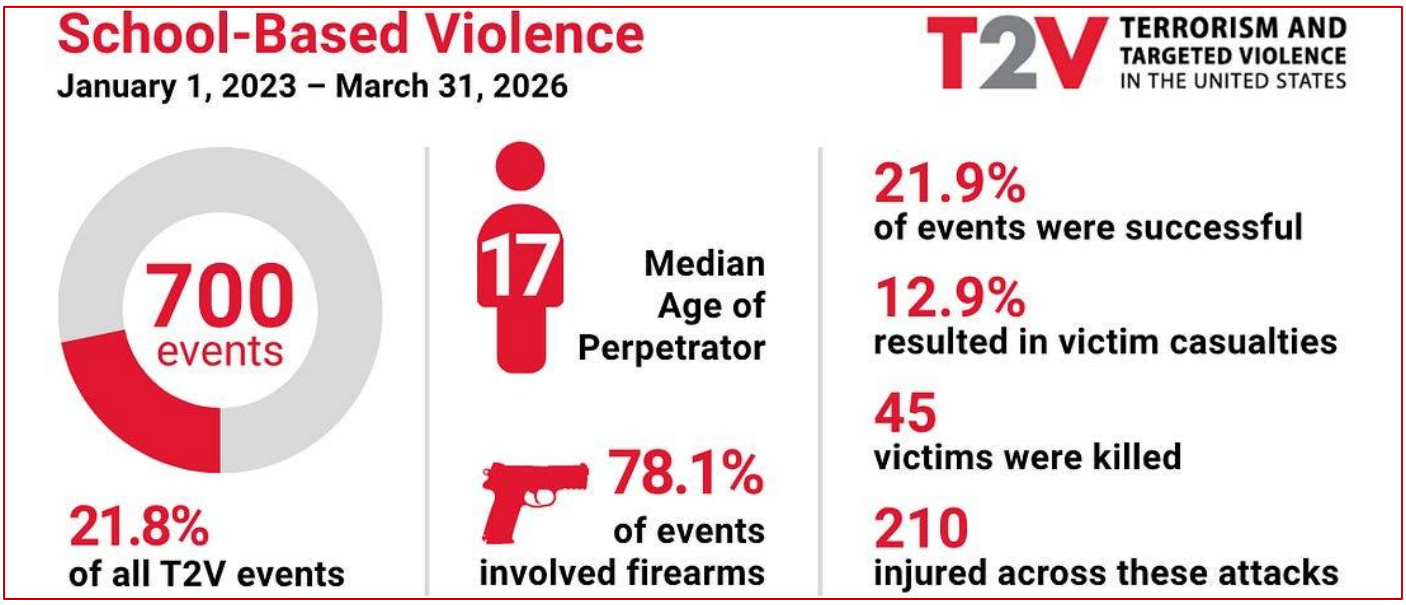
Aleksander Olech is Head of International Cooperation and Editor-in-Chief at Defence24.com. Lecturer at national and international universities, NATO associate, analyst, and publicist. Former Deputy Director of the Department of Africa and the Middle East at the Ministry of Foreign Affairs. Graduate of the European Academy of Diplomacy and the War Studies University. Main research interests: French-Russian relations, challenges in Africa, and NATO security policy.

Terrorism and Targeted Violence (T2V) in the United States: Plots Targeting U.S. Schools

Source: https://www.start.umd.edu/publication/terrorism-and-targeted-violence-t2v-united-states-plots-targeting-us-schools

Abstract

This research brief explores school-based violence in the United States from January 1, 2023, through March 31, 2026. The data for this brief are provided by the Terrorism and Targeted Violence (T2V) in the United States database, which includes comprehensive information on 3,216 foiled, failed, and successful attacks in the U.S. and its



territories that were designed to have a significant impact on public safety or the security of critical infrastructure and key resources. More information about the T2V database can be found in the "About T2V" section at the conclusion of this brief. The analysis presented here explores 700 premeditated plots in the T2V data targeting school spaces in the United States. It analyzes the rates of school-based violence in the U.S., the locations of these plots, the weapon types used by perpetrators of school-based violence, and the intentions and outcomes of these plots. This brief also provides general statistics on the ages of perpetrators of school-based violence. It also examines the intersection of terrorism and school-based violence.

No Ideology Required: Drones and the New Domestic Extremist Threat

By Zeynep Ozharat

Source: https://smallwarsjournal.com/2026/09/21/no-ideology-required-drones-and-the-new-domestic-extremist-threat/

Sep 21 – Drones have no ideology. They work for different motivated groups and individuals, whether they are motivated by jihad, antisemitism, or anti-government rage. Conspirators in the foiled UFC Freedom 250 plot had planned to use unmanned aircraft systems (UAS) armed with explosives to initiate their attack. This was the most recent addition to an emerging pattern in the United States: domestic extremists importing the drone tactic from the international scene. In October 2024, a 17-year-old in Arizona was arrested for planning to deploy an explosive drone at a Phoenix Pride Parade, inspired by Islamic State videos he had found online. Weeks later, FBI agents arrested a 24-year-old white supremacist from Columbia, Tennessee, and disrupted his plot to use an explosive-laden drone to attack power grids in Nashville.

Three cases, three ideologies, same tactic. The UFC Freedom 250 plot is not an anomaly, but the newest data point in an upward trend. Drones may now be the weapon of choice for extremists, whatever the target, whatever the ideology.

Three Cases, Three Ideologies, One Tactic

The Jihadist

The trend starts with Marvin Jalo, a 17-year-old who plotted to attack the

Pride Parade in Phoenix, Arizona, with jihadist motivations. In 2023, Jalo began communicating in online chat rooms with "extremists" who were actively recruiting him to conduct attacks. In these groups, he discussed attack options and shared that he could make his own guns with separate parts ordered from the internet. Jalo also mentioned that he learned how to make triacetone triperoxide, an unstable explosive, through videos made by the so-called Islamic State (IS). He was planning to detonate explosives in buildings close to the parade and deploy an explosive remote-controlled drone to maximize impact.

It was Jalo's mother who disrupted the plot. She reported her son's suspicious online activity to the authorities.

The Federal Bureau of Investigation Hostage Rescue Team conducts a raid (Photo: User/DRUERY, WikiMedia Commons, CC0)

The Accelerationist

On November 2nd, less than two weeks later, federal agents arrested 24-year-old Skyler Philippi of Columbia, Tennessee. According to authorities, Philippi was planning to destroy power grids in Nashville with a homemade explosive drone to further his accelerationist ideology. As far back as July 2024, he had contemplated different attack options including a mass shooting at a local YMCA. Philippi was active on Terrorgram, an accelerationist and neo-Nazi network on Telegram.

The Terrorgram Collective and three of its leaders were designated as Specially Designated Global Terrorists in January 2025. The group has influenced various attacks globally, including a shooting outside a gay bar in Slovakia in October 2022, a July 2024 attack plan on New Jersey's energy facilities, and a knife attack at a mosque in Eskişehir, Turkey in August 2024. Philippi's plot to cause the collapse of the U.S. power grid was also inspired by Terrorgram. Terrorgram has historically shared

detailed manifestos about attacks on infrastructure. Their 2022 "zine," *The Hard Reset*, devotes nearly 50 pages to instructions on how to conduct such attacks as well as encouragement.
Philippi was arrested by FBI agents at the location of his plot after powering up the drone. He later pled guilty.

The "Vanguard of the Old"
The third plot was the most ambitious—and the most ideologically diffuse. In June 2026, federal agents arrested seven suspects from four states: California, Ohio, Missouri, and Nebraska. The conspirators had allegedly plotted to attack the UFC Freedom 250 event at the White House. The group—calling itself the "Vanguard of the Old"—was initially a cell operating on TikTok, which then migrated to Signal. The group showed signs of anti-government tendencies, as well as using antisemitic language.
Their plan entailed deploying a drone armed with an explosive on the White House lawn to force an evacuation. Snipers positioned on evacuation routes would then fire upon "high-value targets." The gunmen planned to escape by traveling along the Potomac River, if needed. Targeting was based on whether the plotters' perception of certain Congress members as being funded by the pro-Israel lobby AIPAC.
In the weeks leading up to their arrest, Vanguard of the Old conspirators shared aerial maps of the White House lawn, divided themselves into tiers, assigned operational roles, and tried to crowdfund the $1,300 needed for the operation.
The plot was disrupted after the mother of one of the conspirators called the police.

A Spectrum of Ideologies
What these cases reveal is a shared, preferred tactic with differing targets. Philippi targeted critical infrastructure while Jalo and the Vanguard of the Old focused on public gatherings and politicians, as well as famous figures they deemed to be "high-value targets."

Lewis and Baumgartner identified the Nashville case as a critical point, arguing that the emergence of the drone in domestic terrorism plots represents a changing domestic extremist strategy. They warn that the U.S. government has been slow to counter this attack vector. They were right. The subsequent UFC Freedom 250 case confirms that the desire to utilize drones and other emerging technologies is not confined to a single ideology and has become an appealing tactic across the ideological spectrum.

Not New, But Newly Dangerous

Domestic extremists did not pioneer drones as a means of maximum destruction, but imported it.
International non-state actors spent decades developing and refining drone weaponization. Hezbollah was the first group to establish a UAS program, with significant support from Iran. The group conducted surveillance missions over Israel back in 2004, later expanding their program to carry payloads against Israeli targets. Hamas also showed early interest in UAS for reconnaissance and attacks. The militants likely re-engineered Israeli drones shot down in Palestinian territory to further their own UAS capabilities.
The mid-2010s saw an acceleration with the rise of the Islamic State, which transformed commercial drones into multi-purpose tools for intelligence, surveillance, and reconnaissance, strikes, and propaganda. The terror group pioneered the large-scale use of drones, on which others would later build. With significant backing from Iran, the Houthis—similarly to Hezbollah—took it further. Beginning in 2018, they conducted attacks against U.S. military assets, regional governments, and commercial shipping in the Red Sea.
The use of drones to carry out attacks has proliferated from the battlefield to the backyard, and the aspiration to use them within the United States predates these three plots.Rezwan Ferdaus, a

U.S. citizen, was arrested in September 2011 for plotting an attack using a remotely controlled aircraft armed with grenades. The attack would have been followed by a ground assault on the Pentagon and the United States Capitol. Ferdaus had already been designing and making detonation devices with cell phones and supplying them to undercover FBI employees. He believed the detonation devices were being used to kill U.S. soldiers in Iraq, as well as train al Qaeda members. His attack was disrupted by the FBI, and he was sentenced to 17 years in prison. But his plan would later bear a striking resemblance to the UFC Freedom 250 plot, with far more external resources available and fewer technological barriers. Like Ferdaus, Ammar Abdulmajid-Mohamed Said was arrested in May 2025 for allegedly plotting a mass shooting at the U.S. Army's Tank-Automotive & Armaments Command facility in Warren, Michigan. Said hoped to assist Islamic State, either abroad or within the United States, and contemplated travelling to IS-controlled territory earlier in 2024. His plot included flying drones to surveil the grounds prior to his intended attack.
Said was arrested by law enforcement shortly after launching the drone.

Different Plots, Different Learning Models

The three cases reveal distinct pathways from radicalization to operational planning and thus, different learning processes. Though inspired by Islamic State, Jalo is believed to have self-radicalized. He learned from publicly available information and became further radicalized in online chat rooms. Furthermore, his young age and lone wolf status made early detection and disruption difficult. The network provided him with both an ideological and technical base, as well as motivation and guidance for acquiring the capability to carry out an attack. Given his involvement with a known terrorist collective and association with other violent extremists, the trajectory Philippi followed is generally easier to track for law enforcement. Counterterrorist agents can effectively disrupt the plot through the use of advanced surveillance and undercover employees. Moreover, an undercover FBI operative was able to render the explosive device Philippi planned to use inert
Lastly, the UFC Freedom 250 plot introduced a new model. The Vanguard of the Old was a crowded, busy cell, highly active on chat groups. It distributed the necessary motivation and expertise among its many members. The accused seven were motivated by a variety of grievances, spanning from antisemitism to antigovernment rage, which informed the different layers of their attack planning. The cell also possessed technical expertise: one of the conspirators allegedly used his prior drone manufacturing knowledge to provide the UAS capabilities. The group's migration from TikTok to Signal (an encrypted application) and internal sourcing of technological knowledge made detection more difficult.

Policy Responses

Legislators and policymakers have been proactive, making good progress in safeguarding against the UAS threat from extremists. The Safer Skies Act of 2025 expands the use of counter-UAS (cUAS) to State, local, Tribal, and territorial law enforcement and correctional agencies with strict reporting requirements. CUAS authority has been concentrated within certain federal agencies, and the rollout of that authority—although within strict boundaries—reflects the growing importance the government attributes to the growing UAS threat. The Joint Interagency Task Force 401 (JIATF 401) was established by the Department of Defense (DoD) to coordinate counter-small UAS efforts across agencies. The task force aims to better align resources and authorities to combat the quickly evolving UAS threat. The creation of the task force comes partly amidst the intensive use of drones by state and nonstate actors in the Middle East and Eastern Europe. Nevertheless, JIATF 401 also addresses homeland security concerns and provides guidance for countering

the threat in the homeland. The DoD fills the gap of a centralized effort to oversee UAS threats at home and abroad, aiming to accelerate testing and procurement. The most recent cUAS manual, published on July 8, goes beyond military guidance and offering a practical resource for local law enforcement.

While the Safer Skies Act covers public gatherings, the implementing regulations took effect on July 1 of this year. The operational aspect is yet untested. Similarly, the $500 million contract supporting JIATF 401 demonstrates willingness and policy momentum, but its efficacy is not guaranteed. The challenge for both initiatives will be the scattered threats that can emerge from any ideology and platform against any target.

Conclusion

Drones are the new weapon in the arsenal of any extremist. The three cases only converge at one point. Not at an ideology or a target, but at their weapon of choice.

When a new tactic becomes common across the ideological spectrum, ideology stops being an effective indicator of the nature of the threat. All three drone attacks were disrupted before they were executed by fortunate interventions: two by a mother's phone call, and one by undercover FBI agents.

The Safer Skies Act, JIATF 401, and other cUAS efforts demonstrate policy progress, but operational capacity must keep pace. Another drone plot with drones will emerge, and law enforcement must be ready.

Zeynep Ozharat is a research fellow at the Program on Extremism at The George Washington University. Previously, she served as a research assistant to Dr. Bruce Hoffman and as an editorial assistant for the journal *Studies in Conflict & Terrorism*. She holds an M.A. in security studies from Georgetown University as a Fulbright Scholar and a B.A. in international relations from Bilkent University, where she graduated as valedictorian.

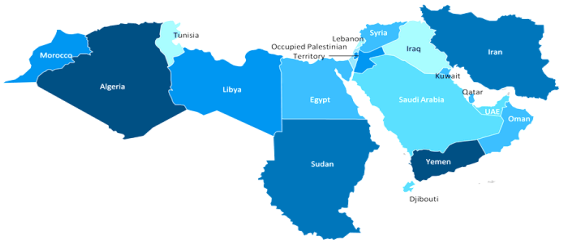
ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

CHEM NEWS

Journal of CONTINGENCIES AND CRISIS MANAGEMENT



ORIGINAL ARTICLE | Open Access

Experts' Opinion on Decontamination and Antidote Strategies: Complementing Contemporary Expert Consensus and Evidence to Optimize Preparedness and Response to CBRN Threats in the Middle East and North Africa

Correction(s) for this article

Hassan Farhat, Derrick Tin, Heejun Shin, Saleh Fares Al-Ali, Daren Mochrie, Brendon Morris, Gregory Ciottone

First published: 16 February 2026 | https://doi.org/10.1111/1468-5973.70128 | VIEW METRICS

Abstract

Chemical, biological, radiological, and nuclear (CBRN) incidents present escalating challenges, particularly in geopolitically unstable regions such as the Middle East and North Africa. Despite advances, gaps exist regarding optimal decontamination protocols and agent-specific antidote selection algorithms, exacerbated by variable operational contexts, fragmented services, and inconsistent training initiatives. This paper synthesizes recent evidence, building on an artificial intelligence-enhanced Delphi study with 40 international experts, to assess current CBRN response strategies. Findings support immediate dry decontamination within 5–15 min, removing over 80% of contaminants and avoiding 'wash-in' effects. Triple-phase protocols achieve > 97% reduction. Medical oversight during decontamination is critical. Antidote readiness must expand beyond organophosphates to include cyanide, biological agents, radiological decorporation, and synthetic opioids. Special populations, such as paediatric, older, and pregnant individuals, as well as those with disabilities, require tailored approaches. Effective CBRN readiness demands integrated, evidence-based strategies that emphasize rapid response, medical integration, and population-specific adaptations within global collaboration frameworks to address evolving threats.

CBRN Operations During the Night

The Editor

CBRN operations in an urban environment are inherently complex, but their difficulty increases substantially after sunset. Darkness does not simply reduce visibility; **it changes the operational environment.** It affects threat recognition, navigation, casualty identification, contamination control, communications, personal protective equipment (PPE), decontamination, vehicle movement, medical

evacuation, command and control, and the psychological condition of both responders and casualties. In a CBRN incident, where hazards may be invisible, odorless, and geographically uncertain, the absence of daylight can transform an already difficult problem into a multidimensional operational challenge.

The fundamental principles of CBRN response remain unchanged at night. The incident must still be recognized, isolated, characterized, controlled, and progressively transitioned from the contaminated area to the contamination-reduction area and ultimately to the clean operational area. OSHA/NIOSH guidance similarly conceptualizes the operational environment as progressively controlled zones: the Red Zone, where significant contamination is confirmed or strongly suspected; the Yellow Zone, where contamination is possible, and initial monitoring exists; and the Green Zone, where contamination is unlikely. Nevertheless, the night environment introduces a second operational dimension: visibility management. Every CBRN activity must now be performed under conditions in which the responder may be unable to see contamination, casualties, obstacles, terrain features, PPE damage, hand signals, warning signs, drainage routes or other personnel. Consequently, effective night CBRN operations require the integration of CBRN detection and protection with lighting, night vision, thermal imaging, navigation, communications, security and medical support. The objective is therefore not simply to "operate at night." It is to create a controlled operational corridor from the Hot Zone to the Cold Zone in which contamination, personnel, equipment, casualties and information are continuously controlled.

The Urban Night CBRN Environment

The urban environment creates a particularly complicated CBRN battlespace. Buildings create multiple vertical and horizontal spaces, streets form channels for movement and potentially for contaminant dispersion, underground

structures can retain contaminants, and large numbers of civilians may move unpredictably through the affected area. At night, these characteristics become substantially more difficult to interpret.
The responder may encounter an environment consisting simultaneously of darkness, artificial illumination, smoke, dust, fire, vehicle headlights, emergency lighting, reflections from wet surfaces, and shadows between buildings. These conditions can interfere with visual identification and, depending on the technology employed, can also complicate interpretation of thermal or night-vision imagery.
Urban geometry can also make the conventional concept of a circular contamination zone misleading. The actual contaminated area may be irregular, affected by wind (urban canyons), ventilation systems, building interiors, underground passages, drainage systems and human movement. A CBRN plume may therefore move through an urban environment in a manner that is not immediately apparent to responders at ground level.
The night environment also increases the possibility of secondary contamination. A responder leaving the Hot Zone may unknowingly transfer contamination to a vehicle, stretcher, medical team, command post or hospital. OSHA specifically emphasizes that the Green Zone should lie beyond the expected significant dispersal range and secondary contamination generated by traffic and emergency responders.
Thus, the operational boundary is not merely a geographical boundary; it is a contamination-control boundary.

From the Hot Zone to the Cold Zone

The classical Hot–Warm–Cold Zone concept remains central to CBRN operations. FEMA describes the Hot Zone as the area immediately surrounding the incident where primary contamination may occur, with the Warm Zone functioning as the contamination-reduction area and containing decontamination operations.
The Cold Zone is the area in which command, logistics, medical support, staging and other support activities can safely occur. Joint CBRN doctrine similarly describes the Cold Zone as a clean area containing command and support functions and emphasizes its accessibility, sufficient space and suitability for responder safety and rest.
During night operations, however, the transition between zones should be understood as a controlled sequence rather than a simple physical movement.
A responder entering the Hot Zone crosses a boundary established on the basis of the available threat information. Within that zone, the primary objectives are lifesaving intervention, reconnaissance, detection, hazard characterization, and extraction. All these depend on how fast responders arrive at the scene and the PPE donned (SCBA limitations). The responder then moves toward the Warm Zone, where contamination reduction occurs. Only after appropriate decontamination and contamination control should personnel or casualties enter the Cold Zone.
At night, every transition point should be clearly identifiable under low-light conditions. The boundaries therefore need to be recognizable not only visually but also through standardized illumination, signs, markers, communications, and physical control points.

The Hot Zone at Night

The Hot Zone presents the highest combination of CBRN and operational risk. OSHA guidance notes that the area may be life-threatening from both skin contact and inhalation when contamination is confirmed or strongly suspected and remains insufficiently characterized.
At night, the responder's principal enemy is uncertainty.
The operator may not know precisely where the contaminant is located, whether a victim has been contaminated, whether an object is contaminated, whether a

liquid on the pavement is water or hazardous material, or whether a darkened building contains additional casualties.
The first requirement is therefore discipline in movement**.** Unnecessary movement increases exposure time and creates additional opportunities for contamination transfer. The second requirement is continuous situational awareness. The responder must maintain awareness of the hazard, PPE condition, team location, exit route, communications status, and available escape options.

Thermal (left) vs night-vision (right) technologies.

Lighting should be carefully controlled. Excessive white light may improve visibility but can compromise tactical security, interfere with night vision and create glare. Insufficient lighting, conversely, increases the probability of falls, collisions and navigation errors. The ideal system is therefore layered: appropriate ambient illumination where operationally acceptable, controlled task lighting for specific activities, and night-vision or thermal systems where required.
A major challenge is the identification of casualties. A victim lying in darkness may be difficult to locate, while a conscious contaminated casualty may move toward responders or attempt to escape independently. Thermal imaging can assist in locating people, but thermal signatures do not establish CBRN contamination and should never be treated as a substitute for CBRN detection.
The distinction is fundamental: Night-vision technology identifies the environment; CBRN detection characterizes the hazard.

CBRN Detection and Monitoring in Darkness

Detection is one of the most important functions in the Hot Zone. Darkness itself does not necessarily reduce the analytical capability of a properly designed detector, but it complicates the operator's ability to interpret the surrounding environment and safely use the equipment.
Monitoring personnel must therefore work with an integrated system consisting of the detector, illumination, navigation, communications, and buddy monitoring.
Instrument readings should be interpreted within the operational context rather than in isolation. A negative reading does not automatically mean that an area is safe. Detection capabilities have limitations, and concentrations may vary spatially and temporally.
The problem becomes particularly important in urban environments where contaminants may accumulate in low areas, confined spaces, buildings or underground structures. The apparent absence of contamination at street level cannot necessarily exclude contamination inside a building or subterranean environment. In addition, self-adhesive colorimetric chemical papers that change color when in contact with liquid CWAs might give results not accurately interpreted at night.
Night operations consequently require a strong principle of progressive confidence: responders should progressively reduce the uncertainty concerning the hazard rather than prematurely declare an area safe.

The Human Factor

CBRN PPE already imposes substantial physiological and psychological burdens. Darkness adds another layer of stress.

Communication becomes more difficult because responders cannot easily use visual cues. Team members may lose sight of one another. Hand signals become less effective. The operator's perception of distance and direction becomes less reliable. Fatigue develops more rapidly, particularly when personnel have already spent time working in protective clothing.
The psychological effect should not be underestimated. A responder entering a contaminated building at night experiences a fundamentally different psychological environment from the same operation during daylight. The combination of darkness, uncertainty, respirator restriction, reduced sensory information and knowledge of invisible contamination can produce cognitive overload.
The consequence is that night CBRN operations require greater simplicity, not greater complexity. Procedures should be standardized, communications concise, team roles predetermined and navigation routes established before entry whenever possible. Personnel should not depend upon improvisation under conditions of darkness and respiratory protection. Inclusion of night drill in the annual training programme will help alleviate stress and boost confidence.

The Warm Zone: The Critical Transition Area

The Warm Zone is arguably the most important area in the entire night CBRN operation because it is the interface between contamination and medical care.
It is where contaminated casualties become potentially manageable casualties, contaminated responders become clean responders, and contaminated equipment must be separated from clean equipment.
FEMA describes the Warm Zone as the contamination-reduction area surrounding the Hot Zone and identifies it as the principal area for decontamination of survivors, responders, and equipment. At night, this area must be particularly well organized.
The decontamination corridor should have a clear direction of flow. Personnel should be able to identify where to enter, where to move, where to undergo decontamination, and where to exit. Casualty movement should be separated from responder movement whenever feasible.
Lighting should support the work without creating excessive glare. Decontamination personnel must be able to see PPE surfaces, casualty skin, clothing, equipment and contamination indicators. At the same time, lighting must not compromise operational security when the incident has a security dimension.
The Warm Zone should therefore be treated as a controlled production line for contamination reduction, rather than as an improvised collection of hoses and tents.

Night Decontamination

Decontamination at night introduces several additional hazards.
Water can accumulate on the ground and create slip hazards. Cold weather can produce hypothermia, particularly among inadequately protected casualties. Steam or aerosol formation can reduce visibility. Electrical equipment can become a hazard in wet environments. Drainage becomes more difficult to monitor, particularly in urban streets where contaminated water may enter storm drains.
NATO CBRN training guidance emphasizes that decontamination planning must consider victims, responders, vehicles and equipment, as well as drainage, weather, cultural considerations, crowd control and the need to maintain casualties' warmth.
This becomes especially important at night because environmental conditions may deteriorate rapidly after sunset.
The traditional assumption that "more water equals better decontamination" is also inappropriate. Decontamination strategy must be determined by the agent, contamination level, victim condition, available resources, and environmental

circumstances. Contemporary response guidance includes algorithms intended to assist responders in determining whether water-based decontamination is appropriate after disrobing and emergency decontamination.
For night operations, therefore, decontamination must be designed before the first casualty arrives, including lighting, drainage, warming, waste management, replacement clothing and casualty identification.

Casualty Management

A major challenge is the coexistence of two priorities: saving life and controlling contamination.
The contaminated casualty cannot always wait for complete decontamination before receiving lifesaving intervention. Conversely, uncontrolled medical intervention inside the Cold Zone can contaminate the entire medical system.
The solution is a graded approach.
Immediate lifesaving actions may be necessary in the Hot or Warm Zone, depending on the nature of the incident and the casualty's condition. Definitive treatment should progressively move toward the Cold Zone once contamination has been adequately controlled.
This requires medical teams to understand that decontamination is part of medical treatment in a CBRN incident, rather than simply an environmental-cleaning procedure.
Night operations make this particularly important because triage personnel may have difficulty distinguishing severely injured casualties from lightly affected or ambulatory casualties. Standardized illuminated casualty identification systems and disciplined triage pathways can therefore become operationally significant.
If there is adequate lighting in the Warm Zone, procedures can progress relatively smoothly. But what if there is no lighting at all? This is the case when improvisation might solve problems and even save lives. Use the cold light of the intubation handle as a torch to perform intubation or inspect pupils. On the other hand, this is why torches are valuable even when lighting is sufficient.

The Cold Zone at Night

The Cold Zone should be regarded as a sanctuary of controlled operations.
It contains the Incident Command Post, responder staging, logistics, communications, medical treatment, transport coordination, and potentially casualty collection and evacuation functions. Joint CBRN doctrine emphasizes that this zone should remain clean and should contain command and support functions.
At night, however, the Cold Zone can itself become a vulnerability.
Brightly illuminated command posts can become highly visible. Vehicles may create traffic congestion. Ambulances may inadvertently enter the wrong area. Personnel arriving from different agencies may not understand the zoning system.
Consequently, the Cold Zone should have a clearly controlled access point and a distinct separation between clean and potentially contaminated personnel.
The principle should be simple: No person, casualty, vehicle or equipment should enter the Cold Zone merely because it appears visually clean.
Entry should be based on the operational contamination-control system.

Security and Force Protection

A CBRN incident in an urban environment may be accidental, deliberate or part of a broader security event. In the latter two circumstances, CBRN responders may operate in an environment containing an active or residual security threat.

The Hot, Warm and Cold Zones therefore have a security dimension in addition to a contamination dimension.
USFA guidance for hazardous and violent environments emphasizes that Hot, Warm and Cold Zones must remain dynamic and that security support requirements vary between zones.
At night, the security problem becomes more pronounced because hostile actors can exploit darkness, restricted responder visibility and predictable responder movements.
The solution is not simply to place more personnel around the incident. Security must be integrated into the CBRN command structure. CBRN teams, fire/HAZMAT personnel, EMS, police and medical authorities must share a common operational picture.
The CBRN responder should know where security personnel are located, while security personnel should understand the responder's contamination-control requirements.

Urban Navigation

Navigation is an underestimated problem during night CBRN operations.
A responder may enter through one street and exit through another. Smoke, darkness, and emergency vehicles can obscure landmarks. Building interiors may look almost identical. Underground structures can produce additional orientation problems.
Navigation should therefore be based on redundant systems rather than visual memory alone.
Digital mapping, GPS where available, pre-established route markers, illuminated identifiers, radio communication, and physical guides can provide complementary navigation systems. Indoor operations may require additional methods because satellite navigation can be unreliable or unavailable. The important principle is redundancy**:** if one navigation system fails, another must remain available. This is similar to the detection equipment principle: always use two pieces of equipment of two different technologies.

Communications

CBRN PPE already degrades communication. Masks and respirators reduce speech intelligibility; hearing protection can further impair communication; and urban structures can interfere with radio propagation. Night operations magnify the problem because visual confirmation becomes difficult.
Communication protocols should therefore prioritize short, standardized messages. Teams should establish predetermined words for entry, withdrawal, casualty identification, contamination findings, equipment failure, and emergency evacuation.
The ability to communicate a simple message such as "withdraw" or "PPE failure" rapidly may be more important than transmitting detailed information.
Communication should also include the Warm and Cold Zones. A casualty arriving at the decontamination area should not become an unexpected event for the medical team.

Vehicles and Medical Evacuation

Vehicle movement presents a significant contamination-control problem.
Ambulances, fire engines and logistics vehicles can become contamination vectors. A vehicle that enters the contaminated area cannot automatically be treated as clean when it exits.
Night operations increase the risk of collision, navigation errors and personnel being struck by vehicles. Vehicle routes should therefore be separated from pedestrian casualty pathways wherever feasible.
Medical evacuation routes should be planned around contamination control rather than merely around distance.
The fastest route to a hospital is not necessarily the safest route if contaminated patients or vehicles pass through uncontaminated areas.

Hospital Interface

The Cold Zone is not necessarily the final point of the operation. The contamination-control chain extends to the receiving hospital.

A hospital receiving potentially contaminated casualties must know whether patients have been decontaminated, whether contamination remains suspected, what agent is suspected, and what PPE is required.

Failure at this interface can transfer the incident from the field to the hospital.

This is particularly important at night because hospital staffing may be lower than during daytime operations, specialist personnel may be on call rather than physically present, and logistics resources may be reduced.

Consequently, night CBRN planning should include a hospital notification and contamination-status system rather than treating hospital evacuation as an ordinary ambulance transport problem.

The hospital's administration should consider the outdoors area as a Warm Zone where certain actions should be performed, including the management of the "worried-well" that are expected to flood into the hospital.

Lighting as a CBRN Operational Capability

Lighting should be considered an operational capability rather than merely an engineering requirement.

The ideal night CBRN site may require several lighting layers. General area lighting provides basic orientation. Task lighting supports decontamination and medical procedures. Low-level pathway lighting assists movement. Specialized illumination can support detection and identification equipment. Night-vision-compatible lighting can support tactical operations where required.

Lighting should also support zone recognition.

A responder arriving at a contaminated area should immediately understand whether they are approaching the Hot Zone, entering the Warm Zone, or reaching the Cold Zone.

The exact colors, symbols, and systems should be standardized within the responding organization rather than improvised at the incident.

Equipment Management

Night operations increase the probability of equipment loss or misidentification.

Gloves, masks, filters, detectors, batteries, medical supplies, illumination systems and communication devices can be dropped or misplaced. Batteries also become a critical logistics consideration because night operations depend heavily on electrically powered equipment.

The responder therefore needs more than a PPE inventory. There must be an energy and equipment continuity plan.

Spare batteries, lighting systems, communication equipment and detector power supplies should be available in the Warm and Cold Zones.

Equipment that has crossed into the Hot Zone must also be managed as potentially contaminated until appropriately decontaminated.

Responder Fatigue

Night CBRN operations frequently extend longer than initially anticipated.

A seemingly short operation can become prolonged because of detection uncertainty, casualty numbers, decontamination requirements, security restrictions or difficulties accessing buildings.

Protective clothing, respiratory protection, heat stress and physical exertion accelerate fatigue. Darkness adds cognitive stress.
Personnel rotation (shifts) should therefore be incorporated into the operational plan from the beginning.
The objective is not simply to have enough responders to start the operation. It is to have enough personnel to sustain the operation.
A responder who becomes cognitively impaired through fatigue is not merely less productive; they may become a contamination-control liability.
A senior responder should be tasked to monitor the well-being of those operating in the field and take immediate actions if any deviation from SOPs is recorded.

The Transition From Crisis to Control

The most important moment in a CBRN operation may be the transition from emergency response to controlled recovery. Initially, information is incomplete, and the Hot Zone may be expanding. Later, monitoring improves, the source is identified or isolated, casualties are removed, decontamination becomes established, and the boundaries can be progressively refined.
Night operations should not continue indefinitely under the assumptions of the initial emergency.
As knowledge improves, PPE requirements, zone boundaries, personnel assignments, and access restrictions may be modified.
OSHA guidance specifically emphasizes that zoning can change as contamination becomes characterized and that PPE decisions should be based on the evolving understanding of the hazard.
This represents an important operational principle:
The CBRN response should become progressively less uncertain as it progresses.
If uncertainty remains unchanged several hours into the incident, the problem may be inadequate detection, inadequate information sharing, or inadequate command and control.

A Conceptual Night CBRN Operational Sequence

A robust urban night operation can therefore be conceptualized as a series of controlled transitions. The first phase is recognition and isolation. The second is establishment of the initial Hot Zone and security perimeter. The third is reconnaissance and hazard characterization. The fourth is controlled casualty extraction. The fifth is establishment of the Warm Zone and decontamination corridor. The sixth is casualty triage and medical stabilization. The seventh is progressive transfer of decontaminated casualties and responders toward the Cold Zone. The eighth is controlled medical evacuation. The ninth is refinement of the contamination boundaries as additional information becomes available. The final phase is recovery, environmental assessment, equipment decontamination, and controlled termination of the response. At every stage, the same question should be asked: "What contamination can move from here to there?"
That question is often more operationally useful than simply asking where the Hot Zone ends.

The "Invisible Corridor" Concept

A useful way of conceptualizing night CBRN operations is the creation of an “invisible corridor”.
The corridor begins inside the Hot Zone and ends in the Cold Zone. Along its length, the responder, casualty, equipment, and information move through increasingly controlled environments.
The corridor consists of five fundamental components: hazard detection, physical movement, contamination control, medical care and command-and-control.
If any component fails, the corridor can fail.
For example, excellent decontamination is insufficient if contaminated casualties are subsequently transported through a clean area. Excellent

detection is insufficient if responders cannot communicate the results. Excellent medical care is insufficient if contaminated patients enter an unprepared treatment area. The CBRN response is therefore a system rather than a collection of individual tasks.

Conclusion

CBRN operations during the night in an urban environment represent one of the most demanding forms of emergency response. Darkness increases uncertainty, complicates navigation and communication, reduces visual confirmation and increases the probability of operational errors. At the same time, CBRN hazards may remain invisible, odorless, and spatially unpredictable.

The solution is not simply to increase lighting or deploy additional personnel. Effective night CBRN response requires the integration of CBRN detection, PPE, night-vision capability, lighting, security, communications, casualty management, decontamination, medical evacuation and hospital preparedness into a single operational architecture.

The Hot Zone must remain an area of controlled exposure and lifesaving intervention. The Warm Zone must function as a carefully managed contamination-reduction interface. The Cold Zone must remain genuinely clean and provide the command, medical, logistical and personnel-support functions required to sustain the operation.

Ultimately, the transition from Hot Zone to Cold Zone should be understood as a progressive reduction of both contamination and uncertainty.

During daylight, the environment provides information. At night, the response system must manufacture that information through detection, illumination, communication, navigation and disciplined procedures.

The central lesson is therefore straightforward: night CBRN operations are not daytime CBRN operations performed in darkness. They are a distinct operational problem requiring a deliberately designed night-capable system from the contaminated Hot Zone to the protected Cold Zone. Unfortunately, night CBRN drills are not part of the training curriculum worldwide, and when done, are only once annually or every two years. Repetition leads to proficiency, leading to confidence.

Bibliography

Civil Unrest Response: Operations. US Fire Administration. Available from https://www.usfa.fema.gov/a-z/civil-unrest-response/operations.html

Chemical Hazards Emergency Medical Management. Available from https://chemm.hhs.gov/onsite.htm

Key Planning Factors and Considerations for Response to and Recovery from a Chemical Incident. FEMA. Available from https://www.fema.gov/cbrn-tools/key-planning-factors-chemical/table-contents

C. Bensiam. NATO's Combined Joint CBRN Defence Task Force. CBNW/ NCT. Available from https://nct-cbnw.com/natos-combined-joint-cbrn-defence-task-force/

CBRN Joint Operating Principles (Version 2.0). JESIP. Available from https://www.jesip.org.uk/wp-content/uploads/2026/07/JESIP-JOPs-Synopsis-March-2026.pdf

Allied joint doctrine for chemical, biological, radiological and nuclear defence (AJP-3.8(A)). UK MoD. Available from https://assets.publishing.service.gov.uk/media/5bf40787ed915d18301589b4/archive_doctrine_nato_cbrn_defence_ajp_3_8.pdf

OSHA/NIOSH Interim Guidance – April 2005 – Notes on PPE Selection Matrix for Emergency Responders. REMM. Available from https://remm.hhs.gov/osha_niosh_cbrn_ppe.htm

Japan Cabinet Adopts Chemical Terror Plan; New Bodies Cannot Intercept Weaponized Drones

Source: https://www.techtimes.com/articles/325698/20260826/japan-cabinet-adopts-chemical-terror-plan-new-bodies-cannot-intercept-weaponized-drones.htm

Aug 26 – Japan's Cabinet formally adopted a sweeping counterterrorism action plan on Monday targeting chemical, biological,

radiological, nuclear, and explosive — or CBRNE — threats, including the creation of a new expert advisory panel and a dedicated cross-ministry intelligence body to track drones and artificial intelligence tools that could be weaponized by terrorists. The twin announcements mark the country's most significant restructuring of domestic counterterrorism architecture in recent years. But both new bodies are analytical and advisory in function — neither is empowered to detect, track, or physically intercept a commercially available drone carrying a chemical or biological payload over an urban area, which is precisely the threat Japan's own officials say they are preparing for.

The structural gap at the center of Monday's announcement — an advisory layer added to a threat that requires an operational response — is the defining tension of Japan's new counterterrorism posture.

Kihara Did Not Mince Words

Chief Cabinet Secretary Minoru Kihara convened Monday's Tokyo meeting at the Prime Minister's Office, issuing a direct warning to a country that has long operated under a cultural presumption of relative insulation from international terrorism. "We can't rule out the possibility that our country will be a target of terrorism in the future," Kihara told assembled officials, ordering relevant ministries and agencies to move quickly. His accompanying instruction to implement measures protecting the public from terrorism signals that Tokyo views the threat as both credible and urgent — not abstract or distant.

What makes the warning notable is what it is implicitly acknowledging: that the threat environment has shifted in ways the existing policy architecture was not designed to address.

Why Drones Change Everything the 1995 Doctrine Assumed

To understand what Japan is responding to in 2026, you need to understand what it responded to in 1995 — and why those two threat pictures are no longer the same.

On the morning of March 20, 1995, five members of the Aum Shinrikyo cult carried plastic bags of liquid sarin onto five Tokyo subway lines during rush hour, puncturing the bags with umbrella tips before exiting the trains. The 1995 Tokyo subway attack used an agent that was only approximately 30 percent pure, meaning the death toll of twelve people — and the more than 5,000 who sought medical attention, including 984 who were moderately poisoned and 54 severely poisoned — could have been catastrophically higher with a more refined synthesis. The attack exposed catastrophic gaps in emergency coordination: trains were allowed to continue on scheduled routes for roughly 40 minutes after the problem was first detected; hospitals near the affected stations received no official notification of what had occurred, learning the agent's identity from television approximately two and a half hours after the first victims arrived at their doors.

That attack became the baseline for Japanese CBRNE policy. And it was based on a specific threat model: a small group of attackers physically present on a transit system, carrying a liquid agent, operating on foot.

The 2026 threat model looks different. Agricultural spray drones — commercially available and capable of carrying liquid payloads in excess of 16 kilograms (35 lbs) — were originally designed for pesticide dispersal over large areas. As the Association of the U.S. Army noted in its foundational commercial UAV threat analysis, research and development of commercial unmanned aircraft systems for agriculture "demonstrate that this is now an accessible dual-use technology that can realistically deliver [chemical or biological warfare] agents." A credibly weaponized drone delivers its payload from altitude, at standoff, without requiring physical transit-system access or the attacker's physical presence at the dispersal site. That is not the threat Aum Shinrikyo's 1995 attack trained Japanese emergency planners to counter.

The CBRN Defense Market's June 2026 analysis put the shift bluntly: "The threat of chemical, biological, radiological, and nuclear (CBRN) attacks has never been more operationally relevant than it is in 2026" — specifically citing drone-delivered irritant agents on the Ukrainian battlefield as evidence the threat environment has fundamentally changed.

What Monday's Action Plan Actually Contains

The action plan is structured around four interconnected pillars:

An expert advisory panel composed of medical doctors, academic researchers, and former officers from the Self-Defense Forces and National Police Agency who previously held anti-terrorism portfolios. The panel is expected to be established to advise a prime-minister-headed antiterrorism headquarters that will be stood up in the event of an actual attack. Its function will be to assess potential damage and advise on countermeasures. This panel responds directly to the most widely documented failure of 1995: the absence of physicians or scientific experts in the command loop during the attack's first critical hours.

Strengthened intelligence functions. The plan calls for expanded collection and analysis of intelligence related to CBRNE threats. Officials have not publicly detailed which agencies will lead those efforts or what new authorities are being granted. Japan's new National Intelligence Bureau — launched on July 31, 2026, as the country's first centralized foreign intelligence coordinating body since World War II — provides the existing framework into which CBRNE threat intelligence can be routed.

Medical system improvements. The action plan includes provisions to

upgrade medical care infrastructure for CBRNE incidents, including securing critical medical supplies. This pillar draws directly on 1995: hospitals received no official notification about the subway attack and were forced to delay treatment protocols for hours.

A cross-ministry drone and AI intelligence tracking body. This is the plan's most forward-looking element. An interagency panel is set to collect and analyze information specifically on drones and artificial intelligence tools that could be weaponized for terrorist purposes. This body is intelligence-focused — tracking what exists, what is technically capable, and what is being acquired by potential threat actors. It is not an operational interdiction body.

What the New Bodies Cannot Do

Neither new entity announced Monday will have authority to physically detect a drone carrying a CBRNE payload over an urban Japanese city, track it through a dense radio-frequency environment that creates radar-detection challenges, and intercept it before it disperses its payload.

That capability sits in a different institutional domain. Japan's Self-Defense Forces are trialing vehicle-mounted laser systems under Kawasaki and Mitsubishi counterdrone contracts of ¥1.5 billion (approximately $9.4 million) and ¥1.9 billion (approximately $12 million) respectively. The Ground Self-Defense Force established new unmanned warfare offices in April 2026, primarily to institutionalize offensive and defensive drone use in military contexts. Japan and the United States conducted joint counterdrone training at Yakima Training Center in November 2025, focused on small UAS detection and interdiction.

All of this is military. None of it is directly linked to the civilian counterterrorism apparatus that Monday's action plan is designed to strengthen.

The gap is structural, and it is not unique to Japan. The National Tactical Officers Association's April 2026 whitepaper on UAS threats at public events specifically documents that CBRNE response capabilities at major public events must be pre-positioned on-site or within rapid-response range to address potential drones carrying hazardous payloads — because the detection-to-interception timeline for small commercial UAS in urban environments, with current civilian law enforcement tools, is inadequate if the response begins after the drone is already in flight.

Japan's new advisory panel will have expertise. Japan's new tracking body will have intelligence. What the action plan as announced does not specify is how those capabilities connect to an operational interdiction chain if a drone carrying sarin or anthrax is identified as airborne over a Japanese city.

A Policy Lineage, Not an Emergency Reaction

Monday's announcement did not emerge from a crisis. Under Prime Minister Sanae Takaichi — who took office in October 2025 and has made technology-driven defense modernization the organizing framework of her security agenda — the government reorganized an existing counterterrorism panel in January 2026 to begin considering further CBRNE measures, driven specifically by concerns over advances in science and technology. That January reorganization fed into the action plan adopted Monday, giving the new framework a more deliberate policy lineage than emergency-reactive measures would suggest.

Takaichi's broader security posture — codified in the 2026 Defense White Paper adopted by the Cabinet on August 4 — has consistently framed emerging technologies as both the central threat and the central opportunity of Japan's current strategic moment. The White Paper introduces a dedicated chapter on "new forms of warfare," highlighting drones and AI as central components of future military operations in Japan. The CBRNE

action plan sits alongside, and shares conceptual framing with, that broader military modernization — but the two operate in different institutional channels.

Takaichi's AI governance agenda is also relevant context. The Congressional Research Service's July 2026 Japan defense analysis documented that the Takaichi administration is preparing a revised national security strategy by end of 2026 expected to include AI as a defense planning pillar — a framework that will eventually need to account for AI-enabled drone threats in the domestic counterterrorism context as well as the military one.

Japan's Multilateral Track: From Quad to UN

The domestic action plan did not develop in isolation. Japan has been an active participant in precisely the multilateral counterterrorism architecture that has been raising alarms about commercial drone threats for the past two years.

The Quad Counterterrorism Working Group — comprising Japan, the United States, Australia, and India — hosted its second meeting in Tokyo in November 2024, conducting a tabletop exercise specifically on "countermeasures against the use of ICTs, chemical, biological, radiological, and nuclear (CBRN) agents and emerging technology for terrorist purposes." In September 2025, India hosted two Quad CTWG workshops specifically on "countering the use of unmanned aerial vehicles (UAVs) for terrorist purposes," as State Department's third CTWG statement confirmed. The third CTWG meeting, in New Delhi in December 2025, committed partners to a counterterrorism tabletop exercise focused on state-sponsored terrorism threats and uncrewed aerial vehicles — conducted in Australia in June 2026.

Separately, the UN Security Council Counter-Terrorism Committee Executive Directorate conducted a follow-up assessment visit to Japan from February 24 to 27, 2026, reviewing Japan's implementation of counterterrorism resolutions and examining specifically the role of information and communications technology in counterterrorism efforts. Monday's action plan is, among other things, a domestic institutional response to the pressure that multilateral engagement has been generating.

Can the New Machinery Prove Adequate?

The immediate task for the expert panel will be to stand up its advisory function and begin producing guidance for the prime-ministerial antiterrorism headquarters before a crisis forces improvisation. The interagency drone and AI tracking body faces the more open-ended challenge of developing collection and analytical frameworks for technology categories that evolve faster than policy typically can.

Both structures are advisory and analytical rather than operational. Their practical impact will depend heavily on how well their outputs feed into the agencies — the SDF, National Police Agency, Fire and Disaster Management Agency, and relevant ministries — that would actually execute a response. And it will depend on whether Japan develops, in parallel, the operational counterdrone layer that neither Monday's announcement nor the existing military drone programs directly address for civilian urban CBRNE scenarios.

For a country that spent decades treating terrorism as a distant foreign problem before 1995 forced a reckoning, Monday's action plan represents a further institutionalization of the lesson that preparedness cannot be deferred. Whether an advisory apparatus adequately answers a threat that requires interdiction capability is the harder question — and it is the one that Monday's announcement, for all its comprehensiveness, leaves open.

Frequently Asked Questions

What is CBRNE, and why does Japan's action plan single out drones and AI?

CBRNE stands for chemical, biological, radiological, nuclear, and explosive — a category of weapons and hazardous materials defined by their mass-casualty potential. Japan's policy has been shaped since 1995 by the Aum Shinrikyo subway attack, which used sarin delivered manually by attackers physically present on the trains. Drones and AI are specifically called out because they represent a delivery paradigm shift: a commercially available agricultural spray drone can carry liquid agents over 16 kilograms (35 lbs), disperse them from altitude across a wide area, and do so without requiring the attacker to be physically present. That is a fundamentally different operational challenge from the 1995 scenario, as documented in the AUSA's commercial UAS threat analysis.

What does the new expert advisory panel actually do, and who sits on it?

The expert panel is expected to be established as an advisory body to the prime-minister-headed antiterrorism headquarters that would be activated in the event of an actual CBRNE attack. Its membership will include medical doctors, academic researchers, and former officers from the Self-Defense Forces and National Police Agency with prior counterterrorism portfolios. Its function will be to assess potential damage and advise on countermeasures — filling the specific gap the 1995 attack exposed: there were no physicians or CBRNE scientists in Japan's emergency command loop during the critical first hours after the subway attack.

Can Japan's new drone and AI tracking body intercept a weaponized drone?

No. The cross-ministry body announced Monday is an intelligence function: it will collect and analyze information on drones and AI tools that could be weaponized for terrorist purposes. Detection, tracking, and physical interdiction of a commercial drone carrying a chemical or biological payload over an urban area is an operational problem that requires different institutional authority and different hardware — neither of which is addressed in Monday's announcement. Japan's Self-Defense Forces are developing counterdrone laser systems and have conducted joint US-Japan counterdrone training, but those capabilities are primarily in the military domain. The NTOA's April 2026 UAS whitepaper documents that the civilian counterterrorism CBRNE-interdiction link remains a gap in the architecture.

How does this action plan connect to Japan's broader defense buildup under Prime Minister Takaichi?

The CBRNE action plan shares conceptual framing with the Takaichi government's 2026 Defense White Paper, adopted August 4, which specifically identifies drones and AI as "new forms of warfare" requiring urgent attention. Takaichi's administration has simultaneously launched Japan's first centralized foreign intelligence coordinating body (the National Intelligence Bureau, July 31, 2026), enacted the country's most significant arms export reform in decades (April 2026), and is preparing a revised national security strategy that is expected to include AI as a defense planning pillar by year-end. The CBRNE action plan is domestic counterterrorism; the defense buildup is external; but both operate under the same framework that treats emerging commercial technologies — particularly drones and AI — as the central organizing challenge of Japan's current strategic moment, as Stars and Stripes reported.

Meet The 'Bottle Tree' Whose Sap Is Both Poison And Medicine

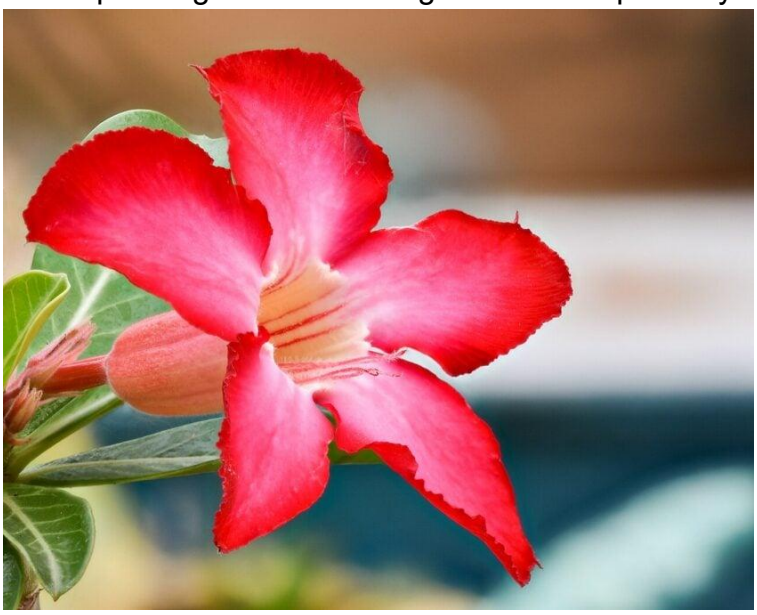
Source: https://www.sciencealert.com/this-tree-has-sap-so-toxic-it-causes-blurred-vision-and-can-kill-you

Aug 27 – The Socotra variety of the desert rose (*Adenium obesum*) looks like a tree that a child might draw. Its rounded, bulbous trunk, spindly branches, and brilliant pink blooms appear both otherworldly and too delicate for its home.

It is only found on the rocky landscape of Socotra, a Yemeni island in the Indian Ocean, where it's sometimes called the bottle tree.

Bottle trees on Socotra. (Rod Waddington/Wikimedia Commons/CC BY 2.0)

With a base that can grow to about 2.4 meters (8 feet) across, that name makes perfect sense – it looks like a giant soft-sided water bottle plopped down on Earth's surface.
That swollen form is an adaptation to life in a harsh, dry environment: The plant stores water in its enlarged trunk and roots.
After spending months looking like an exceptionally strange piece of desert architecture, it puts on a show. From early March through late April, Socotra's desert roses can erupt in striking pink-and-white flowers.



A desert rose flower. (Timothy A. Gonsalves/Wikimedia Commons/CC BY-SA 4.0)

It's a weird-looking plant – but its strangeness is more than skin-deep.
It's also medicinal. Ceremonial. And poisonous.
All five varieties of *A. obesum* grow in dry places: some are native to the Sahel regions south of the Sahara Desert, some to southern Africa, and others found on the Arabian Peninsula (like Socotra in Yemen).
But back to the poison: *A. obesum* belongs to the Apocynaceae family, known for containing latex and, in many species, biologically active compounds including cardiac glycosides.
The Socotra desert rose is no exception.

When it's injured, it produces a milky white latex, and that sap contains compounds that can affect the heart.

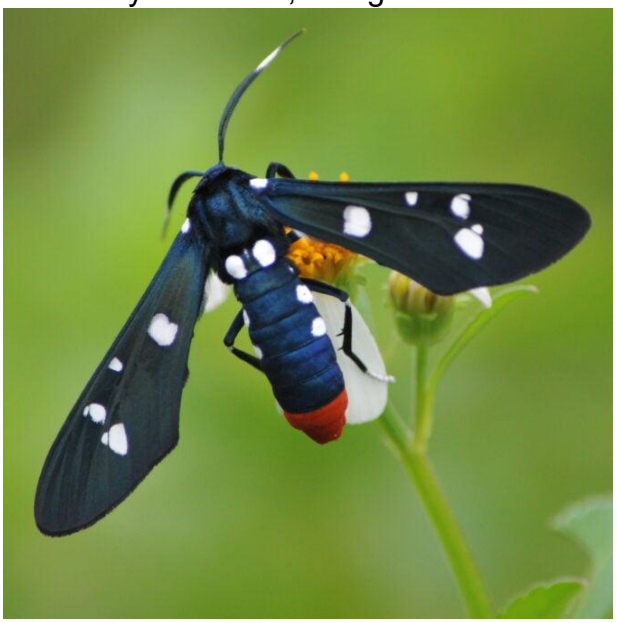
Those compounds are part of what makes this toxic tree so fascinating – and so dangerous. If consumed in small quantities, cardiac glycosides can increase the force of the heart's contractions while simultaneously slowing its rate, and so they can be useful for treating various kinds of heart failure.

The same chemistry that makes the plant potentially helpful for healing also makes it a poison.

In a perfect example of the old adage "the dose makes the poison," too much of the cardiac glycosides can cause vomiting, blurred vision, dangerously abnormal heart rhythms, and other potentially life-threatening effects.

That goes for both humans and animals.

In a well-documented case, a blue and gold macaw (*Ara ararauna*) – kept as a pet – ate the bloom from a desert rose houseplant and had an immediate, severe reaction that required 12 days of veterinary treatment, though it recovered.



In another contradiction, the polka-dot wasp moth (*Syntomeida epilais*) relies on the leaves of this poisonous-to-many plant for food when it's a caterpillar. It later repays the favor as one of the plant's primary pollinators, along with other nocturnal moths.

The polka-dot wasp moth is a primary pollinator of the desert rose. (Andy Blackledge/Wikimedia Commons/CC BY 2.0)

But again, poison can also be useful.

In northern Tanzania, for example, the Hadza have traditionally used *A. obesum* as an arrow poison for hunting animals including buffalo, zebras, giraffes and birds.

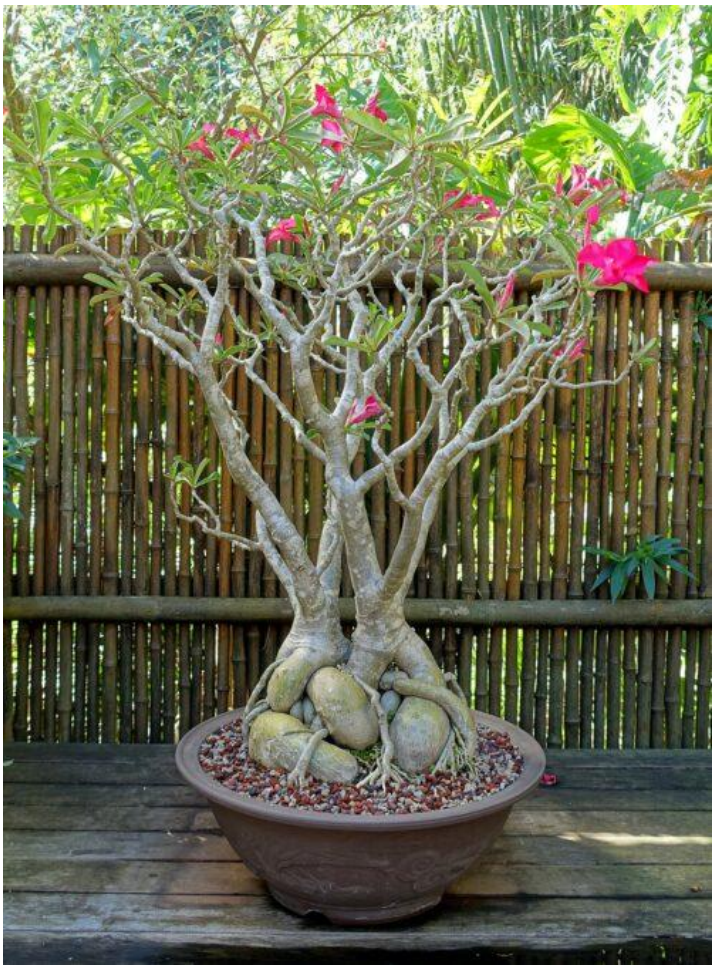
Other communities have used the plant to poison fish, pests and vermin.

A 2024 review of the plant's ethnobotanical uses found an incredibly wide range of applications. In different regions, people have used parts of the plant for skin problems, wounds, earaches, tooth decay, lice, and various infections.

The review notes that the seeds and roots are particularly potent sources of the plant's poisonous compounds.

Some communities have also used *A. obesum* in treatments for diseases including malaria and other parasitic infections.

Which of these treatments may be effective isn't clear, but researchers have identified dozens of compounds in *A. obesum*, some with reported antibacterial, antiviral, antioxidant, or anticancer activity.



One review identified 53 compounds from previous research, but also emphasized that some are toxic.
This wide range of uses may explain why the desert rose is also used in mystical or religious practices.
"The sap is believed to be efficacious in collaring illness caused by the evil eye, and is used as a protection tool against evil spirits and ill-wishers," write the authors of a 2020 review published in the *Journal of Medicinal Plants Studies*.
And of course, the desert rose is cultivated as an ornamental plant and prized not just for its flowers but for its bizarrely swollen roots, which can be shaped around rocks and into stunning bonsai.

Bonsai specimen in the Marie Selby Botanical Gardens - Sarasota, Florida, USA. (Daderot/Wikimedia Commons/CC0)

Its flowers have also been used in eco-printing, transferring natural pigments onto fabric.
In some Buddhist ceremonies, the stems, leaves, and flowers are used as offerings, while in parts of Indonesia the flowers are associated with cemetery visits and remembrance of the dead. The subspecies of the desert rose plant are not just one thing; they are many – beautiful flowering plants, living water tanks, a source of traditional medicines, ceremonial plants – and, under the right circumstances, a poison.

Responding to a Chemical Attack in a LSCO Fight

By Captain Alex T. Roan
Source: https://home.army.mil/wood/contact/publications/cr_mag-2/Immediate-Response-Force-Responding-to-a-Chemical-Attack-in-a-LSCO-Fight

Although nuclear weapons remain the most destructive weapons in the world, chemical weapons top the list of the most taboo and fear-inducing weapons of modern warfare. The use of chemical weapons violates multiple international treaties.[1], [2], [3] As such, the slightest possibility of a chemical attack draws worldwide distress. In response to this threat, President Joseph R. Biden attempted to make the U.S. stance against chemical weapons known by "drawing a red line" and explicitly stating that the United States would directly respond to any Russian use of chemical weapons against Ukraine.[4] If Russia decides to leverage chemical weapons, it will fall to the chemical, biological, radiological, nuclear, and explosives (CBRNE) Soldiers and commanders of Task Force 82 (TF82), 82d Airborne Division, Fort Bragg, North Carolina, to accurately assess and plan a ground response. As a TF82 company commander, responding to this possible chemical threat is the primary mission. The

CBRN Reconnaissance Platoon, Headquarters and Headquarters Company (HHC), 307th Engineer Battalion, 3d Brigade, 82d Airborne Division, which is under my command, allows our brigade to detect, assess, and confirm the presence of chemical weapons. This article highlights potential shortfalls in our tactical organizational design and in the equipment that our unit carries when responding to a chemical attack on a modern urban target within a large-scale combat operations (LSCO) setting.

A Polish CBRNE unit demonstrates the capabilities of an armored reconnaissance vehicle.

To understand this article, it is essential to understand what constitutes a current urban target, why a LSCO setting matters, and what capabilities are available. This article establishes tactics for emerging chemical attacks, describes our ability to respond with special equipment and techniques, and explains the deficits between theory and capability. This analysis assesses our capability to effectively respond to emerging scenarios and drive organizational change.

Assessing a Threat

Henry Kissinger aptly stated, "The more powerful the weapons . . . the greater the reluctance to use them."[5] While this sentiment generally holds true for nuclear weapons, it does not necessarily prove true for chemical weapons. Although the most prolific use of chemical weapons occurred during World War I, such weapons continue to plague the battlefield. However, the implementation of chemical weapons has become more sporadic; the tactics for employing these weapons have also evolved.

For the purposes of this article, overt chemical munition attacks by state level militaries are excluded from discussion. Such attacks would escalate far beyond company missions, and responses would likely be kinetic. Instead, this article examines a more likely, and potentially more damaging, scenario involving a subversive enemy employing chemical weapons to delegitimize the U.S. military.

I define a modern urban battlefield as city infrastructure capable of sustaining large populations and providing first-world commodities. This setting contributes to the complexity of chemical weapon employment due to the inevitability of the daily lives of a large number of civilians being suddenly interrupted by warfare. The establishment of this setting under the banner of a LSCO fight results in a posture that includes many government agencies, nongovernmental organizations, humanitarian aid, and modern Army equipment on both sides of the conflict.

The type of attack that I am most concerned about is one that would target civilians and military forces alike. An attack of this type would almost certainly aim to degrade the perception that the military was able to provide refuge to those fleeing the conflict. In the most sinister of scenarios, this might even appear to be the military's fault. These types of scenarios have occurred and have created a precedent for future implementation.

For example, during the Moscow Theatre hostage crisis in 2002, Chechen rebels stormed a theatre, taking more than 100 hostages; the Russians responded by pumping a gas mixture containing a lethal substance into the theater to incapacitate the hostage-takers, resulting in the deaths of more than 120 people.[6]

Russia's deployment of a lethal substance against

the Chechen rebels proves that certain substances weapon like this at a refugee center or a border crossing location under the guise of riot control could create a massive problem for our forces. Additionally, Russia could use a similar tactic to control riots within its own country, further legitimizing this application without risking an international response.

U.S. Army Soldiers decontaminate Polish soldiers during training.

Another example recently occurred in the Russia-Ukraine conflict but, fortunately, did not result in death. Heavy Russian shelling resulted in the rupture of ammonia storage tanks in the northern Ukrainian city of Rubejny, Lugansk Oblast, spilling toxic ammonia and causing nearby residents to seek shelter.[7] This scenario demonstrates that, under the right conditions, the enemy could improvise, creating a chemical weapon using civilian industrial chemical plants and effectively destabilizing an urban objective. This improvised tactic would actively combine toxic industrial materials (TIMs)- and artillery-based targets to form a TIM-artillery approach to urban-centric objectives. Although attacks like this can cause severe hardship to civilians and military personnel, they do not constitute the direct employment of a chemical munition and, therefore, do not cross that ever-diminishing red line.

Responding to a Threat

To understand how the 82d Airborne Division would respond to the scenarios described above, it is important to understand how TF82 mobilizes and postures. It is no secret that the 82d Airborne Division can deploy anywhere in the world within 18 hours, but that feat translates to a large force of very light paratroopers arriving armed to the teeth with little else to sustain or protect it. The TF82 CBRN Reconnaissance Platoon carries everything it needs to assess a target for the presence of chemical or toxic materials and decontaminate its members. The design creates two distinct mission-critical gaps in capability: the lack of superior-level capacity to investigate and determine the type of chemical compounds present and the inability to decontaminate a large population, including vehicles. To better convey the importance of capabilities, I would like to address each of the two scenarios described above and explain how the U.S. Army might respond.

In the first scenario, the toxic substance is employed in gas form in an urban center, killing more than 120 people. Most U.S. Army CBRN units carry organic equipment that will protect Soldiers from a gas threat, thus allowing continued operations in and around the target area. However, the TF82 CBRN Reconnaissance Platoon does not carry drugs that counter the effects of toxic substances. For that, it would be necessary to coordinate for outside support.

The CBRN Reconnaissance Platoon

has the tools necessary to take samples of any chemicals detected on-site and rely on coordination to determine definitive chemical presence based on sample chemistry. A tremendous higher-level asset that could bolster TF82 is the U.S. Navy preventative medical team. The team's Level 2 assessment capability applies to theater level rather than tactical-level decision making. The naval team can only support forward tactical operations if the assessment is time-consuming and would stall tactical operations. The naval team is not equipped to accompany a forward tactical element, meaning that all samples must be returned to a designated site that employs leak prevention measures. Once the analysis is complete, a diagnosis produces two outcomes—a treatment and a defense. Given limited time to respond, the tactical commander will be able to respond to a suspected chemical attack only by cordoning the area and tending to casualties. Once the catalyst is known, the ability to save lives depends on a higher level of medical care and the proper drugs for countering the chemical deployed.

In the ammonia spill scenario, the ability of the CBRN Reconnaissance Platoon to respond would be quickly degraded and dictated by the chemical concentration. TF82 cannot contain the spill or clean or decontaminate affected areas. TF82 has a containerized kit that includes a full-body encapsulation suit with a self-contained breathing apparatus (SCBA) for extended presence on an objective.

Recommendations

The underlying logic in determining the posture of the company commander, brigade commander, and TF82 commander to respond to a chemical attack depends on a precarious balance between threat assessment and budget constraints. The mission is highly fluid, and it would not be feasible to account for all possible attack vectors. Assessing the threat involves considering the likelihood of an attack and the potential damage it could cause. So far, the approach demonstrates a willingness to accept a high level of risk based on the unlikeliness of a chemical attack. However, the potential for significant casualties in such an attack remains.

Three levels of change could be implemented to better posture TF82 forces to respond to a chemical attack on military and civilian populations. I am not suggesting that we overhaul our force posture for the most dangerous course of action; rather, I propose an intermediate approach that aligns assets to set the stage for a response.

The first level of change would be the simplest to implement. Any potential for future operations must be aligned in Europe, so the U.S. Army should coordinate with the North Atlantic Treaty Organization (NATO) regarding any changes in the response to the threat of chemical warfare. NATO would benefit from this proposal due to the proximity of NATO allies to the frontlines. TF82 would also greatly benefit from receiving a second CBRN reconnaissance platoon as an attachment to HHC. This added workforce would allow maintenance of the same posture across multiple locations.

As the HHC commander responsible for the CBRN Reconnaissance Platoon, I am uniquely positioned to recognize that preparedness requires a shared understanding of higher-level assessment and treatment assets. This level and type of readiness are critical to TF82. Preparedness begins with posturing the necessary personal protection, detection, and medical treatment equipment in theater and ends with a rehearsal in which these assets are coalesced within an acceptable timeline. The second level of change would be to coordinate directly with emergency services in the host country. This change would allow a faster return on investment. Since the assessed scenarios take place in a modern urban setting, emergency services would be readily available. This option would enable the 82d Airborne Division to

circumvent the bureaucratic red tape that is linked to dealing with host nation armed forces and allow on-the-ground coordination. TF82 should attach a chemical decontamination company to its ranks to facilitate this option. This company would not be a part of the 82d Airborne Division and would need to come from an enabling unit. The challenge of coordinating the restructuring of TF82 to accommodate such a company would be outdone by the benefit of having a dedicated company to assess, plan, and respond to a chemical attack.

Polish soldiers conduct decontamination after a mission.

The third level of change would require a redesign of organic equipment and force composition. The addition of a dedicated chemical decontamination company is a concept that has been previously introduced, and the company even existed at one point. However, due to threat level, downsizing, and force restructuring, this asset was removed from the division. The strongest argument against this change is simple: We have not needed that company asset. However, I contend that the weaponry and the intensity of a LSCO battlefield warrant the return of this internal asset.

Conclusion

From my perspective, one of the keystones in responding to a chemical threat is the authorization for U.S. forces to engage. This type of authorization is weightier than an order for paratroopers to rush forward into an unknowable situation. Secondary effects must be considered. The 82d's current mission requirements do not exactly warrant the mobilization of massive supplies in preparation for a chemical attack; however, improving our posture is possible and is the responsible thing to do.

A LSCO war will test every level of readiness and stress the ability to adapt. The U.S. Army must continue to build shared understanding at all levels. Army leaders must accurately assess organizational design and how it relates to the enemy, constantly considering chemical weapons and how U.S. forces can respond to them. Tailoring the force posture to respond to chemical weapons (whether intentional or unintentional) within a city will be crucial. This posture must provide detection, assessment, diagnosis, and treatment capabilities. In any future conflict, the possibility that civilian populations would become a target for chemical weapons must be considered—and these crucial aspects will save military and civilian lives.

Urban battlefields hold a special place in the U.S. Army history; 100 years ago, the U.S. Army established military

dominance across European cities. Although the way we fight urban battles has been molded by the contemporary age, the daunting threat of chemical weapons remains eerily familiar and frighteningly effective.

Captain Alex T. Roan was the commander of Headquarters and Headquarters Company, 307th Engineer Battalion. He holds a master's degree in engineering management from Missouri University of Science and Technology at Rolla.

The CBRN Warrant Officer of 2030

By Warrant Officer One Alejandra Gallego

Source: https://home.army.mil/wood/contact/publications/cr_mag-2/The-CBRN-Warrant-Officer-of-2030

The U.S. Army is undergoing a significant modernization effort in order to prevail in large-scale combat operations and against its current near-peer adversaries. For the Army of 2030, it will strive to focus on reorganizing the force, modernizing equipment, and transforming the way it trains.

During my time in the Chemical, Biological, Radiological, and Nuclear (CBRN) Warrant Officer Basic Course, I was constantly challenged and enriched by different mentors who provided us with lessons learned and pointers, guided us toward success, and shared ways that we could positively impact our cohort. After graduating from the course, one particular question has lingered with me: What will the CBRN warrant officer of 2030 bring to the fight? Chief Warrant Officer Four Humphrey B. Hills, our Regimental Chief Warrant Officer, had posed that question during one of the many CBRN Warrant Officer Basic Course mentorship sessions.

The CBRN warrant officer of the next decade will play a key role in developing the Army of 2030 modernization strategy and achieving superiority over near-peer adversaries. We will be crucial trainers of specialized teams and integrators of new technologies covered in the Army 2030 strategic plan. We will be required to equip ourselves with extensive knowledge and fluently advise maneuver commanders concerning all warfighting functions. We will be subject matter experts in CBRN protection functions during all phases of large-scale combat operations and will possess unmatched skills for integrating CBRN capabilities across all multidomain operations. My futuristic view is one in which technology will be maximized to purposely engage and educate the Soldiers of 2030 and to understand their needs. Technological innovation during the next decade will play a vital role in how we train our force to use new equipment. Expanding on our current capabilities in military gaming by improving the ability to create simulated scenarios tailored to specific CBRN organizational training gaps could result in endless training benefits. Using virtual reality to simulate CBRN environments is the way ahead for training, based on the positive reception of the new generation of Soldiers to computer-generated reality. Warrant officers are critical for the effective modernization and integration of new equipment.

The Chemical Branch is now experiencing a significant equipment upgrade with the update to the Nuclear, Biological, Chemical, Radiological Vehicle (NBCRV) platform and many other progressive innovations aligning with the Army of 2030[1] strategy. We are mandated to master new-equipment operations and to be the driving force in training and adequately maintaining new equipment. I am honored to be a part of this ever-changing time in which, each day, CBRN warrant officers

spearhead the Chemical Branch into a more lethal, multiskilled, and technologically superior organization. The warrant officer of 2030 will be challenged daily, will thrive in virtual reality, and will offer unlimited value to any Army organization.

Warrant Officer One Alejandra Gallego is an assistant team operations technician for a CBRN response team, 501st Chemical Company, Camp Humphreys, Korea. She holds a bachelor's degree in health care administration from the University of Arizona Global Campus.

CBOA 22

By Chief Warrant Officer Three Macio E. Brown
Source: https://home.army.mil/wood/contact/publications/cr_mag-2/CBOA-22

The **Chemical Biological Operational Analysis** (CBOA) event, developed and executed by the Defense Threat Reduction Agency (DTRA), provides researchers an opportunity to elicit warfighter feedback during the technology development process of emerging chemical, biological, radiological, and nuclear (CBRN) capabilities for use in a realistic operational environment.

CBOA 22 was held at Eglin Air Force Base, Florida, in May 2022. In its role as the Joint Science and Technology Office (JSTO) for the Chemical and Biological Defense Program, Chemical and Biological Technologies Department, DTRA is the Department of Defense hub for chemical and biological technical expertise. The JSTO, which leads the defense community in preparing for chemical and biological threats, identifies and provides cutting-edge technology solutions to protect the security of the American people while empowering warfighters to achieve their missions in dangerous environments. The JSTO is responsible not only for protecting against the known threats of today but also for anticipating the major threats of tomorrow. In addition, JSTO provides science and technology support to the Department of Defense, other government agencies, and the international community.

DTRA sponsored more than 300 U.S. government, academia, and industry representatives as participants for CBOA 22, which addressed military capability gaps and high-priority mission deficiencies. During the week-long event, new CBRN-related technologies were assessed by capturing user feedback from all branches of the U.S. armed forces. Technologies were rated at technology readiness levels ranging from 3 to 8, based on four mission areas corresponding to the CBRN core functions: assess, protect, mitigate, and integrate command and control management. The assessment focused on the following characteristics of the technologies: performance, adaptability, ability to be integrated into the mission command common operating picture, digital security, environmental robustness, training burden, ease of use, task-load requirements for system operations, propensity for system malfunctions, routine maintenance burden, and logistical impacts. The event consisted of three lanes, which contained multiple operational scenarios to demonstrate the effectiveness of the technologies.

CBRN Protection 2030 and Beyond

According to Army Doctrine Publication (ADP) 3-37, Protection, "Many state and nonstate actors (including terrorists and criminals) possess or have the capability to possess, develop, or proliferate [weapons of mass destruction] WMD. The most likely adversaries during large-scale ground combat have significant WMD capabilities and the doctrine to employ them

during conventional operations. The training to conduct operations in a WMD environment is critical to operational success."[1] In order to achieve freedom of action, increase lethality, and enable movement and maneuver in the execution of large-scale ground combat operations in the complex CBRN environment, the Army must aggressively develop future CBRN defense capabilities to outpace our adversaries.[2]

U.S. Army Futures Command (AFC) Pamphlet (Pam) 71-20-7, Army Futures Command Concept for Protection 2028, builds upon the ideas of the multidomain operations concept and serves as the baseline for required CBRN protection capabilities to enable Army forces in multidomain operations through CBRN reconnaissance and surveillance, integrated early warning, real-time understanding, inherent survivability, and mitigation of CBRN hazards.[3] The key to successful all-domain protection includes improvement of artificial intelligence and machine learning for CBRN detection and mitigation capabilities. CBOA 22 highlighted breakthrough scientific discoveries and technological innovations that support the central idea of the core CBRN competencies (assess, protect, and mitigate) and the integrating activity of hazard awareness and understanding in support of the United States Army Chemical Biological Radiological Nuclear (CBRN) Science & Technology Strategy.[4] By employing capabilities that enable decision making and protect the force, commanders can sense, assess, understand, decide, and act faster and more effectively, thereby gaining an information advantage.

CBOA Technologies Overview

CBRN assessment capabilities enable commanders to understand the environment as early as possible so that they may make informed, risk-based decisions that protect the force while retaining freedom of action in a CBRN environment. The following assessment technologies were assessed during CBOA 22:

- **Dial-a-Threat Assay**—a hand-held, unpowered, human-readable biological threat identifier.
- **Biological Automated Collector/Detector for Expeditionary Reconnaissance (BioACER©)**—a fully automated biological collection and identification device that can be released from an unmanned aerial system (UAS) for remote analysis over a plume.
- **Falcon 4G©**—a 4th-generation laser-based CBRN standoff detector (which was used in a base defense scenario).
- **FentAlert©**—an all-environments screening assay for pharmaceutical fentanyl-based agents.
- **Far-Forward Advanced Sequencing Technology**—a technology used to identify deoxyribonucleic acid- or ribonucleic acid-based organisms.
- **Hazardous-material small UAS**—a UAS that is used to fly optimized patterns through hazardous areas, detecting, identifying, quantifying, and mapping hazardous data in real time, thereby enhancing situational awareness and improving decision quality.
- **MUSA P3I©**—a semiautonomous quadrupedal robot with integrated chemical and radiological detection/identification instruments that can also take photographs in the hot zone and conduct most CBRN reconnaissance/sampling missions.
- **NuGBall©**—a portable sensor network for real-time CBRN contamination mapping.
- **Pendar X10©**—a handheld standoff Raman spectroscopy chemical identification system used to identify unknown materials (liquid, solid, gel) at a distance of 1 to 6 feet within a few seconds (Figure 1).
- **Raman spectrometer**—a

spectrometer used to identify collected particles.

- **Rigaku©**—a portable handheld, dual-technology 1064-nanometer for the identification of chemicals and toxic industrial chemicals.

Figure 1. Pendar X10

CBRN protection capabilities enable inherent survivability (individual and collective) in support of large-scale combat operations, without degradation or loss of combat effectiveness in a CBRN environment. The following protection technology was assessed during CBOA 22:

- **Second Skin©**—a mask cover that is installed on a standard M50 mask to improve the protective garment hood and mask interface.

CBRN mitigation contributes to the negation of hazard effects by providing commanders the flexibility to make risk-based decisions about the mitigation of residual CBRN contamination without the reduction of combat power or unnecessary expenditure of time and resources. The following mitigation technology was assessed during CBOA 22:

- **Decontaminating skin soap**—a soap that is used to rapidly decontaminate sensitive equipment, materials, and skin from chemical warfare agents, biological warfare agents, toxic industrial chemicals, toxic industrial materials, nontraditional agents, pharmaceutical-based agents, and other emerging threats.

Digital Battlespace Command and Control Management

Digital battlespace command and control management systems provide CBRN staffs with the information required for commanders to make decisions with enhanced situational awareness and understanding in a timelier manner. Digital battlespace command and control management tools allow CBRN staffs to receive large amounts of CBRN threat information and intelligence, conduct analysis, and develop trends related to enemy CBRN employment. Technology developers presented the following capabilities during CBOA 22:

- **CBRN Analysis Software**—a commercial, off-the-shelf knowledge management application.
- **Multiintelligence-Enabled Discovery**—artificial-intelligence, machine-learning algorithms that use Azure Cloud© and Azure Cognitive Services© to provide near-real-time processing of multiple types of raw, unformatted environmental and intelligence data to provide intelligence insight and information to decision makers.

Conclusion

CBOA forges the future of CBRN modernization by showcasing experimentation, demonstration, and capability development for the joint force. Commanders need the ability to see the adversary, deny it anonymity, counter specific strengths, achieve positions of advantage, and expand and exploit gained areas. Lieutenant General D. Scott McKean, director of the Futures and Concepts Center, Army Futures Command, Fort Eustis, Virginia, prefaced his CBOA 22 speech on AFC Pam 71-20-7 by stating, “Looking forward, the Army must develop capabilities that can support and integrate with our joint, interagency, interorganizational, and multinational partners to expand the protection capability, increase capacity in competition, and operate at scale in armed conflict.” This guidance exemplifies the Army commitment to protecting the force, improving survivability, and reestablishing the readiness of forces through the development of modernized capabilities.

Chief Warrant Officer Three Macio E. Brown is a materiel development technician assigned to the Combating Weapons of Mass Destruction Branch, Requirements Determination Division, Futures and Concepts Center, Maneuver Support—Capabilities Development and Integration Directorate, Army Futures Command, Fort Leonard Wood, Missouri. He holds an associate of arts degree from Central Texas College and a project management professional certificate from the Project Management Institute.

New Yorkers were 'lied' to about toxic air after 9/11 attacks, says Mamdani

Source: https://www.bbc.com/news/articles/cjdvyk3pm27o

Sep 09 – Toxic air quality was being recorded in Manhattan soon after the 9/11 attacks even as officials played down health risks to the public, according to a trove of newly released files.

Asbestos was found "nearly everywhere" tested near Ground Zero, where the World Trade Center towers collapsed in 2001, New York City Mayor Zohran Mamdani said.

"People got sick because the leaders they trusted lied and told them they were safe to breathe in toxic air," he said, announcing the release of 170,000 documents related to the attacks.

Illnesses related to the dust and smoke from the towers' collapse have claimed more lives than the nearly 3,000 who died in the attacks, US health officials say.

Thousands of people have experienced health effects like cancer, including many who have died, after breathing in hazardous contaminants after the Twin Towers collapsed.

Speaking alongside Mamdani at Tuesday's news conference, TV host and 9/11 survivor advocate Jon Stewart said the new files show the city knew by October 2001 - a month after the terrorist attacks - that the air in Manhattan was toxic.

"So to be fair to them, they only buried that information for 25 years," he said sarcastically.
The records show asbestos was found near Ground Zero for months after the attacks at the same time people were being advised it was safe to go there.

The files, which include air-quality reports and communications among city officials, include October 2001 correspondence known as the "Harding Memo".
In it, an aide warned former Deputy Mayor Robert Harding that the city could face as many as 35,000 legal claims for its response to the attacks.
The document states that the city could be sued because health advisories caused individuals "to return to the area too soon (causing toxic exposure or emotional harm)".
City officials also told citizens to clean up dust and debris with "wet mops and rags" despite the presence of asbestos, which is only supposed to be cleaned by licensed professionals, according to another memo documenting the concerns of congressman Jerry Nadler.
The memo pointed to testimony from the city's top health official at the time saying a study had found "no elevated levels of asbestos in indoor air", but that tests showed dust had "low levels of asbestos in some samples".
The memo, attributed to Ester Fuchs, a special adviser at the time to Mayor Michael Bloomberg, acknowledged "potential problems for City Hall".
Days after the attack, city and federal officials - including the US Environmental Protection Agency (EPA) - declared that the air near the Twin Towers was safe.
Christine Todd Whitman, the head of the EPA at the time, later apologised for this declaration, saying the agency "did the very best we could at the time with the knowledge we had".
Tuesday's release of documents resolves a lawsuit brought by advocacy group 9/11 Health Watch, which sued after officials said they did not have the records.

City officials found 68 boxes of documents last year.
The pages of air quality reports and other records were released through an online portal timed for this Friday's 25th anniversary of the attacks. More documents are to be shared over the next year.
Karen Klingon, who was involved in the 9/11 Health Watch lawsuit, told the BBC on Tuesday her brother **Robert** (photo left) lived five minutes away from Ground Zero. He developed asthma, was later diagnosed with cancer and died at 61 of a related brain tumor. "There's a lot of research, probably, that can be done about what was in the air, and the kind of illnesses that derived of those toxins that were in the air, like what happened to my brother," she said. "Hopefully it helps people that were sick know and in the future."

Phil Alvarez, whose brother Luis Alvarez died of cancer in 2019 after exposure to Ground Zero toxins, told the BBC that **people "continue to get sick every single day, continue to die**".

Terrorists and Weapons of Mass Destruction: A History of Hype and the Possibility of a Dystopian Future

CTCENTINEL | September 2026, Volume 19, Issue 9

By Peter Bergen

Source: https://ctc.westpoint.edu/terrorists-and-weapons-of-mass-destruction-a-history-of-hype-and-the-possibility-of-a-dystopian-future/

The United States went to war against Saddam Hussein's regime in Iraq in March 2003 based on the false assertions of dodgy defectors and the faulty assumptions of U.S. policymakers that the Iraqi dictator had weapons of mass destruction that he might give to his allies in al-Qa`ida. None of this was true, but the subsequent invasion of Iraq and Iraqi civil war claimed the lives of some 200,000 Iraqi civilians[1] and those of 4,418 American service members,[2] and in the process greatly damaged global perceptions of American power and undermined faith in the U.S. government at home. This article will not rehash any of this well-documented history but instead will attempt to explain why senior Bush administration officials became preoccupied with the idea of terrorists deploying weapons of mass destruction (WMD) following the 9/11 attacks. The article will then examine the history of how terrorists experimented with WMD, producing only relatively crude weapons in the two decades that followed the 2003 invasion of Iraq despite much of the hyperbole surrounding the issue. It will then try to answer two pressing questions: Do advances in the fields of genetic editing and artificial intelligence change the game, so that what was once a fanciful notion—that terrorists might kill very large numbers of people with WMD—could become a bleak future reality? Does the history of hype about terrorists deploying WMD hold lessons that might be applicable today? The 9/11 attacks came as a complete surprise to senior Bush administration officials, even though they had received a stream of highly classified warnings from the CIA during the spring and summer of 2001 that al-Qa`ida was planning a large-scale attack, including possibly in the United States.[3] At the time, key Bush officials were so preoccupied by the purported threats posed by states such as Iraq that they discounted the notion that a non-state actor such as al-Qa`ida was a real threat. Underlining their preoccupation with state sponsors of terrorism, immediately after 9/11 senior Bush officials such as Secretary of Defense Donald Rumsfeld pushed for attacks against countries such as Iraq, which had concealed its active weapons of mass destruction WMD program during the 1980s.[4] After 9/11, the thinking of President Bush and his war cabinet was greatly influenced by the anthrax attacks in the United States that took just place just weeks after al-Qa`ida had attacked the World Trade Center and the Pentagon. During October 2001, letters containing anthrax were sent to American journalists and members of Congress, killing five people and shaping President Bush's understanding of the post-9/11 threat landscape, as they seemed to show that terrorists were now deploying WMD in the United States. The letters themselves contained the phrases "Death to America," "Death to Israel," and "Allah is great."[5] In fact, the FBI would eventually determine that Bruce E. Ivins, a biological weapons researcher working for the U.S. government who had access to highly secure biolabs, was solely responsible for the attacks.[6]

At the Bush White House, worries about terrorist access to WMD intensified

when the CIA discovered that before 9/11, Usama bin Ladin had met in Afghanistan with Dr. Sultan Bashiruddin Mahmood, a Pakistani nuclear scientist who had been fired from his country's nuclear program in 1999 because of his militant jihadi views. Bin Ladin had claimed to Mahmood that he possessed fissile materials suitable for a nuclear weapon, while Mahmood had shown bin Ladin a sketch about how to build a nuclear bomb.[7] Sketching a nuclear bomb design is a very long way from actually building one, and bin Ladin's boast about fissile materials was almost certainly false; instead, al-Qa`ida had very likely purchased quantities of radioactive waste. Still, Mahmood's meeting with bin Ladin indicated that al-Qa`ida's leaders were interested in learning about the most lethal forms of WMD and had connections to scientists who appeared to share their worldview.

After 9/11, al-Qa`ida's leaders stepped up their public rhetoric about their purported access to WMD. On November 8, 2001, bin Ladin told Pakistani journalist Hamid Mir, "I wish to declare that if America used chemical or nuclear weapons against us, then we may reply with chemical and nuclear weapons. We have the weapons as deterrent." This statement was followed in May 2003 by a *fatwa* from a militant Saudi cleric, Nasir bin Hamd al-Fahd, that gave religious sanction to those who wanted to use WMD on large numbers of American civilians.[8]

Vice President Dick Cheney became so concerned about the possibility of some kind of chemical or biological weapons terrorist attack that after 9/11, he kept a full biohazard suit on hand when he traveled.[9] Yet, if Bush administration officials had had more familiarity with the history of non-state actors using WMD, perhaps they would have been more skeptical that al-Qa`ida could pull off a large-scale attack with weapons of mass destruction.

The case of Aum Shinrikyo is instructive. A Japanese cult with tens of thousands of followers who subscribed to obscure, apocalyptic beliefs, Aum actively recruited from among the best and brightest in Japan and had access to hundreds of millions of dollars donated by its followers.[10] Despite recruiting scientists and possessing large-scale resources, when they manufactured sarin gas, a highly toxic nerve agent, they were able to kill only the relatively small number of 13 people in the crowded, enclosed environment of the Tokyo subway on March 20, 1995.

The Aum attack underlined that even terrorists with real scientific knowledge and considerable financial resources did not successfully build true weapons of *mass destruction*, although they could deploy weapons of *mass disruption* that could sow panic with relatively small-bore chemical or biological weapons attacks.

In one of the grimmer ironies of the war on terror, the Iraq War helped to create an alliance between some of Saddam's Ba'athist officials and members of al-Qa`ida, which resulted in the creation of al-Qa`ida in Iraq (AQI) that deployed crude WMD weapons. In other words, the Iraq War produced the al-Qa`ida–Ba'athist–WMD nexus it was supposed to prevent.

From late 2006 through mid-2007, AQI detonated a series of crude chemical bombs in Iraq that were designed to spread what they hoped would be lethal quantities of chlorine, widely available in the Middle East for treating water. The U.S. military killed or captured many of the insurgents who were deploying these bombs. Charles Faddis, who headed the CIA's operations against AQI's chlorine bomb network, explained, "There was a lot of effort to secure the chlorine, to get a hold of the tanks, to track these guys down (who were responsible for building the chlorine bombs) to kill them or capture them. Meanwhile the attacks are not being particularly successful. The people are dying in the blast, but fortunately nobody is dying from chlorine."[11]

Over time, AQI would morph into the Islamic State, which in 2014

seized much of Syria and Iraq. The Islamic State also experimented with WMD weapons, but again these were relatively crude chlorine-based devices. The group used these bombs dozens of times against the Iraqi military and Syrian Kurdish forces.[12] The Islamic State mounted a more ambitious chemical weapons effort between 2015 and 2017, producing mustard gas and adding the agent to bombs and rockets. Yet, they only produced mustard gas at relatively low concentrations, unlike the mustard gas that was used by the armies that fought during World War I.[13]

Overall, the Islamic State's chemical weapons efforts were not much more sophisticated than AQI's, although the Islamic State, a terrorist army of some 30,000 fighters, at one point controlled a population greater than that of New York City that it was able to tax and extort from at will.[14] At its height, the group's claims to be the "Islamic State" had some basis in truth, and yet even with its substantial resources and its large-scale recruitment of militants, including 40,000 jihadis from around the Muslim world, the Islamic State still could not create an effective WMD program.

During the post-9/11 period, several would-be terrorists hoped to create effective chemical weapons by manufacturing ricin. Ricin, which can be extracted from widely available castor beans, can kill, but only if it is deployed by those with real chemical weapons expertise, as it does not aerosolize well and must typically be injected directly for lethal effects. The most infamous case of ricin poisoning was that of the Bulgarian defector Georgi Markov, who was stabbed by a ricin-tipped umbrella in London in 1978 as he was waiting for a bus near Waterloo Bridge. Markov subsequently died, a death that was almost certainly the work of the KGB or an allied Eastern Bloc intelligence service.[15]

But in the hands of terrorists, ricin weapons were almost invariably duds. In 2003, an al-Qa`ida-linked militant based in the United Kingdom, Kamel Bourgass, attempted to produce ricin. So too did a Tunisian man living in Cologne in 2018, who was identified by German authorities as Sief Alla H., an Islamic State supporter.[16] In 2025, Indian authorities in Gujarat arrested a doctor linked to Islamic State Khorasan, the group's affiliate headquartered in Afghanistan, who was carrying castor bean mash suitable for making ricin.[17] In none of these cases did the militants deploy a ricin weapon.

All this history suggests that terrorists could not deploy true weapons of mass destruction because the barriers to entry were so high. But will those barriers be lowered now that we are in the age of AI and synthetic biology?

Militant groups often recruit educated young men, a demographic that is likely to understand aspects of these emerging technologies. In 2006, New America researcher Swati Pandey and I examined the educational background of 79 jihadi terrorists responsible for five major anti-Western terrorist attacks—the World Trade Center bombing in 1993, the bombings of two U.S. embassies in Africa in 1998, the September 11 attacks, the Bali nightclub bombings in 2002, and the London bombings on July 7, 2005. All those who had masterminded the attacks had university degrees. More than half the terrorists involved in them had attended university. Of those who attended a university, more than half had scientific or technical degrees, with engineering being the most popular subject studied.[18]

A dozen years after our study was published, sociologist Diego Gambetta and political scientist Steffen Hertog co-authored *Engineers of Jihad: The Curious Connection between Violent Extremism and Education*, which examined the educational background of 335[19] terrorists across the ideological spectrum, from jihadis to right-wing extremists to leftist terrorists. Gambetta and Hertog found that engineering was by far the most popular subject studied by the militants who had attended university, underlining that terrorists are often well educated with a scientific bent.[20]

Which brings us to recent developments in the field of AI: In August 2026,

Stanford University scientists announced that they had developed an AI program that had designed and made 16 new viruses. These viruses were not pathogens, but the study showed that entirely *de novo* viruses could now be made by AI. While there are plenty of reasons to celebrate that discovery—the viruses made by the Stanford scientists could be used to kill bacteria that cause disease—it also raises significant questions around biosecurity since *de novo* viruses are now an alternative path to making biological agents.[21]

Similarly, when it comes to chemical weapons, in 2022 North Carolina-based Collaborations Pharmaceuticals was contracted by the Swiss Federal Institute for Nuclear, Biologic and Chemical Protection to investigate whether AI systems involved in drug discoveries could generate thousands of novel chemical agents. Using the MegaSyn AI model, which was used to generate safe drugs, a scientist rewarded the model for finding toxic chemicals instead of safe drugs. Within hours, the model generated thousands of highly toxic potential new compounds.[22] That said, it is important to emphasize the word "potential." As Audrey Kurth Cronin pointed out in these pages four years ago, "generating a list of chemicals did not mean the results could be synthesized or would prove stable and effective. Pharmaceutical companies use the same method to create drugs; yet out of millions of compounds, they find few viable enough to enter into production."[23]

While much of the focus on the promise and perils of AI is on large language models (LLMs) such as Claude and ChatGPT that can provide detailed answers to a wide range of questions, additional AI tools known as biological design tools (BDTs) can be used to design novel organisms far quicker than any laboratory can.[24] Some BDTs are open source, such as AlphaFold, while others require expensive hardware such as Graphics Processing Units (GPUs) that can cost tens of thousands of dollars.

Could terrorist groups exploit these tools in coming years? As scholars Daniel Byman and V.S. Subrahmanian noted in July 2026, terrorists "are not technological pioneers in the conventional sense, but they are often capable adopters."[25] A similar skeptical note had been struck two months earlier in these pages by Andrew Glazzard, David McIlhatton, and Paul Martin, who pointed out that terrorists typically favor technologies that are both accessible and reliable.[26]

Indeed, the history of terrorism is rife with example of terrorists sticking with tried-and-true methods to murder large numbers of civilians, such as mass shootings, because they are relatively easy to do, especially in the United States where semi-automatic weapons are readily accessible. The most lethal terrorist attack in the United States since 9/11 was carried out by Omar Mateen, an American citizen inspired by the Islamic State, who killed 49 patrons at the Pulse nightclub in Orlando in 2016 using semi-automatic weapons. Mateen managed to kill around 10 times more people in his attack than Ivins had with his anthrax attacks, even though Ivins was one of the leading biological weapons researchers in the United States, while Mateen had no training from a terrorist group.

Vehicle ramming requires little skill and preparation. We have seen several of those in the United States since 9/11: an Islamic State-inspired terrorist killed eight in Manhattan using his vehicle as a weapon in 2017,[27] for instance, the same year a right-wing extremist rammed a protestor in Charlottesville, Virginia, killing her.[28] Early on New Year's Day 2025, an Islamic State supporter killed 14 people with a truck in New Orleans.[29]

By contrast, the science around creating *de novo* viruses is presently highly complex and requires special labs. That said, it is worth noting that, like the much of rest of the world, terrorists are increasingly using AI in their work. In a study of the Nigerian Boko Haram militant group published in July 2026, Antonia Juelich of Cambridge University interviewed 27 former members of the group and found that they had used AI to plan

attacks and design explosives. Islamic State members had also provided in-person AI training to the Boko Haram militants. None of this involved WMD research or planning, but it demonstrates that terrorists have moved beyond using AI to create propaganda and have now used these tools for operational planning.[30] There is an as-yet unsettled debate about the origins of the COVID-19 virus: Was it inadvertently leaked from a biolab in Wuhan, China, or did the virus cross over into humans from a nearby "wet market" selling exotic animals? This article does not take a position on that important debate, but if the Wuhan lab leak theory is in fact correct, it underlines the very real dangers of "gain of function" research that uses genetic editing to tinker with the traits of viruses, experimentation that was going on at the Wuhan biolab in question.[31] This points to how such gain of function research could be used for nefarious purposes; the massive global death toll and the calamitous economic and social consequences of the COVID-19 pandemic speak for themselves.

Among AI thought leaders, the possibility that AI tools could be used for gain of function research with nefarious intent is now a very real concern. Efforts to preclude that kind of research are built into closed American AI models such as ChatGPT, which are programmed with ethically based considerations that will, at least in theory, not allow the models to perform substantive research on how to manufacture WMDs.[32] In July 2025, OpenAI announced that it was introducing a new framework that explicitly guarded against any queries that were aimed at "bioweaponization."[33] The effectiveness of these guardrails is open to debate since there are ways to circumvent them if inquiries are posed in a deceptive manner, known as jailbreaks. In July 2026, this journal published research from the non-profit Tech Against Terrorism that queried 27 AI models about WMDs and found that 15 came up with information that exceeded what was publicly available, while a third gave "real assistance" to either make or plan a WMD mass casualty attack, a sobering finding.[34]

So where does that leave us? Senior Bush administration officials, caught completely by surprise by the 9/11 attacks, went into overdrive in the other direction and adopted a sky-is-falling approach to WMD that embroiled the United States in a disastrous war of choice in Iraq. During the quarter century since 9/11, terrorists have created and used chemical weapons, but with a scant record of success in terms of their lethality, despite all the hype around the topic of terrorists armed with WMD. We now stand on the brink of a new era, and the capabilities of AI and synthetic biology do present terrorist groups or individuals with idiosyncratic motives new tools to potentially create mass mayhem and murder. This feels like a dystopian reality rather than politicized hype, because it is AI industry leaders, not politicians, who are sounding the alarm about the issue. Demis Cambiss, who founded Google's DeepMind and won the Nobel Prize for Chemistry in 2024, as well as Sam Altman, CEO of OpenAI, warned publicly in June 2026 that some AI systems "now outperform PhD-level virologists on questions about highly technical laboratory procedures."[35]

Thomas Schelling succinctly observed in his preface to Roberta Wohlstetter's 1962 book, *Pearl Harbor: Warning and Decision*: "There is a tendency in our planning to confuse the unfamiliar with the improbable."[36] The United States discovered that to its cost on 9/11. Policymakers around the world must ensure that the fruits of the dual revolutions in AI and gene editing do not end up in the wrong hands, creating a weapon that might rival, or even eclipse, 9/11 in its impact on the world.

Peter Bergen is a vice president at New America, a professor of practice at Arizona State University, a CNN national security analyst, and the author of *All the Presidents' Wars: Twenty-Five Years of America's War on Terror* (New York: W. W. Norton & Company, 2026).

Investigation finds evidence of possible chemical weapons use in Sudan

By Eleonora Vasques

Source: https://www.euronews.com/2026/09/09/exclusive-investigation-finds-evidence-of-possible-chemical-weapons-use-in-sudan

Sep 09 – Former Organisation for the Prohibition of Chemical Weapons officials say they have found evidence that the Sudanese government may have deployed chemicals amid the country's ongoing civil war.

Acute respiratory distress, unusual odours, coloured explosive blasts, long term health problems, and environmental degradation are among the indicators that a group of experts has identified as credible evidence to support witness accounts of exposure to toxic chemicals linked to military activity in Sudan between 2024 and 2025.

The findings are described in a 32-page investigation, seen by Euronews, into the use of chemical weapons in civil areas in Sudan amid the ongoing war that started in 2023.

The investigation was led by former senior officials of the Organisation for the Prohibition of Chemical Weapons (OPCW), two of whom served with the organisation when it was awarded the 2013 Nobel Peace Prize for its work to implement the global ban on chemical weapons.

The two former senior OPCW officials leading the team talked to Euronews, but requested that their names remain anonymous due to the sensitive nature of the content.

“Given that at least one State Party has sanctioned individuals in relation to the alleged use of chemical weapons, that there are new and increasing allegations of a hidden programme, and that there is strong witness testimony indicating that there was an incident in September 2024 that may have involved chlorine, the OPCW and it’s States Parties need to launch an investigation,” the two former senior officials told Euronews.

The report cites the testimony of eight Sudanese witnesses, corroborated by video, pictures, and other digital material produced by the alleged victims, which indicates that chemical weapons might have been used in the conflict. Euronews reviewed the pictures contained in the report, but could not talk to the witnesses nor inspect their video footage or other digital evidence. This is not the first time that evidence has been produced indicating the possible use of chemical weapons in Sudan. Both the New York Times and the Washington Post published investigations in early September drawing on evidence provided by Middle Eastern intelligence, including pictures of stockpiles and correspondence among Sudanese officials. It was the alleged use of chemical weapons that led the US government to impose sanctions on Sudan in April 2025. But the investigation reviewed by Euronews adds both a human dimension and substantive grounds to the serious allegations, and is set to draw further attention. The Sudanese government has denied any wrongdoing on multiple occasions.

The report

According to the report, the team of experts interviewed eight witnesses in the Kenyan capital, Nairobi. Together, they identified "a number of credible incidents involving unexplained illness following military activity".

The group was composed of "individuals reporting direct exposure to alleged incidents, persons involved in emergency response activities, a healthcare professional who treated affected patients and individuals able to provide supporting documentary and digital material relevant to the investigation," the report reads. The strongest evidence were provided by two witnesses interviewed separately who were both present during an **incident at the Al-Jili Oil Refinery near Khartoum in September 2024.**

At the time, the area was under the control of the Rapid Support Forces, the leading group fighting against the Sudanese army that has been sanctioned by the EU and the US for serious human rights violations.

"Both witnesses described a military aircraft flying overhead immediately before the incident," the report says, listing "barrel-shaped objects associated with the overflight; impacts that did not resemble conventional explosive attacks; unusual airborne emissions; unfamiliar odours; acute respiratory symptoms affecting approximately twenty workers; treatment provided at the refinery medical clinic; subsequent change to vegetation close to the impact area".

It specified that the acute respiratory and ocular effects described by the two witnesses are consistent with exposure to an airborne irritant or hazardous chemical. However, the team of experts was not able to identify the substance.

The other testimonies report other incidents in different places with recurring patterns.

"Several witnesses described aerial attacks followed by the rapid onset of respiratory symptoms affecting those in the immediate vicinity," the report reads, explaining that the common described symptoms included "coughing, difficulty breathing, eye irritation and, in some cases, gastrointestinal or dermatological effects".

Similar to the witnesses at the oil refinery they also described "unusual odours, coloured airborne emissions and the apparent absence of the explosive effects normally associated with conventional aerial bombardment".

The team of experts could not conclusively confirm that the incidents were caused by the use of chemical weapons due to gaps that need to be filled in the findings.

However, they found credible and consistent evidence suggesting this may be the case, and have called on the OPCW to consider this evidence and pursue further investigation stemming from their preliminary findings.

According to UN data from April 2026, some 14 million people have been displaced since the Sudanese war began in 2023.

The conflict has also triggered what is widely described as one of the world's worst hunger crises, with nearly 19.5 million people facing acute food insecurity and famine conditions.

Euronews approached the Sudanese government for comment, but received no reply before publication.

EDITOR'S COMMENT: So, diagnosis based just on clinical reports! It reminds me the White Helmets in Syria operating with just a gas mask without PPE.

10.3 Japanese Abandoned Chemical Weapons: grievance as durable leverage


THE CBRN FILES
RICIN
ONE PLANT.
TWO VERY DIFFERENT WORLDS.
RICINUS COMMUNIS
THE CASTOR OIL PLANT
AVAILABLE IN PHARMACIES & STORES
CASTOR OIL
PHARMACEUTICAL GRADE
Used in medicine, cosmetics and industry.
RICIN
SCHEDULE 1 CHEMICAL CONTROLLED UNDER THE CHEMICAL WEAPONS CONVENTION (CWC)
Listed in CWC Schedule 1 (Item 1A(8)).
RICIN
SCHEDULE 1 CHEMICAL CONTROLLED UNDER THE CWC
SAME BIOLOGICAL SOURCE. COMPLETELY DIFFERENT RISK.
A HISTORY LINKED TO:
ASSASSINATIONS
TERRORISM PLOTS
SUSPICIOUS LETTERS
CASTOR OIL
A common, safe product used every day.
It does not contain ricin as a toxic component.
CBRN THREATS CAN BEGIN IN UNEXPECTED AND UNASSUMING WAYS.
DETECTION & FORENSICS
Critical for early identification.
MEDICAL RECOGNITION
Essential for appropriate care.
PREPAREDNESS MATTERS
Training, awareness and response.
INTERNATIONAL CONTROL
The CWC strengthens global security.
PROTECTING PEOPLE
From the unexpected, from the familiar.
DOES A NATURALLY OCCURRING SOURCE CHANGE HOW WE THINK ABOUT CBRN PREPAREDNESS?
STAY INFORMED.
STAY PREPARED.
THE CBRN FILES

MMSL Military Medical Science Letters

Mil. Med. Sci. Lett. (Voj. Zdrav. Listy) 2013, vol. 82(2), p. 46-54
ISSN 0372-7025
DOI: 10.31482/mmsl.2013.007

REVIEW ARTICLE

HOW MILITARY HOSPITALS GET READY FOR CHEMICAL WEAPON VICTIMS

Levent Kenar ✉, **Mesut Ortatatli**

Department of Medical CBRN Defence, Gulhane Military Medical Academy, Ankara, Turkey

Received 8th January 2013.
Revised 15th February 2013.
Published 5th June 2013.

Summary

The deliberate use of chemical weapons has emerged as a significant threat especially in last decades, mainly after the terrorist attack on 11th September 2011, and the use of these agents in future wars and terror attacks still remains a realistic concern. Despite the existence of many conventions and aggreements like Chemical Weapons Convention and 1925 Geneva Protocol against the use of chem-bio weapons, they have been used in many wars and conflicts. From this point of view, other than civilian state hospitals, military hospitals should be aware and get prepared to manage the victims injured due to chemical weapons. Military hospitals must be prepared to give support to health care system as well as military troops in treating and preventing casualties resulting from chemical weapons. Moreover, military hospitals are required to possess protective suits, masks, antidotes and other drugs. This article summarizes some important aspects which might be useful not only for military hospitals but also for civilian hospitals and public health organizations.

EUROJUST CBRN-E handbook

Source: https://www.eurojust.europa.eu/sites/default/files/assets/eurojust_cbrn_e_handbook_2017_en.pdf

The goal of this Handbook is to provide EU practitioners, in particular prosecutors and police authorities, with an overview of EU and international legislation applicable to CBRN (Chemical, Biological, Radiological and Nuclear) substances and Explosives and with a description of supranational entities, systems and databases active in the field of CBRN-E in support of investigations and prosecutions of transnational crimes involving the use of Chemical, Biological, Radiological and Nuclear substances and Explosives (CBRN-E).

Sixth version of the Eurojust CBRN-E handbook

The first two versions of the Eurojust CBRN-E Handbook listed in alphabetical order all relevant legal instruments and supranational entities, systems and databases. The third version brought a change in the structure of the Handbook, while the fourth and fifth version provided an update on relevant legislation dealing with CBRN-E substances.

Following from the structure introduced by the third version, this sixth version of the Eurojust CBRN-E Handbook provides a further update on relevant developments and legislation dealing with CBRN-E substances, namely:

- PIC Convention revised text of 2015;
- The Final Regulatory Action Evaluation Toolkit;
- The eighth and ninth amendments to Regulation (EC) No 1272/2008 on the Classification, Labelling and Packaging of Substances and Mixtures (CLP Regulation);
- The Inter-Organization Programme for the Sound Management of Chemicals;
- A number of relevant United Nations General Assembly and Security Council Resolutions;
- The United Nations Conference on Disarmament;
- The Decision 2014/504/EU implementing Decision No 1082/2013/EU;
- The Vienna Declaration on Nuclear Safety;
- The consolidated version of the Regulation No 98/2013;
- The consolidated version of the Directive 2008/68/EC;
- The Commission Directive 2016/970/EU of 27 May 2016 and the Commission Directive 2017/433/EU of 7 March 2017;
- The Commission Decisions 2014/955/EU and 2014/955/EU

SYSTEMATIC REVIEW

Gaps in Prehospital Care for Patients Exposed to a Chemical Attack – A Systematic Review

Stephane Bourassa, RN, MSc, PhD(c);[1,2,3,4] Emmanuelle Paquette-Raynard, MSI;[5] Daniel Noebert;[4] Marc Dauphin, MD;[4,6] Pelumi Samuel Akinola, BSc;[7,8] Jason Marseilles, RN;[7] Philippe Jouvet, MD, PhD;[1,2] Jacinthe Leclerc, PhD, RN[6,7,9]

1. Sainte-Justine University Hospital Research Center, Montreal University, Montreal, Quebec, Canada
2. Faculty of Medicine, Montreal University, Montreal, Quebec, Canada
3. Retired - Canadian Armed Forces Intelligence Service
4. Medical Intelligence CBRNE Inc., Quebec City, Quebec, Canada
5. Library Services, Laval University, Quebec City, Quebec, Canada
6. Retired - Royal Canadian Medical Service
7. Department of Nursing, University of Quebec at Trois-Rivières, Trois-Rivières, Quebec, Canada
8. Department of Nursing, Faculty of Health Sciences, University of Pecs, Pecs, Hungary
9. Research Center, Quebec Heart and Lung Institute – Laval University, Quebec City, Quebec, Canada

Abstract

Introduction: The survivability of mass casualties exposed to a chemical attack is dependent on clinical knowledge, evidence-based practice, as well as protection and decontamination capabilities. The aim of this systematic review was to identify the knowledge gaps that relate to an efficient extraction and care of mass casualties caused by exposure to chemicals.

Methods: This systematic review was conducted from November 2018 through September 2020 in compliance with Cochrane guidelines. Five databases were used (MEDLINE, Web of Science Core Collection, Embase, Cochrane, and CINAHL) to retrieve studies describing interventions performed to treat victims of chemical attacks (protection, decontamination, and treatment). The outcomes were patient's health condition leading to his/her stabilization (primary) and death (secondary) due to interventions applied (medical, protection, and decontamination).

Results: Of the 2,301 papers found through the search strategy, only four publications met the eligibility criteria. According to these studies, the confirmed chemical poisoning cases in acute settings resulting from the attacks in Matsumoto (1994), Tokyo (1995), and Damascus (2014) accounted for 1,333 casualties including 11 deaths. No study reported comprehensive prehospital clinical data in acute settings. No mention was made of the integration of specialized capabilities in medical interventions such as personal protective equipment (PPE) and decontamination to prevent a secondary exposure. Unfortunately, it was not possible to perform the planned meta-analysis.

2026 C²BRNE TERRORISM CONFERENCES

NCT APAC

20-21 October, 2026
Jakarta, Indonesia

PRO Asia

13-18 December 2026, Hua-Hin, Thailand

NCT USA

31 August - 3 September, 2026
Lorton (VA) & Edgewood (MD) USA

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.

Themes & Topics

- **Ecology and Epidemiology** – Global patterns and emerging risks
- **Detection & Diagnostics** – Innovative tools and forensic approaches
- **Pathogenesis** – Mechanisms of disease in animals and humans
- **Medical Countermeasures** – Vaccines and therapeutics
- **Decontamination & Remediation** – Strategies for safe environments
- **Biosafety & Biosecurity** – Risk management, policy and counter proliferation
- **Biosecurity Policy workshop -** MOD lead/ selected audience

Cranfield University

Source: https://cbrneworld.com/events/nitazene-workshop

Nitazene – Europe's latest synthetic opioid threat

Most European nations have been spared the devastation that fentanyl wreaked on the US. It not only killed tens of thousands, and ruined hundreds of thousands of lives, but provided challenges to law enforcement, fire hazmat and health professionals that encountered it. The toxicity of fentanyl is such that the US has categorised it as a weapon of mass destruction, and some of the analogues have a LD50 of chemical warfare agents. Now the same problems that US first responders and families had are going to happening in European cities with the advent of Nitazene.

Nitazene and its analogues are another synthetic opioid that poses a danger to life and health. The difference between an 'effective' dose and a lethal dose is incredibly small, and the individuals that are creating this narcotic are not skilled chemists. This one-day workshop will assess the threat from three angles, the detection of Nitazene, the decontamination of people and equipment and the health challenges should you encounter it. The Netherlands has a long history of illicit drug labs, and while it missed the fentanyl wave, they are seeing a worrying amount of Nitazene being shipped in. Organisations like the Netherlands Forensic Institute are excelling in detection and prosecution of these cases and will be a key partner in this workshop. This event is open to serving first responders, military, academics and scientific personnel from European and Nato partners.

Welcome Message

Dear colleague,
We are excited to welcome you as Co-Chairs of Qatar Health 2026!
This year's Qatar Health 2026 promises to be the nation's flagship event for health education OR advancement, spotlighting "Advancing Surgical Care Through Integration and Innovation." Join us from November 11-14, 2026, at the iconic Sheraton Grand Doha Resort & Convention Hotel for a landmark OR sentinel academic experience. Get ready for an inspiring scientific and educational program designed to spark new ideas, foster meaningful connections, and ignite collaboration throughout our Emergency and Trauma Surgery community. This year's Congress partners with the 13 th World Society of Emergency Surgery (WSES) Congress, the 2 nd World Congress of Trauma and Emergency Leagues (WCTEL), the 3 rd Eastern Mediterranean Trauma Round Table (EMTRT3), and the Advanced Trauma Life Support [ATLS] MENA Region 17 Meeting to create an unparalleled platform for scientific exchange and breakthrough discoveries in Emergency and Trauma Surgery and related fields.
This year, we invite you to join more than 2,000 healthcare professionals from Qatar, the Gulf region, and across the globe who will converge to share cutting-edge strategies, innovative research, and best practices in multidisciplinary care and surgical innovation. At the Congress, you will connect with thought leaders from Qatar and around the world—including experts from WSES, WCTEL, ATLS MENA Region 17, and the World Health Organization—who are driving transformative progress in emergency and trauma surgery. You will be inspired by renowned speakers, visionary industry leaders, and engaging educational sessions, all offering deep insights into emergency and trauma surgery, allied specialties, quality improvement, clinical research, medical education, and the exciting world of artificial intelligence. We look forward to welcoming you to this world class event.

Strengthening hospital preparedness for chemical, biological, radiological and nuclear emergencies: CBRN Hospital Preparedness Workshop

15 – 17 September 2026

Vilnius, Lithuania

Hospitals are at the forefront of responding to chemical, biological, radiological and nuclear (CBRN) emergencies. Preparing health facilities to manage these complex incidents while maintaining essential health services is critical to strengthening national health security.
On 15–17 September 2026, the WHO Regional Office for Europe, in collaboration with the Health Emergency Situations Centre of the Ministry of Health of Lithuania and national partners, will convene a 3-day CBRN Hospital Preparedness Workshop in Vilnius,

Lithuania. The workshop is implemented under the joint European Commission Directorate-General for Health and Food Safety–WHO/Europe CBRN Action.

Bringing together hospital leaders, emergency managers, clinicians, national authorities and international experts, the workshop will strengthen hospital preparedness using an all-hazards approach while focusing on the unique challenges posed by CBRN incidents. The programme combines strategic discussions with practical technical sessions covering hospital emergency planning, incident management, staff preparedness, personal protective equipment, decontamination, radiation protection, clinical management, mental health considerations and coordination mechanisms. Participants will also explore how hospitals can strengthen resilience through the 4S framework of health service delivery: System, Staff, Stuff and Space.

A highlight of the workshop will be a full-day interactive simulation using the internationally recognized Emergo Train System. Through a realistic radiological emergency scenario, multidisciplinary hospital teams will test decision-making, coordination, surge management, patient flow, contamination control and resource allocation in a safe learning environment. The workshop forms part of WHO/Europe's ongoing support to Member States to strengthen hospital resilience and enhance preparedness for high-impact emergencies, ensuring that health systems are better equipped to protect patients, health workers and communities during CBRN events.

In Memory of

Prof. Brig. Gen. Levent Karaca

Organized in collaboration between the CBRN Society and the Ankara Branch of the Clinical Biochemistry Association

THE FIRST PRACTICAL NBC (CBRN) COURSE FROM THE LABORATORY PERSPECTIVE

20–21 October 2026

University of Health Sciences,
CBRN Training and Simulation Center, Etlik – Ankara

Correct diagnosis, effective protection, and rapid response are of vital importance in confronting chemical, biological, and radiological/nuclear threats. With this understanding, the CBRN Society and the Ankara Branch of the Clinical Biochemistry Association will organize a special training program aimed at strengthening the role of all laboratory personnel in CBRN incidents.

The First Practical NBC Course from the Laboratory Perspective will bring together theoretical knowledge and hands-on training with the contributions of an important team of distinguished national and international academics and experienced instructors. The course aims to enable participants to recognize NBC (CBRN) threats, use personal protective equipment correctly, approach suspicious samples safely, assess contamination risks, and respond to incidents from a laboratory perspective.

The course is dedicated to the cherished memory of our esteemed teacher, Prof. Dr. Levent Karaca, who introduced the NBC concept to our country for the first time and established the related academic unit.

COURSE OBJECTIVES

- Recognize NBC/CBRN threats
- Use PPE correctly
- Approach suspicious samples safely
- Assess contamination risks
- Respond from a laboratory perspective

DIAGNOSE • PROTECT • SAVE

CEMEC
WINTER SCHOOL 2026

Health Security, CBRNe, Emergency Medical Teams and Disaster Medicine

Republic of San Marino • 23–25 October 2026

European Centre for Disaster Medicine
EUROPA

WHO Collaborating Centre
for Health Security, CBRNe, and the Emergency Medical Teams (EMTs) Initiative

UNIVERSITY OF THE REPUBLIC OF SAN MARINO
Center for Security Studies

TOR VERGATA
UNIVERSITÀ DEGLI STUDI DI ROMA
UNIVERSITY OF ROME "Tor Vergata"
Department of Electronic Engineering

OSDIFE
Observatory on Security and CBRNe Defence

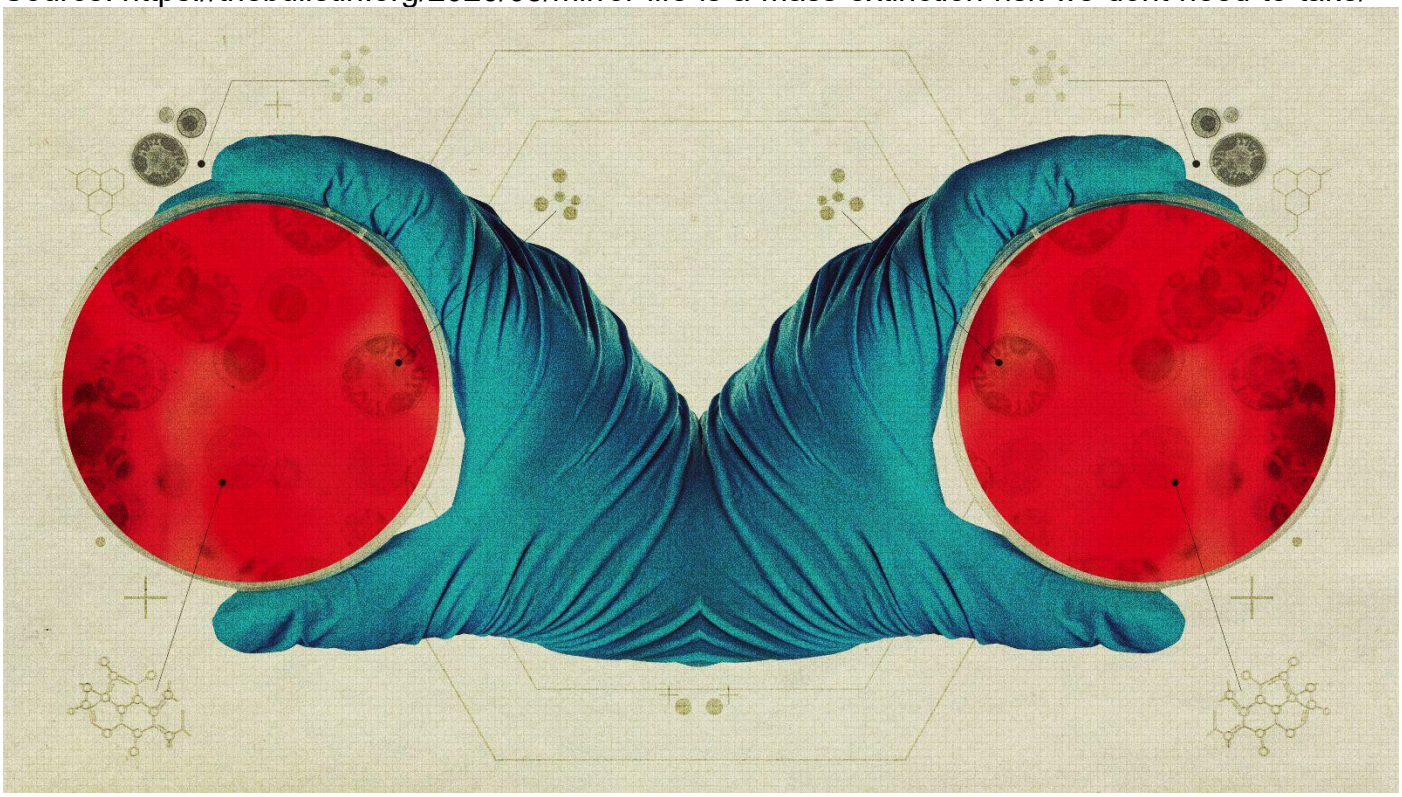
FOR INFORMATION:
CEMEC SECRETARIAT 0549-994535 cemec@iss.sm
WWW.CEMEC-SANMARINO.EU


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

Mirror life is a mass-extinction risk we don't need to take

By Georgios Pappas

Source: https://thebulletin.org/2026/08/mirror-life-is-a-mass-extinction-risk-we-dont-need-to-take/



Aug 21 – In 2024, dozens of prominent researchers wrote an article in *Science* that introduced the world to a dizzying concept: the existential perils of so-called "mirror-life," a type of organism based on molecular structures not found on Earth. The molecules and proteins that would make up these organisms could make for useful medicines or industrial materials. But a mirror bacterium, the scientists warned, could also lead to mass ecosystem destruction and extinction, because existing life forms would not have competed with it or evolved defenses to it. They called for a halt to any research that had the goal of making mirror life.

"Without effective predation and an accompanying increase in the number of predators, mirror bacterial populations could potentially reach very high densities, with extraordinarily damaging consequences for the environment, agriculture, and human wellbeing," the authors wrote, in a technical report accompanying the warning.

That was nearly two years ago. Since then, while no new regulations have been developed for mirror life research, scientists have met in Paris, California, Japan, and elsewhere to debate what should be done. Many have sided with the 2024 authors, a group that includes Nobel laureates, but not all. Ting Zhu, who researches mirror-image biology and believes the field has great promise in drug discovery and other areas, argued in *Nature* for being cautious about a pre-emptive ban. Stopping progress in mirror-image molecular biology would be the equivalent of banning work on "alternating current long before the electrification of cities," he wrote.

Zhu's views appear to be odds with leading experts and scientific bodies raising the alarm over the dangers of mirror life. The debate ultimately comes down to whether the potential benefits of mirror-life research outweigh the risks. They

don't. Though there's some reasonable speculation that mirror molecules may produce useful medicines and materials, and studying mirror biology could help answer fundamental questions of science, none of those benefits requires creating an actual mirror organism. Given the possibility that such an organism could cause existential harm, research that makes progress toward mirror life should be strictly regulated, and creating mirror life should be prohibited. Many experts have forcefully made this argument, but as of yet, no regulatory body exists to address the issue.

The significance of handedness

The units that make up life like proteins and amino acids have a specific handedness, or chirality: Most amino acids and all proteins are "left-handed." All nucleic acids, including DNA and RNA, are right-handed. Louis Pasteur, the famed French scientist who developed pasteurization in the 19th century, first outlined the concept of molecular handedness when he observed that sodium-ammonium tartrate crystals in a solution had slight differences on the left or on their right edge. Like the left and right hands, they mirrored each other but could not be superimposed on one another. Pasteur described the phenomenon as molecular dissymmetry.

Mirror molecules can have advantages in therapeutic drug development. Part of their appeal is that most forms of degradation in the body are chiral; a drug based on mirror molecules may persist longer in the body. Outside of medicine, mirror molecules may be useful in combatting climate change, as non-degradable materials, or in the food industry as non-absorbable sweeteners.

Is mirror-life feasible?

Cells are complicated structures, and building a mirror bacterium is not feasible at present. One would have to create a series of mirror proteins and nucleotides, assemble them in organelles, and structure them in three-dimensional form in a functional manner. Another approach may be to gradually replace or reproduce mirror forms of each cellular component in a normal cell. Both possibilities seem years or even decades away. But scientific leaps, either through novel approaches and techniques or through artificial intelligence assistance may make this distance significantly shorter.

Why would one want to build a mirror cell?

The chemical synthesis of the mirror molecules that might be useful as medicines remains burdensome and offers limited ability to create complex molecules. Mirror bacteria, on the other hand, might make efficient factories for creating mirror molecules, just as genetically modified cells can produce insulin for the treatment of diabetes. Mirror bacteria could be useful in other ways, too. Imagine a bacterium that could photosynthesize like carbon-absorbing plants and thereby help to combat climate change.

Lastly, developing a mirror life might help to answer questions about the origin of molecular handedness. How did the first organism, the last universal common ancestor (LUCA), evolve? Is life with a different handedness feasible, perhaps on other planets?

The risks

In the environment, natural bacterial predators such as viruses called phages use chiral features to attack bacteria. Not being subject to this predation, mirror bacterial populations might bloom endlessly, undetected by phages and resistant to attack.

In humans, the innate immune system, the first line of immune defense against microbial threats, relies on pattern recognition receptors that identify certain chiral molecules on invaders. The second line—the adaptive immune response that happens after infection or vaccination—produces chiral antibodies. Neither immune defense may recognize mirror bacteria or may not recognize them as efficiently as they do natural bacteria.

Instead of causing standard infections, mirror pathogens might act more

like cancer: a space-occupying lesion that uses bodily energy sources and for which we have no existing countermeasures. This could also happen to other forms of life, including animals and plants. Although the latter might be more resistant to such risks given that bark and other characteristics serve as strong physical barriers to internalization, their defenses might still be limited. Imagine mirror life slowly accumulating and covering such rigid living surfaces like sludge.
Through unimpeded growth, mirror cells could result in extinction events for animal species, crops, and whole ecosystems.

A ban?
Over the last year and a half, many scientists have echoed the 2024 call for a moratorium on mirror life research. Scores of researchers signed onto a statement seeking the establishment of "governance mechanisms capable of preventing the creation of mirror life." There have been statements or critical reports from the UN Secretary-General's Scientific Advisory Board, the World Health Organization (WHO), the Nuclear Threat Initiative (NTI), the China Arms Control and Disarmament Association (CACDA), the UK Government Office for Science, and Germany's Central Commission for Biological Safety, among others. The *Bulletin*'s Doomsday Clock incorporated the risks of mirror life in its current countdown. And the Mirror Biology Dialogues Fund emerged as a forum of further discussion of mirror life risks.
Some groups have advocated a "look before you leap" approach. "The field needs ways to pause and reassess research as it progresses down the multi-step process of creating a mirror cell," one group of authors wrote. An outright ban on technological research that could carry benefits might be harmful. "The key," the authors wrote, "is finding spots to stop the advance toward mirror life and create conceptual space to reassess."
More specifically, participants at the Paris Conference on Risks of Mirror Life in June 2025 identified four key technical milestones: a fully synthetic natural-chirality or mirror-image ribosome; a fully-defined, successfully "booted" synthetic natural-chirality cell; a mirror-image genome; and a so-called "PURE" system efficient enough to be self-sustaining. This is a non-cellular platform that can produce proteins if given the proper molecules and the proper energy sources; a self-sustaining one is able to self-produce the components of the platform (molecules) and the energy sources. Such systems are considered steppingstones in the creation of a synthetic cell.
Building a PURE system may have just been achieved. The first two steps outlined by the Paris conference are the most difficult, and creating a ribosome, the cellular structure where genetic instructions are translated into proteins, may be the most crucial step of them all. Achieving this would be particularly dangerous, a recent National Academies of Sciences, Engineering, and Medicine (NASEM) workshop found, because it might be "a viable pathway to self-replication" if a PURE system were incorporated into a cell.

The other side
As ban proponents look for research red lines, skeptics of a ban are continuing to raise questions about the need one: For instance, can we be confident that mirror life does not actually exist around us as a shadow biosphere? After all, scientists estimate Earth contains 1 trillion microbial species, almost all undiscovered. Or wouldn't mirror life, if it exists, already have come to Earth on meteorites?
Finally, given that nutrients also have a natural handedness, it's important to ask whether mirror life could even survive on a planet with food they might not be able to eat. A recent modeling study concluded that they might struggle to gain a foothold in Earth's ecosystems; they might be outcompeted by well-adapted natural organisms; and they might have limited access to suitable food. "Rather than being a passive environment," the authors wrote, "the

biosphere acts as an active and highly structured system that strongly constrains the establishment and spread of biological novelty, even the extreme case addressed in this work." Zhu, who leads a group advocating against a ban on mirror-life research, has been working on the creation of a mirror ribosome for years. He wants the mirror-life red line to be set at the creation of an entire cell. Some experts in Japan are also advocating for continued research toward mirror life. At a meeting of the Japanese Society for Cell Synthesis Research, "the floor discussion and the web survey made it clear that the majority opinion at this year's [meeting] was that there is no issue with the creation itself, provided the entities are controllable, such as fragile mirror artificial cells," according to a summary of the meeting in *Biophysics and Physicobiology*, a scientific journal. Attendees also argued for "rigorous management to contain mirror artificial cells" in labs.

In the absence of an international regulatory organization, like the International Atomic Energy Agency (IAEA), any restrictions will be difficult to implement. The "only way to ensure that everyone respects a red line is to make it impossible for anyone to cross on their own," said Gerald L. Epstein, an adjunct senior physical scientist at RAND and one of the participants in the National Academies workshop. To that end, RAND issued a report on a potential US strategy to prevent the creation of mirror life that proposes an agreement with China in order to avoid making mirror life research a geopolitical competition arena. RAND wants to have the countries prioritize transparency, scientific collaboration on the fine-tuning of where red lines stand, and an open sharing of risk assessment research on the subject. Is it a matter of life and death to scale production of medicinal or industrial mirror molecules with mirror cells? No, it's simply more cost-efficient to do so. Is it a matter of life and death to learn about how our asymmetrical life emerged? As a matter of satisfying scientific curiosity, yes. Is it a matter of life and death to avoid recreating a new tree of life of unknown behavior? Without what the *Science* writers called "compelling evidence" to the contrary, the answer is yes. Even in the long term.

Dr. Georgios Pappas is the *Bulletin*'s biosecurity editorial fellow. He is a physician from Ioannina, Greece; his research focuses on zoonoses (brucellosis in particular), epidemic preparedness, and social aspects of infectious diseases.

Novel Protective Antibody Target Against Crimean Congo Hemorrhagic Fever Virus Identified

FORT DETRICK, MARYLAND, UNITED STATES
United States Army Medical Research Institute of Infectious Diseases
Source: https://www.dvidshub.net/news/573071/novel-protective-antibody-target-against-crimean-congo-hemorrhagic-fever-virus-identified

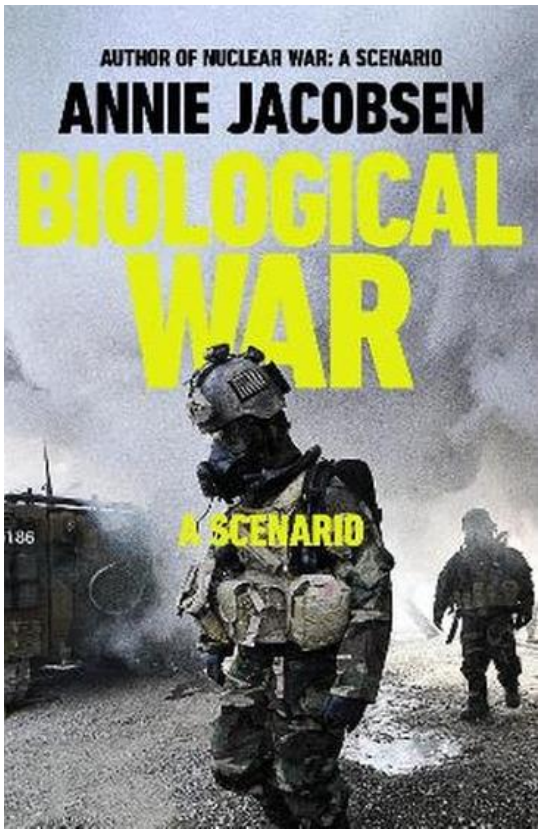
A research team led by the United States Army Medical Research Institute of Infectious Diseases has discovered an important protective antibody target against https://www.who.int/news-room/fact-sheets/detail/crimean-congo-haemorrhagic-fever, or CCHFV. Their work, which appears online today in the journal Nature Communications, could lead to the development of protective antibodies for infected patients. CCHF is considered a priority pathogen by the World Health Organization, or WHO, as it is an emerging zoonotic disease with a propensity to spread. It is also endemic in large portions of the world. CCHF outbreaks have a mortality rate of up to 40 percent. Originally

described in Crimea in 1944–1945 and decades later in the Congo, the virus has recently spread to Western Europe through ticks carried by migratory birds. The disease is already endemic in Africa, the Balkans, the Middle East, and some Asian countries. CCHFV is designated as a biosafety level 4 pathogen (the highest level of biocontainment) and is a Category A bioterrorism/biological warfare agent. There is no vaccine to help prevent infection and therapeutics are lacking. USAMRIID has worked with CCHFV going back several decades. During this work, the institute amassed an extensive collection of mouse monoclonal antibodies against CCHFV. However, suitable animal model systems to study antibody protection against CCHFV were only recently developed, some at USAMRIID. In a previous work, USAMRIID scientists Aura R. Garrison and Joseph W. Golden studied these collections of monoclonal antibodies in newly developed animal systems to identify a novel CCHFV therapeutic antibody target called glycoprotein 38, or GP38. GP38 was previously identified by the US Centers for Disease Control as a viral protein with unknown function. Here, Garrison and Golden explored the protective efficacy of a CCHFV monoclonal antibody targeting the nucleocapsid protein (NP). The scientists found that the NP targeting antibody protected mice against an otherwise lethal infection. This included providing substantial protection against a strain of CCHFV taken from a lethal human case. This work therefore opens another new direction for immunotherapeutics targeting CCHFV. The group is currently exploring the mechanism of protection of anti-NP antibodies. "We hope to combine antibodies targeting NP with those targeting GP38 to produce a robust immunotherapeutic cocktail that can protect humans," said Garrison. The antibody used for these studies is called MAb-9D5 and prior to this study was used as a laboratory reagent. NP is generally not thought of as a key target for protective antibody because it is buried withing the virus structure and not believed to be expressed in a manner accessible to protective antibodies. The work in this study revealed that NP is present on the surface of infected cells, which may be the reason why the antibody is able to provide protection. The University of California Riverside School of Medicine (led by Scott Pegan) and the US Centers for Disease Control (led by Éric Bergeron) joined in this study and showed that NP targeting antibodies can interact with NP from several CCHFV strains suggesting that this product could protect against most strains of CCHFV circulating throughout the world. "Exposure of hospital workers and overseas military service personnel to CCHFV is a major problem, therefore, an antibody-based drug that broadly protects prophylactically against existing strains of CCHFV, while also providing therapeutic protection is ideal," stated Professor Pegan. The research was funded by grants to Golden and Garrison from the Military Infectious Disease Program. Pegan (University of California Riverside School of Medicine & U.S. Military Academy) and Bergeron (Center for Disease Control) were funded with grants from the National Institutes of Health and the Department of Defense. Garrison and Golden were joined in the study by Vanessa Moresco, Xiankun Zeng, Curtis Cline, Michael Ward, Keersten Ricks, Scott Olschner, Lisa Cazares, Elif Karaaslan, Collin Fitzpatrick, Éric Bergeron and Scott Pegan.

Annie Jacobsen: Biological War

Source: https://www.commonwealthclub.org/events/2026-10-02/annie-jacobsen-biological-war

A bio attack. A lab accident. A global pandemic. The collapse of human society. Who else would want to explore the possibilities of biological warfare than Annie Jacobsen, investigative journalist and the best-selling author of *Nuclear War*? For her latest book, *Biological War*, Jacobsen interviewed dozens of experts in



politics, governments, medicine, and the military to explore a scenario of bio warfare. She says it would only take days from the beginning of a global bio infection before we'd be in a battle for human existence. Is the infrastructure that was

built to handle this very scenario up to the task?
How would people deal with a dystopian world with mass death, societal breakdown, violent insurrections, anarchy, and a plague-ravaged wasteland in place of modern civilization? Jacobsen lays out what would happen, providing a ticking-clock roadmap to the hours, days, and weeks following the release of a biological agent that serves as startling, forward-looking journalism in preparation for urgent societal upheaval.

Annie Jacobsen is a Pulitzer Prize finalist and New York Times bestselling author. Her books include: AREA 51; OPERATION PAPERCLIP; THE PENTAGON'S BRAIN; PHENOMENA; SURPRISE, KILL VANISH; and FIRST PLATOON. Her last book, NUCLEAR WAR: A SCENARIO, is an international bestseller. Her newest book, BIOLOGICAL WAR: A SCENARIO, hits bookstores everywhere on July 28. Jacobsen's books have been named Best of the Year and Most Anticipated by outlets including The Washington Post, USA Today, The Boston Globe, Vanity Fair, Apple, and Amazon. She has appeared on countless TV programs and media platforms—from PBS Newshour to Joe Rogan—discussing war, weapons, government secrecy, and national security. She also writes and produces TV, including Tom Clancy's JACK RYAN. Jacobsen graduated from Princeton University, where she was Captain of the Women's Ice Hockey Team.

Russia Restores Biological Weapons Research Facility on Lisyi Island

Source: https://militarnyi.com/en/news/russia-restores-biological-weapons-research-facility-on-lisyi-island/

Aug 21 – Russia has restored a biological weapons research facility known as the "Center for Experimental Physiology," located on Lisyi Island in the middle of the Vyshnevolotsk Reservoir in Russia's Tver Region.
The Defense Intelligence of Ukraine reported the development, while satellite imagery analyzed by Militarnyi also appears to confirm it.

According to the Defense Intelligence of Ukraine, the biological research facility was rebuilt on orders

from Russian President Vladimir Putin as a high-priority project aimed at "ensuring Russia's defense capabilities and security." The facility is under tight security, including protection by air-defense missile crews against potential aerial attacks.

The facility, officially known as the "Center for Experimental Physiology," is located on Lisyi Island in the middle of the Vyshnevolotsk Reservoir. The reservoir provides fresh water to several settlements, including the city of Vyshny Volochyok, and is also the source of the Tvertsa River, which flows into the Volga. Since 2023, the waters around the island housing the biological laboratories have been closed to fishing, swimming, and boating, having been designated a "specially protected area of regional significance."

Biological laboratories on Lisyi Island

An official historical account from the All-Russian Research Institute of Experimental Veterinary Medicine states that the facility was established in 1938 to conduct "acute experiments involving infectious diseases of farm animals." Today, the facility appears within the structure of the "Center for Strategic Planning and Management of Biomedical Health Risks" under the name "Center for Experimental Physiology." It is subordinate to Russia's Federal Medical-Biological Agency.

In May 2026, the Russian Federal Medical-Biological Agency posted a vacancy for a laboratory assistant whose duties explicitly included working with pathogenic biological agents belonging to Groups I–IV. Under the Russian classification, Group I biological agents cause particularly dangerous and fatal infections that are easily and rapidly transmitted from person to person. Effective means of prevention or treatment are either unavailable or limited.

Lisiy Island had appeared in U.S. intelligence documents as a possible site of the Soviet biological weapons program since at least the 1950s. A declassified index of CIA reports from 1957 contains the entries "Lisiy Island BW Research Facility" and "Lisiy Is[land] BW Research" – "biological warfare research facility on Lisiy Island" and "biological warfare research on Lisiy Island."

The island is also mentioned in the 1961 CIA report The Soviet BW Program. It described a branch of the All-Union Institute of Experimental Veterinary Medicine on Lisiy Island as one of the facilities that U.S. intelligence associated with the Soviet biological weapons program.

According to an analysis by Militarnyi of publicly available satellite imagery, the laboratory complex gradually fell into disrepair throughout the 2000s and 2010s. The buildings progressively deteriorated, with no signs of repairs. However, in 2022, Russia began a large-scale reconstruction, demolishing the old buildings and constructing modern laboratories.

At the beginning of 2022, the Russian company ABT-GROUP received a contract to manufacture load-bearing steel structures for the reconstruction of the laboratory and testing facility. That same year, the design, construction, and connection to the power grid of three new packaged block transformer substations were carried out for the laboratory and testing facility.

In 2022–2023, the company PIRS GROUP carried out work as part of the construction of a new research center of the Russian Federal Medical-Biological Agency on the island. The contractor equipped 1,200 m² of GMP Class C–D cleanrooms and installed the same area of conductive and commercial linoleum.

In October 2024, it became known that Russia had begun restoring and expanding a biological weapons research center in the Moscow region, which had been the Soviet Union's main research center for biological weapons, viruses, and other biological agents during the Soviet era.

The Fight against Biological Weapons

Source: https://www.diplomatie.gouv.fr/en/the-ministry-in-action/action-for-peace-and-respect-for-human-rights/security-disarmament-and-non-proliferation/disarmament-and-non-proliferation/the-fight-against-biological-weapons

Jan 2026 – While the use of biological weapons dates back to ancient times (there are examples of epidemics being intentionally caused as early as antiquity), it was during the 20th century that advances in biology enabled the development of vectorized bioweapons, tested in certain theatres of operations (by Japan in Manchuria in 1932 and 1933, for example).

Currently, in light of the development of science and technologies applied to biological and biomedical research and the pharmaceutical industry, along with advances in genetics and nanotechnologies, this threat remains a highly relevant issue.

International instruments on biological disarmament and non-proliferation

1925 Geneva Protocol

After the end of World War I, the international community understood the danger of biological weapons and created the 1925 Geneva Protocol. This text, which concerns "the prohibition of the use in war of asphyxiating, poisonous or other gases, and of bacteriological methods of warfare", remains fully relevant today.

France is the depositary of the 1925 Geneva Protocol, which is conserved in France in the diplomatic archives of the Ministry for Europe and Foreign Affairs. In 1996, France, like nearly all of the signatories, withdrew the reservations it attached when it ratified the Protocol, concerning the possibility of using such weapons in retaliation.

The 1925 Protocol relates more to humanitarian law and the law of war than disarmament law. It does not provide for the prohibition of chemical and biological weapons, but rather prohibits their use in war.

1972 Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction

This convention, also known as the Biological Weapons Convention or BWC, is the main legal tool for preventing the proliferation of biological weapons. The BWC established the legal bases for banning biological weapons and currently has 187 States Parties.

France became a State Party to the BWC in 1984. It previously considered the absence of verification measures to be an obstacle to the text's implementation. However, it adopted domestic legislation in 1972 incorporating similar provisions to the obligations stipulated in the BWC.

Strengthening the BWC and improving its implementation

Since its ratification of the BWC, France has worked tirelessly in support of strengthening the Convention's regime and authority and improving its implementation. In 2019, it chaired the BWC Meeting of States Parties.

Organization

In the absence of verification measures, compliance with the ban remains subject to the good faith of the States Parties. Every five years, a review conference is held, responsible for making the main decisions concerning the BWC. Meetings of States Parties are also held annually in Geneva, with the aim of finding common viewpoints on ways to improve the implementation of the Convention. The Working Group on the Strengthening of the BWC meets twice per year. In addition to the States Parties, these meetings can also include observers.

Recent developments

During the Ninth Review Conference held in November and December 2022, the States Parties agreed to establish a new intersessional programme, responsible for developing recommendations, including legally binding measures, to strengthen the Convention in all its aspects:

- International cooperation and assistance (Article X of the Convention)
- Scientific and technological developments relevant to the Convention
- Confidence-building and transparency
- Compliance and verification
- National implementation of the Convention
- Assistance, response and preparedness (Article VII of the Convention)
- Organizational, institutional and financial arrangements

  The Working Group is responsible in particular for establishing a mechanism for international cooperation and assistance (Article X) and scientific and technological developments relevant to the Convention.

France's position

Faced with the major risks posed by biological weapons, France is working resolutely to ensure the credibility and

effectiveness of the prohibition rules, by implementing the following actions:

- Taking an active part in the meetings of the Working Group on the Strengthening of the BWC, to ensure that the international community remains attentive to biological proliferation issues and to advance consensus on ways to strengthen and effectively implement the Convention.
- Annually submitting confidence-building measures for the BWC and encouraging States who have not yet done so to submit them. Confidence-building measures are annual reports submitted by States Parties on their activities in relation to the BWC (biological research, scientific development, etc.). Their submission is politically binding, meaning that biological activities developed in the country must comply with the terms of the Convention (prohibition on developing biological weapons, for example).
- For France, this reporting mechanism is essential to the BWC. It increases transparency and improves confidence between States Parties to the Convention.
- Working to establish a peer review mechanism through voluntary transparency exercises carried out in different regions of the world.
- Ensuring compliance with export control measures.
- Supporting the BWC Implementation Support Unit (ISU), which carries out activities to promote universal membership and support the implementation of the BWC.
- Promoting the SecBio platform, which aims to improve the overall level of biosafety and biosecurity of practitioners and facilities by centralizing all national and international standards and practices within a single platform to make them available to all States Parties. In addition to its database function, SecBio offers a training feature in the form of learning modules, as well as a forum to facilitate direct exchanges between experts.
- Making the BWC universal: through its diplomatic network, France is taking steps to raise awareness among States that have not yet joined the BWC about the Convention's objectives and principles.
- Taking practical action to combat proliferation through the G7-led Global Partnership Against the Spread of Weapons and Materials of Mass Destruction. In 2011 in Deauville, the G8 Leaders decided to renew the Global Partnership and widen its goals, notably making biosecurity a major priority. France has undertaken several projects in this field.
- Conducting numerous assistance projects and programmes in the field of public health and the fight against infectious diseases.
- Actively supporting European initiatives for disarmament and the fight against biological proliferation. These initiatives include the launch of EU regional centres of excellence aimed at spreading European best practices for controlling chemical, biological, radiological and nuclear (CBRN) threats. France is an active participant.
- Supporting the UN Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons (UNSGM), of which independence is a key principle, in the event of allegations.

France's biodefence programme

For a number of years, France has been pursuing biodefence programmes designed to improve the protection of civilian populations and military forces deployed in the field against potential biological attacks. These programmes are carried out in strict compliance with the Biological Weapons Convention. Biodefence programmes to protect military forces have two components:

- epidemiological surveillance systems, in complement to the WHO global surveillance network, and means of detecting biological agents in the environment;
- biomedical protection capabilities against certain biological agents, including vaccines, antibiotics, serums and antidotes.

The capabilities developed can be used to protect civilian populations on French territory, in response to the risk of bioterrorism, for example. They contribute to the effectiveness of the global health security strategy developed by the WHO, taking into account challenges related to infectious and emerging diseases.

Biological safety and security

- **Biosafety refers to a set of standards and procedures** that define all aspects related to the protection of workers and the environment against the accidental dissemination of biological agents. Technologies used to ensure the containment of pathogens (filters, sealed containers, etc.) contribute to biosafety.
- **Biosecurity refers to the procedures that aim to prevent the voluntary dissemination of pathogenic agents** (through theft, misuse or other malicious acts). In an intense epidemiological context (SARS, avian influenza, H1N1, Ebola, COVID-19), the security of biological facilities is a major concern.

A set of procedures to ensure the traceability of all laboratory operations (from site security and access control to operations involving equipment and pathogens) are therefore put in place. Measures also include identifying and avoiding sources of involuntary error. This process can help identify a malicious act.

Within the framework of the G7 Global Partnership, France has offered its assistance in the area of biosafety and biosecurity. In recent years, France has carried out several cooperation projects in this field, in particular in Georgia and Azerbaijan. Strengthening biosafety and biosecurity standards is an effective way to fight against biological proliferation.

AI and the New Age of Bioweapons

Preparing for a World of Synthetic Pathogens

By Beth Sherwood-Randall

September/October 2026 Published on August 18, 2026

Source: https://www.foreignaffairs.com/united-states/ai-new-age-bioweapons-sherwood-randall

Pathbreaking scientific discoveries can create transformational possibilities. They can also create catastrophic risks. The integration of artificial intelligence, biotechnology, and bioengineering is already enabling life-changing achievements, from combating disease to supercharging agricultural productivity to solving energy challenges. But it is also generating capabilities that can be weaponized more easily than ever by a growing number of actors. The United States is unprepared for these threats.

In the foreseeable future, a terrorist group with minimal skills could access a jailbroken AI model (one that has evaded safety controls) trained on the world's most comprehensive biological data set. The group could use the model to design a new strain of H5N1 avian influenza that is more lethal and more easily spread from animals to humans than existing strains. Connecting remotely to one of the new generation of fully equipped, contract-for-service "cloud" labs, it could anonymously arrange for the virus to be built and tested and then sent to a biomanufacturing facility to be produced at scale. From there, the group could stealthily disperse the new strain through air-handling systems at major livestock farms across the United States.

Before long, the American poultry, beef, and dairy industries would suffer massive losses. When the virus inevitably jumped to the human population, it would cause severe illness and could result in hundreds of thousands or even millions of deaths. The

response from U.S. public and private institutions—lacking both an integrated strategy and adequate tools—would be too slow, too uncoordinated, too underresourced, and too overwhelmed to stop the spread and mitigate the consequences. And soon, the virus would also cross borders, triggering food insecurity, widespread sickness, and mass casualties around the world.

U.S. policymakers have long contended with the possibility of biological attacks from hostile nation-states. Along with surveillance and global risk-reduction initiatives, Washington successfully deterred such attacks with the threat of significant retaliation, including the use of nuclear weapons. Yet that strategy was effective because only a small number of governments were developing the most dangerous biological weapons. It no longer works in a world in which AI allows more actors—rogue states, terrorist groups, even individuals—to develop new bioweapons of their own.

In this new threat landscape, biological attacks are unlikely to be prevented entirely, given the proliferation of biological capabilities and the fact that some actors cannot be deterred by traditional means. Policymakers need a new strategy in response—one that accepts that biological attacks are likely and prepares to contain the harm, helps the country recover more quickly, and uses new tools to identify and hold perpetrators accountable. Ultimately, this resilience to biological attacks could dissuade malicious actors from attempting to use them in the first place, knowing that the effects will be minimized—a strategy of deterrence by resilience.

Consider the attack scenario described above, but with a comprehensive strategy in place. The U.S. government would use a sophisticated biological monitoring system to provide early warning of the emergence of a new viral pathogen. Employing many of the same technologies that enable the threat in the first place, federal laboratories would determine its origin from telltale signatures in the AI model used to design the virus—enabling prompt efforts to track and target the perpetrators. Public health authorities would have the tools to integrate scientific and intelligence data to suppress the disease's spread. Based on pre-negotiated contracts to provide surge capacity, the biomanufacturing sector would accelerate the production of diagnostics, therapeutics, and vaccines. Although the crisis would not have been prevented entirely, its effects would be speedily and effectively contained: vulnerable human and animal populations protected, contagion minimized, agricultural production recovered, public confidence restored.

Such bioresilience is far from today's reality. In 2024, H5N1 bird flu spread from poultry to dairy and beef herds and eventually to more than 70 humans. As the White House homeland security adviser at the time, I coordinated the federal response to this potentially catastrophic threat. The virus was naturally occurring, not the result of a deliberate attack. It nevertheless showed that even in this base case, there were considerable weaknesses and gaps in U.S. prevention, monitoring, attribution, and response systems. Data on disease incidence and spread were hard to acquire and exasperatingly incomplete. Mobilizing sufficient preventive action by the poultry and cattle industries proved difficult and slow. And in order to deliver sufficient quantities of human vaccines to protect the American people, we needed to provide substantial new federal funding to rapidly create an mRNA vaccine and divert U.S. pharmaceutical industry production lines to make it at scale, and there would still have been inadequate drug supplies for many months.

The United States urgently needs a new system to generate resilience against AI-enabled biological threats. The reality of this technology means that the very innovation that drives the revolutionary discoveries also creates the new threats—and the same tools that make those threats so dangerous are also essential to countering

them. That system, accordingly, will depend on leveraging advances at the intersection of AI, biotechnology, and bioengineering—and staying ahead of adversarial exploitation of the very same advances.

BRAVE NEW WORLD

During the Cold War, U.S. security experts warily monitored the Soviet Union's biological weapons programs. Their concerns focused on the possible weaponization of rare but known pathogens such as anthrax, Marburg virus, and Variola virus (which causes smallpox) that could be used against American forces in combat—or even against U.S. civilians. After the Soviet empire collapsed, I oversaw the Pentagon's efforts to reduce the threats posed by its arsenal of weapons of mass destruction. We closely tracked and worked to eliminate legacy stockpiles of deadly pathogens in Russia and other newly independent states.

For decades, Washington relied on deterrence to counter the possibility of adversarial biological attacks—but, notably, not by threatening biological attacks of its own. Indeed, in 1969, U.S. President Richard Nixon officially forswore the research, production, and use of offensive biological weapons. Instead, American doctrine was based on credibly threatening nuclear retaliation.

As the Cold War receded and Moscow and Washington shrank their nuclear arsenals through cooperative threat reduction initiatives, national security experts began questioning whether it was moral or effective to threaten the use of nuclear weapons to deter biological attacks. Nevertheless, across multiple administrations, the United States retained deliberate ambiguity on this front. The most recent U.S. Nuclear Posture Review, in 2022, concluded that "our nuclear strategy accounts for existing and emerging non-nuclear threats with potential strategic effect for which nuclear weapons are necessary to deter." It added that the "fundamental role" of nuclear weapons is to deter nuclear use against the United States and its allies, but it did not go so far as to assert that nuclear deterrence is the "sole purpose" of the arsenal. The current Trump administration has thus far decided that another nuclear posture review is not necessary, pointing to the adequacy of the doctrine promulgated by the first Trump administration in 2018. That review stated that nuclear weapons could be used against "non-nuclear strategic threats," which, although not specifically referring to biological attacks, is understood to include them.

Given technological changes at the intersection of AI, biotechnology, and bioengineering, changes that substantially lower the bar to lethal pathogen production and wide diffusion to uses beyond secret state laboratories, this doctrine is no longer fit for purpose, if it ever was. A decade ago, leading experts began to focus on novel pernicious uses of biology. In late 2016, for example, the President's Council of Advisors on Science and Technology issued the first thorough, unclassified warning about the potential national security risks posed by biotechnology. Those risks, the council wrote, were "real and will only grow as biotechnology becomes more sophisticated in the years ahead."

The report's authors went on to explain why. "Biothreats," they wrote, "differ in significant ways from nuclear or chemical threats in that the initial creation of biologically engineered organisms requires much more modest resources and smaller facilities that cannot be readily distinguished from ordinary research labs. Work undertaken with malevolent intent is thus harder to distinguish from work undertaken for benevolent purposes."

The report highlighted the gene-editing tool CRISPR, in particular, for its revolutionary positive and simultaneously pernicious potential. CRISPR enables DNA sequences to be quickly cut and modified, giving users the capacity to eradicate hereditary diseases but also to insert changes in the genome that could affect a specific group of individuals—or even alter the human germline, which determines the genetic

inheritance of future generations. CRISPR is also, as the advisory report emphasized, a dual-use tool (one with both civilian and military applications) that can be employed without massive investment or expertise.

The brave new world of synthetic biology, in other words, is radically democratizing and dispersing access to the tools used to make bioweapons. Rapid DNA sequencing and synthesis capabilities have collapsed the cost of reading and writing genetic information, just as tools such as CRISPR have broadened the availability of precise genome modification. Now, AI systems trained on biological data can design proteins and predict a multiplicity of interactions at scales previously unimaginable. AI systems and advanced computing also enable generative biology, which makes possible the construction of synthetic biological systems. Finally, digital designs are being linked to increasingly automated laboratory processes, facilitating the production of digital instructions in the real world.

All this innovation is powering immensely positive discoveries across multiple sectors, the most obvious of which is health care. But it is also evaporating the barriers that until now have made it very hard to engineer dangerous biological agents. Performing complex biological work is no longer limited to people whose advanced education and professional occupations would impress on them the gravity of their responsibilities to do no harm. Today, a much greater variety and number of people, including those with little or no formal training, have access to sophisticated AI-enabled biological tools. This dramatic widening of usability—"uplift," in the parlance of artificial intelligence experts—has become a key measure of how much improvement an AI system provides over what a human being can do without it. And American frontier AI models have rapidly advanced the material uplift available to nonexperts who want to acquire biological knowledge or lab skills to complete scientific tasks. Three years ago, large language models failed simple biology tests. But by April 2025, a group of university and nonprofit researchers found that large language models consistently outperformed Ph.D.-level virologists on tests of the knowledge needed to conduct laboratory experiments.

This fact might be less concerning if large language models and other leading-edge biological tools were cloistered in government labs. But they are not. They are widely distributed, and AI science agents are now available for hire and are ready to accompany their clients on creative journeys, whether benign or malign.

For now, turning a digitally designed pathogen into a real-life threat is restricted by the fact that, in the United States, the work is still done by human beings in traditional "wet labs," where the physical production of digital orders takes place. But the human role is now increasingly accompanied by robots and automation, in particular with the advent of "cloud labs," which can receive digital orders, design and execute experiments based on them, and evaluate the outcomes, combined with specialized contract manufacturers that provide biotech production services. Right now, there are no regulations governing any of this activity.

SCIENCE FICTION TO SCIENCE FACT

Today, public officials and private-sector leaders need to be concerned not only about sophisticated states developing and using bioweapons but also about organized nonstate groups, including terrorists, criminal syndicates, and mercenaries, as well as lone wolves. In addition, well-intentioned people might cause a dangerous accident because they do not fully understand the powers they wield.

There are innumerable scenarios for which Washington needs to be prepared. For example, malicious cyber-hackers seeking to wreak havoc could use AI to corrupt the pharmaceutical manufacturing process, creating dangerous,

tainted drug products. The results could exacerbate illnesses or cause deaths—and could damage confidence in products more generally, destabilizing the market for American medicines or deleteriously affecting national health care through a reluctance to use previously respected therapeutics.

In another plausible scenario, a politically motivated, loosely organized anarchist network could use an open-source large language model to figure out how to deliver a highly pathogenic virus into large human populations. It might order what appear to be benign fragments from multiple commercial DNA synthesis providers. A member with relevant expertise could then assemble those fragments into a deadly new virus and possibly release that virus into a major American urban area, such as New York or Los Angeles, where it would spread rapidly. In such a scenario, many deaths would precede conclusive diagnoses, treatments would not be readily available, and health-care systems would be overwhelmed. Emergency response mechanisms would be unable to react fast and at scale. Mass panic would ensue.

There are also pernicious potential nation-state applications of AI-enabled biology. For example, a technologically sophisticated foreign adversary could leverage AI, biological design systems, and biomanufacturing tools to engineer a stealthy respiratory pathogen. Through advanced bioengineering, the disease's symptoms might not emerge until six months after infection. The adversary could surreptitiously release the pathogen near several American military bases, both across the U.S. homeland and elsewhere, as part of a broader plan to launch a military campaign that coincides with emerging mass illness. Simultaneously, under the guise of an annual domestic flu shot program, the adversary country could secretly inoculate its own population against the pathogen. American troops and the civilians with whom they have been in contact would eventually start coming down with severe symptoms, disrupting the U.S. military mobilization and deployment required to respond to the adversary's initiation of overt hostilities.

And there are possibilities extending beyond human disease vectors. For example, an ideologically motivated American terrorist organization could genetically modify a plant pathogen so that it destroys a key crop such as rice, corn, or wheat in the United States. This would rapidly disrupt domestic food supply and the agricultural economy on which so many livelihoods depend, resulting in food insecurity at home and famine in regions of the world that depend on U.S. crop exports.

These scenarios are not science fiction, and the United States is underprepared to handle any of them. The U.S. biological monitoring and attribution architecture is a patchwork of systems with significant gaps. Its various components are not always interoperable, and the country has no real-time capability to integrate and analyze diverse streams of data at scale. The American monitoring system is designed to diagnose, recognize, and report existing pathogens, but it cannot yet recognize new ones that may be created by AI-enabled biotechnology. Meanwhile, the country's system for fielding countermeasures to treat and prevent diseases is not primed to move quickly, and it has relatively little surge capacity. The global response system is even more deficient. The early warning network for international biological threats—akin to the national missile defense early warning system—that the United States established and championed over the last two decades across multiple presidencies, including an expansion to more than 50 pivotal countries during the Biden administration, was largely dismantled by the Trump administration in 2025.

These scenarios also vividly demonstrate that with new biothreats, the long-standing U.S. deterrence-by-punishment concept designed for a small number of state-level adversaries—threatening the imposition of pariah status and the prospect of employing nuclear weapons against a biological attack—is no

longer adequate. Today's AI-enabled biotechnology challenge upends reliance on punishment for four reasons. First, the bio-risk club is already large and will inevitably become much larger than the nuclear club. Biodeterrence needs to shape the behavior of numerous countries and, more consequentially, private-sector and individual actors who are likely to be much less sensitive to state-level interests. Because the building blocks of biological threats are most often dual-use technologies and because they have immense upside, it is not possible to fully prevent the generation of potentially harmful materials or lock them down in government-controlled laboratories and sites, as has been done with nuclear fissile materials. Ultimately, it is not a plausible strategy to threaten to use nuclear weapons against the full array of risks and threats posed by AI-enabled biology, so the threat of nuclear-scale punishment loses credibility.

Second, given the role that AI-enabled biotechnologies already play in multiple sectors of the economies of Washington's allies and partners, extended deterrence will not be plausible. The United States cannot offer them protection in exchange for forbearance as it has done in extending its nuclear umbrella to protect European and Asian allies. The benefits of bioconvergence—the synergy of advances in AI, biotechnology, and bioengineering—matter too much to each country's economic and societal well-being.

Third, it is highly doubtful that Washington can either persuade or compel U.S. competitors and adversaries to reliably withhold development of AI-enabled biotechnology capabilities in the same way that it managed the nuclear arms race with the Soviets because nuclear weapons had no other market value than deterrence and warfighting. Bioconvergence, by contrast, promises and indeed is already delivering immense positive potential, and the AI-enabled biotech economy is global.

Fourth, and relatedly, the Trump administration has episodically sought to make it harder for other countries to access and use American frontier AI models, including in June 2026, when it suddenly imposed export controls on Mythos and Fable—cutting-edge Anthropic products that provided AI capabilities to the United Kingdom and the European Union. The controls resulted in an abrupt and total cutoff of access to any foreign user, including allies and U.S.-based individuals. This draconian action was subsequently reversed, but it is likely to stimulate even more international interest in developing domestic AI capabilities, including at the intersection of AI and biotechnology, because dependence on the United States may create vulnerability.

DETERRENCE BY RESILIENCE

Given the near inevitability of natural, accidental, and weaponized biological incidents in the future, anxiety about growing risks is warranted, and it is magnified by the absence of a strategy to effectively manage those risks. The American people are not powerless in the face of this epochal challenge, but it requires a comprehensive plan of action and a sustained commitment to adaptive implementation, both of which must leverage the vibrant U.S. innovation ecosystem to manage biological risks—including those that may be existential.

As a foundational capability for biological risk management, the United States needs a nationwide monitoring system that can provide early warning of emerging pathogens, whether naturally occurring or synthetic. This requires federal and state investments in building the underlying sensing and collection infrastructure, such as wastewater surveillance, and in establishing a distributed laboratory network to rapidly process the data this infrastructure generates.

Those tools would undergird the effort to quickly identify pernicious actors, which would be essential in establishing deterrence. Although some attackers, such as lone wolves, are unlikely to be responsive

to threats of punishment, if state-level or state-sponsored adversaries believe that biological attacks will never be attributed to them, they can act with impunity. It is therefore a matter of national security that the United States develop the capacity to quickly determine which hostile adversary is the source of a biological agent.

A new, resilient ecosystem will depend on a backbone of rapid data access, integration, and analysis that should be owned by the federal government but managed as a collaborative consortium with private-sector partners. This will ensure that the United States can absorb, fuse, and evaluate AI and biological data streams from across the country and, optimally, around the world. This enterprise would serve national and homeland security missions, including being able to continuously identify emerging biothreats and understand what they are and what they can do—such as recognizing engineered pathogens that do not match any list of known organisms—and rapidly develop targeted responses. It must feature the capacity to do work in a classified context that provides dedicated computing power and infrastructure for training and evaluating frontier biological models and for managing sensitive biological data.

Detection and attribution, of course, will not stop the spread of disease on their own. In the event of an attack, Washington must be ready to instantly respond to save lives and preserve the economy. After the 9/11 attacks, U.S. President George W. Bush created a national "critical infrastructure" designation, applied to 16 sectors such as chemicals, financial services, energy, and transportation, that enables the federal government and private companies to securely share information and develop thorough plans for effective crisis management. The biotechnology industry should now be designated as a critical infrastructure sector. As part of this designation, Washington should establish a coordinating council for the biotechnology sector that includes DNA synthesis providers, AI model developers, genomic data platforms, cloud lab operators, and high-containment laboratories. The group should exercise regularly with federal, state, and local government partners for biological incident responses, just as the electricity sector does to strengthen grid security and build resilience against all hazards.

Leveraging additional capabilities in the private sector to enable a "warm start"—in which the bio-innovation ecosystem is primed to surge its tools in response to an emerging biological crisis—the United States should establish a national strategic readiness reserve for handling biothreats. This can be modeled on the Civil Reserve Air Fleet, which enables the federal government to promptly make use of commercial planes and pilots when a military aircraft shortage emerges. In the context of a biological threat, similar, preestablished arrangements would assure the federal government of emergency access to the computing power, laboratory facilities and personnel, and production capacity needed for accelerated discovery, design, and development of diagnostics, therapeutics, and vaccines, along with scalable biomanufacturing capacity to make urgently needed tests, medicines, and inoculations. Although the Defense Production Act could enable government access, it does not provide the flexibility needed to prepare for long-term resilience, and invoking it in the midst of a crisis can cost the country precious, potentially life-saving time.

As part of its readiness efforts, the United States must fix the federal clinical trials process, which is far too slow and cumbersome to effectively address a biological crisis. This major bottleneck already limits U.S. biotech competitiveness and diverts activity to China, creating supply chain dependencies with potentially ominous implications for American security. The United States would benefit right now from a reformed clinical trials process, which would help U.S. companies regain their

competitive edge—and help Washington demonstrate to would-be attackers that it can move fast to field countermeasures.

Without a comprehensive technological edge, the United States will not be able to rapidly discern the nature of a biological attack, determine where it came from, and quickly figure out how to mitigate its harms by fielding targeted diagnostics, therapeutics, and vaccines. That capability is essential for reducing adversaries' confidence in their use of biological weapons, for shaping global norms, and for responding effectively when prevention fails.

Unlike in previous eras, the U.S. government alone cannot maintain the country's technological supremacy. The ability to characterize and attribute threats, develop countermeasures, and respond rapidly to novel pathogens will depend heavily on the private sector, which needs to be not only a supplier but also an enduring national security partner. The United States must therefore maintain a strong private-sector AI and biotechnology ecosystem that is aware of emerging dangers and incentivized to work with the government to reduce them.

Meeting this challenge requires a sustained, deliberate effort to rebuild and protect the United States' capacity for biotechnology innovation. Over the last five years, American companies have become increasingly dependent on China for the components used in many drugs sold in the U.S. market and for access to the latest research in therapeutic molecules that can treat or cure diseases, creating substantial supply chain risks. The U.S. pharmaceutical industry is also acquiring a large number of Chinese biotech assets—buying the intellectual property and rights to develop Chinese drugs—particularly in innovative therapeutics. At the same time, it is competing to sell pharmaceutical products into the gigantic Chinese domestic market despite deep concerns that Beijing is stealing intellectual property.

Washington can tackle this challenge and strengthen American firms by revitalizing federal funding for basic science and investing in the human talent to win the biotech race. To do so, Congress should enact legislation that reduces growing dependencies on China and supports the U.S. biotech and pharmaceutical industries via targeted subsidies, public investment in research and development, tax incentives, and other measures. This bill might be modeled, in part, on the 2022 CHIPS and Science Act, which invested hundreds of billions of dollars in research and manufacturing for strategically important sectors. These actions should be paired with measures that expand protections for the United States' biotech innovation infrastructure, including the strengthening of a national security review process governing foreign investment in the sector. Incentives for collaborative development and production with aligned foreign partners should also be prioritized. In addition, Congress should immediately pass legislation to mandate that DNA synthesis companies screen customers and the sequences they order to prevent malicious actors from abusing this technology; this action needs to be synchronized with comprehensive efforts to strengthen the U.S. biotech innovation sector that can counterbalance the potentially onerous burden of such requirements.

MEET THE MOMENT

Pathogens know no borders. All countries should share the responsibility for preventing terrorists and rogue actors from developing and using AI-enabled biology to perpetrate mass harm. But without American leadership, it will not be possible to build the global institutions, regimes, norms, and practices that advance U.S. interests in prevention and effective crisis response and help protect the entire world from AI-enabled biological attacks. To that end, the United States, in collaboration with close international partners, should launch a series of global biosecurity summits modeled on the four international nuclear security summits that took

place from 2010 to 2016. The agenda could include setting common standards for DNA synthesis screening, generating market incentives for secure and resilient AI-biotech tools and systems, conducting pathogen surveillance, ensuring supply chain resilience, and pursuing responsible AI-enabled biotechnology development. Whether within this framework or parallel to it, China and the United States should establish a high-level, technically sophisticated dialogue on AI-enabled biological risk management.

On the home front, American frontier AI companies, such as Anthropic, Google, and OpenAI, have committed to testing their models and ensuring novice users cannot employ them to generate biological weapons. But these undertakings remain voluntary, their effectiveness has not been proved, and these companies' private incentives will inevitably diverge from public interests. The U.S. government should work concertedly with frontier AI companies and biotechnology developers to establish a framework for tiered access to the most sophisticated of AI-enabled bio models: an AI model trained not on words and text but on sequences of DNA that can predict, edit, and design novel proteins, cells, and viruses. They should also collaborate to establish and enforce specific guardrails for what these models can generate. This includes embedding safety features that prevent malign bioweapons development and embedding mechanisms that enable such misuse to be easily detected. It also includes establishing guardrails around what biodesign tools that facilitate the construction of novel proteins and cells are permitted to do—and how autonomous laboratories are allowed to operate, specifically with respect to whether human beings must remain in the loop to prevent abuse.

Given the pace of innovation, responding to this multidimensional challenge will be an ongoing and iterative process. But this is not the first time the United States has tackled an emerging and potentially existential security threat. In the early 1990s, Indiana Senator Richard Lugar, a Republican, and Georgia Senator Sam Nunn, a Democrat, came together to enact landmark legislation that enabled the United States to prevent the proliferation of nuclear weapons and fissile materials after the collapse of the Soviet Union. Congress authorized and appropriated funds for a comprehensive and consequential series of actions—some unilateral and some cooperative—at home and around the world that ensured that the Soviet Union's nuclear legacy did not create multiple new nuclear nations and that terrorists could not access Soviet nuclear weapons or the essential components to build their own bombs and delivery systems.

With similarly visionary bipartisan action today, the United States can position itself to excel in developing hugely beneficial commercial applications of biotechnologies while also effectively monitoring, attributing, and responding to biological threats. This will require synergy and deft management between private-sector innovation and public interests. But the United States is capable of balancing these two imperatives. If a nationwide biological monitoring network that depends on private companies to provide services is established, it will offer continuous benefits, including early warning and attribution for a variety of risks. If the clinical trials system can be transformed, it will benefit consumers by strengthening the competitiveness of U.S. industry and onshoring more biotech production. Coupled with investments and incentives for the American biomanufacturing sector, these measures will build up the infrastructure necessary to secure Americans against biological risks. That, in turn, will enable the country to respond promptly in the event of a deliberate attack and make it less vulnerable to supply chain disruptions. The United States will establish deterrence and therefore reduce risks, creating a virtuous cycle in which Americans can begin to have greater confidence in a bioresilient future.

AI-designed viral genomes

The generation of functional viral genomes has urgent biosafety and biosecurity implications

By Thomas V. Inglesby and Moritz S. Hanke

Science | 6 Aug 2026 | Vol 393, Issue 6811 | pp. 563-564

Source: https://www.science.org/doi/10.1126/science.aej8512

Abstract

Artificial intelligence (AI) has been used to generate proteins, protein complexes, and short portions of genomes (*1*). Designing a complete genome is harder because it requires understanding its higher-level architecture, such as how the coding sequences for different genomic products overlap. On page 589 of this issue, King *et al*. (*2*) report the synthesis of a complete functional viral genome, designed using generative AI. Although this is promising for life sciences applications, it also raises urgent biosafety and biosecurity questions. The ability to compose viral genomes using generative AI now exists; the governance to safely steer it does not.

South Korea's Bioterrorism Response Training Program Shows Strong Gains

Source: https://globalbiodefense.com/2026/08/29/south-koreas-bioterrorism-response-training-program-shows-strong-gains/

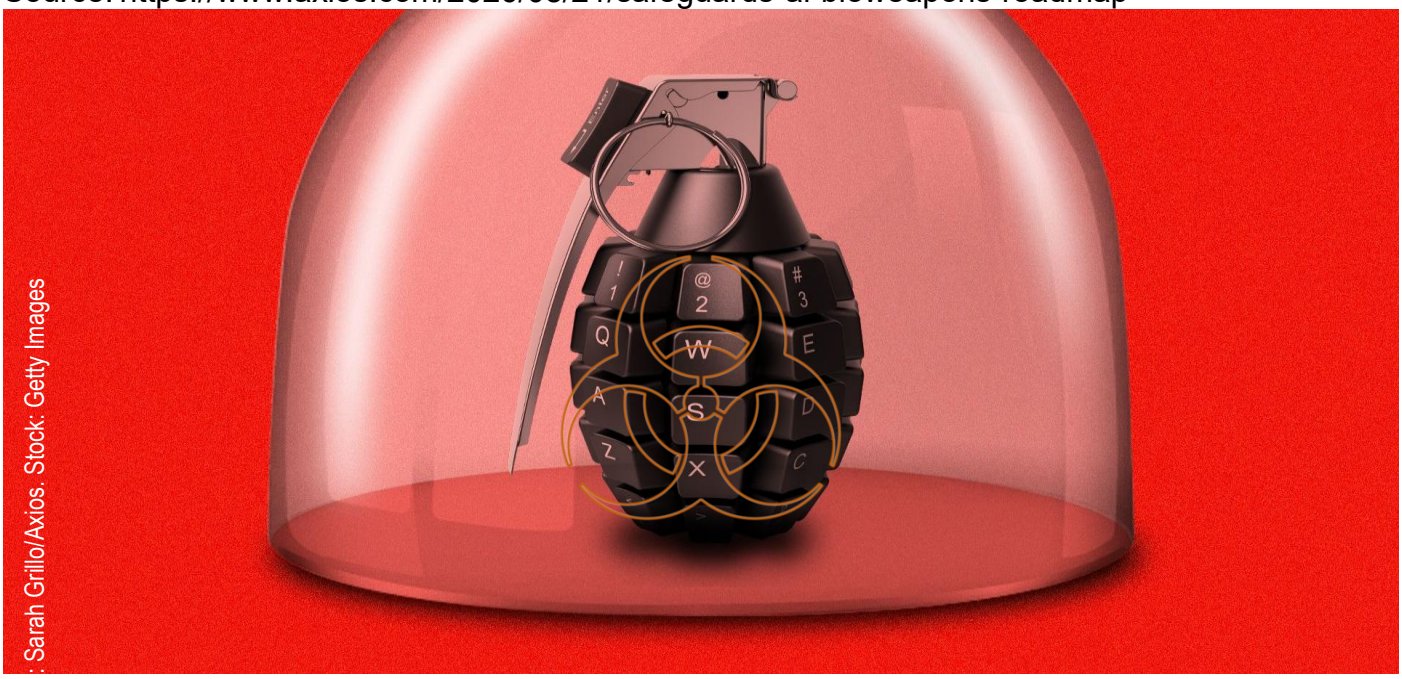
Aug 29 – When a new pathogen emerges, or a bioterrorism event unfolds, the frontline workers who don protective gear and manage the first patients often determine how well an outbreak stays contained. A new evaluation of South Korea's national training program for exactly those responders offers new perspectives on which training approaches actually build that capability, and which measurement gaps still need closing. The study, published in *Public Health Weekly Report (PHWR)*, comes from researchers at the Korea Disease Control and Prevention Agency (KDCA). It evaluates the agency's 2025 professional training project for medical personnel responding to emerging infectious diseases and bioterrorism, run in partnership with the National Central Medical Center's Public Health and Medical Education Training Center. The program reflects a broader post-COVID-19 push to treat workforce training as core infrastructure rather than a one-time response to a specific outbreak. The curriculum ran fourteen separate course offerings across 2025, split between three basic-level courses and four advanced ones. Basic training covered outbreak response principles, infection control, and a full day of intensive instruction in Level C personal protective equipment, donning, doffing, and decontamination procedures, while advanced courses added case-based instruction for physicians and administrators along with scenario-driven simulation exercises modeled on real outbreak events from the prior year, covering tasks like patient transfer and isolation ward operations. Demand outpaced capacity substantially: against 230 planned training slots, the program drew 631 applications and ultimately graduated 234 people, a completion rate of 101.7 percent relative to the original target. Nurses made up the large majority of trainees, at 84 percent, with physicians and emergency responders filling most of the remainder. Practical confidence, largely centered on comfort using Level C protective equipment, rose by 87.6 percent, the largest gain of any measure, moving from an average score of 5.09 to 9.55 out of a possible 10. Academic knowledge of outbreak response principles and infection control improved 58.2 percent, while a separate written knowledge test showed a more modest 13.3 percent gain in correct-answer rates. Every one of the 47 trainees who completed

the dedicated Level C protective equipment course passed its hands-on performance evaluation, a 100 percent pass rate the authors highlight as evidence that repeated, scenario-based practice translates into demonstrable skill. The findings signal that hands-on, simulation-based training appears to build practical confidence more effectively than lecture-based instruction alone. The authors call for expanding practice-oriented training capacity and diversifying which occupational groups receive it, alongside sustained investment in training infrastructure for pandemic preparedness.

A roadmap for safeguarding against AI bioweapons

By Caitlin Owens

Source: https://www.axios.com/2026/08/21/safeguards-ai-bioweapons-roadmap



: Sarah Grillo/Axios, Stock: Getty Images

Aug 21 – AI-enabled bioweapons are a potentially catastrophic yet manageable risk — if government, the scientific community, the public health sector and leading tech companies can develop appropriate safeguards, a new report argues.

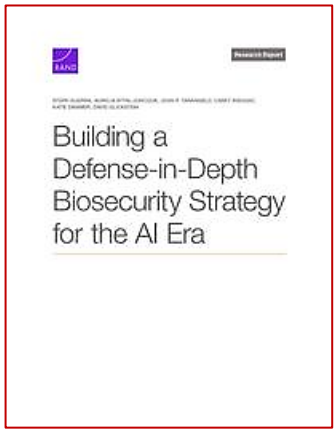
Why it matters: The debate over AI and public safety isn't one that the health care or research communities can ignore.

Driving the news: A RAND report out this week outlines nine mitigation strategies targeting a range of actors who could use AI to design and release a biological weapon.

- While there's already considerable debate about government oversight and safeguards around frontier AI companies, RAND calls for more controls and a wide range of cross-industry cooperation.
- It recommends protecting the same biological tools and datasets that are contributing to some of today's most exciting medical advances.
- And though we all think of public health preparedness as a response to an outbreak, the report frames it as a form of deterrence.

The big picture: The nine measures would prevent a large-scale AI-enabled biological attack by managing access to information that can fall into the wrong hands, disrupting access to the materials needed to make a weapon, proactively detecting signs of misuse and deterring nefarious activity from occurring in the first place.

- Part of the problem with AI's rapid advancement is it expands the field of players potentially capable of making a biological weapon, from lone wolves to state-backed actors.
- "AI capabilities in biology are advancing really fast, but luckily most dangerous thresholds have not yet been crossed," RAND lead author Steph Guerra told me.
- Given the nature of the threat, "we need this layered system of mutually reinforcing approaches."



Zoom in: Remember all of that talk about AI helping discover drug candidates?
Some of the technology enabling that work could turn dangerous in the wrong hands, Guerra told me.

- A lot of the tools and biological data being generated by pharmaceutical companies and biotechs are proprietary, meaning access is already restricted.
- Open-source biological tools and data are more concerning — including those emerging from academia and research institutes.
- "Right now, data for biology is freely out there and open because biology ... [is] for discovery and saving lives. It's not warfare first, which is a good thing," Guerra said.

Yes, but: Restricting what's publicly accessible risks slowing down scientific progress.

- "Let's build big moonshot projects and biodata factories that produce the data we need to cure diseases, but we can also create tiered systems of access so legitimate scientists are the ones who access the most misuse-relevant datasets," Guerra told me.

The intrigue: The RAND team has been exploring how the use of AI agents can make biological developments more widely accessible, lowering the bar for the level of expertise needed to make bioweapons.

- Just this week, Anthropic announced that Claude successfully designed protein binders against 14 targets — an important step in the drug development process.
- In a blog post, Anthropic acknowledged both the promise and the danger, noting that protein design and other research biology capabilities aren't available for general access in the company's most capable model.
- "The uplift provided by the increasingly autonomous research capabilities of AI models will undoubtedly speed the development of human therapies and fundamental scientific discoveries," the company wrote.
- But, it added, "without robust safety measures, they could enable bad actors to perform dangerous research, such as the development of bioweapons.

Newly created viruses are a warning. We still have a window to stop AI-enabled bioweapons

By Steph Guerra
Source: https://thebulletin.org/2026/09/newly-created-viruses-are-a-warning-we-still-have-a-window-to-stop-ai-enabled-bioweapons/

Sep 4 – "Nature is the world's worst bioterrorist" is a common maxim in the field of biosecurity, a reference to the idea that naturally emerging pathogens cause far more deaths than any biological attack a terrorist could carry out. But the trope may soon be outdated. In an article published Aug. 6 in the journal *Science*, scientists demonstrated that

trained AI models can design novel viruses as well as—if not better than—nature itself.

The ability to rapidly respond to disease outbreaks may deter biological attacks. Pictured: UK National Health Service medical workers prepare to fight an Ebola outbreak in Sierra Leone in 2014. Credit: DFID - UK Department for International Development via Wikimedia Commons. CC BY 2.0.

Their experiment created viruses that infect bacteria, not humans. Still, much like the multiple AI models that escaped their test environments to hack other networks this summer, these newly revealed capabilities give biosecurity experts like me pause. How do we keep enabling legitimate scientific progress, while also preventing AI from assisting in the creation of biological weapons? As AI capabilities advance, viral bioweapons could become much easier to design and produce and could cause even more harm than the weapons used in the past. Consider that almost all the bioterrorist attacks in our modern era have involved substances like anthrax or ricin. While they've harmed dozens of people at a time, the illnesses these attacks caused weren't transmissible between humans. Designing novel viruses, on the other hand, could enable biological attacks that spread, infections that leap from person to person and that could even spark a pandemic. To prevent this outcome, we need to build mechanisms for restricting access to the tools, data, and materials that might allow someone to misuse emerging capabilities in this way. And we should also go further by building defenses that can deter nefarious activity in the first place. One prevention strategy is mandatory gene synthesis screening, an idea gaining traction among the highest levels of the AI industry and political leadership. This type of screening focuses on the scores of US companies that sell synthesized DNA or RNA to labs for use in biological experiments. Mandatory screening would require these companies to verify that a customer is a legitimate researcher; record the details of every order so that each can be traced and investigated; and check orders against a list of known dangerous genetic sequences. Eventually the goal would be screening that can detect novel biological threats that aren't on any pre-determined list. The

same screening policies should apply to the sale of gene synthesis equipment, which can operate in labs outside of a company's manufacturing facilities. The CEOs of all the leading AI companies in June endorsed an approach to gene synthesis screening, and federal legislation along these lines has been proposed. Gene synthesis screening essentially makes it harder to get the physical materials required to make biological weapons. While synthesis screening is necessary, it's not sufficient. We also need digital controls to complement this physical chokepoint. AI models learn to design viruses by training on curated, laboratory-validated datasets. These datasets include the DNA or RNA sequences of different viruses. They're often produced for beneficial purposes such as part of biological surveillance campaigns to better understand how to respond to active outbreaks or develop medical countermeasures to combat viruses. Unfortunately, the data is not just useful for this sort of scientific research, but also as potential recipes for misuse. Datasets can also include attributes of the virus like how transmissible or deadly it has been, information that could be quite useful in the design of a bioweapon, especially if we train new AI models on it. Even as we screen lab orders for risky ingredients, we should also be thinking about how to limit access to the digital cookbooks to those that need them for combatting viral outbreaks rather than for creating them.

This will be a balancing act. For biological research, any restrictions will have to be calibrated to enable beneficial research while preventing misuse. While in the atomic age, any information on the design or development of nuclear weapons or energy systems was considered "born classified," by policymakers, biological research is mostly for the benefit of society, not warfare. Restricting access to certain sets of data means potentially slowing the science that saves lives, and getting any policy right will take careful thought.

Having gene synthesis screening and access restrictions would create friction at two critical points on the road from idea to actual AI-enabled biological weapon. But they are not foolproof solutions. Some actors can culture biological materials on their own; they don't need to use commercial suppliers of nucleic acids. Others have enough expertise to design dangerous pathogens without AI assistance. We've already seen test cases where AI was used to design molecules that eluded gene synthesis screening. Even the most heavily guarded AI models can be jailbroken—that is, manipulated using specially crafted prompts to bypass safety filters and allow access to restricted information. For the advanced adversaries who can sidestep controls, we will need additional layers of defense.

Another part of a defensive arsenal should be a pathogen early warning system designed to catch a novel viral outbreak as quickly as possible. Paired with current and future forensics and attribution technologies that can pinpoint the source of any engineered virus, early detection becomes a deterrent to biological weapons. When would-be bioterrorists know that an engineered outbreak will be identified, traced back to its origin, and rapidly contained, their calculus changes. The certainty of being caught discourages a biological attack before it begins.

Likewise, other actors may be dissuaded from using biological weapons if they believe the impact of their potential attack will be low due to rapid response capabilities, a concept known as deterrence by denial. This type of deterrence only works if these response capabilities are publicly demonstrated. We do this by rapidly responding to any outbreak in the world, preventing them from becoming pandemics. The work of organizations like the Coalition for Epidemic Preparedness Innovations, which just funded a fast-track vaccine development to combat the Ebola outbreak in Uganda and the Democratic Republic of Congo, is one example. Governments and other organizations around the world should support more robust responses like this. Developing a

resilient defensive strategy against the misuse of AI and biology requires dedicated resources, technological breakthroughs, and sustained political leadership. And because the United States is not the only country advancing in AI and biotechnology, this effort demands international coordination—particularly with China. No set of access controls or early warning system will work if it only covers half the globe. Thankfully there is still time to act. The capabilities of AI models are not yet advanced enough to design human-infecting viruses. Producing the novel bacteria-infecting viruses described in *Science* took elite scientists working with state-of-the art equipment in well-furnished laboratories. They had substantial resources to design, test, and optimize hundreds of viruses to find the right ones for their research.

Yet, if an AI model were able to produce hundreds of infectious virus designs and reliably generate functional results for a significant share of them, it would substantially reduce the time and effort needed to use that capability, for good and bad. Similarly, AI agents—AI bots that can interact with other AIs, software, or people on the internet—could someday use the AI biodesign tools necessary for creating novel viruses, further reducing the need for expertise and opening up new risk pathways.

The *Science* paper serves as an important warning. We have a window of opportunity to build the layered system of defense we need now, before AI-enabled bioweapons capabilities become undeniably advanced—or worse, demonstrably effective.

Steph Guerra led the study *Building a Defense-in-Depth Biosecurity Strategy for the AI Era* at the RAND Center on AI, Security, and Technology. She's a molecular biologist who previously led strategic partnerships at the Center on AI Standards and Innovation under the Biden and Trump administrations and worked on biodefense policy in the White House.

Army sets new biodefense plan to counter pandemic, adversary threats

Source: https://breakingdefense.com/2026/09/army-sets-new-biodefense-plan-to-counter-pandemic-adversary-threats/

FORT BELVOIR, Va. — The Army announced today its new biodefense strategy to build a force that can fight to its full operational potential in a "biologically contested environment," an official from the US Army's Nuclear and Countering Weapons of Mass Destruction Agency told reporters today (USANCA) said. Such contested environments can consist of: naturally occurring threats like the COVID-19 pandemic or malaria, accidental threats caused by pathogen leaks from facilities, and deliberate biological threats manufactured by adversaries, Lt. Col. Dave Kingery, the biological defense integrator for the Army's headquarters and USANCA, told a small group of reporters today during a media event. "We have to ensure that a global pandemic or some other health event does not stop us from our ability to project those forces forward, so we can be in the place to fight and win the war and endure through any conflict," Kingery said.

New Lines Of Effort

The new strategy, signed by former Army Secretary Dan Driscoll, has five lines of efforts that the service hopes to implement by 2035, according to the strategy document sent to reporters ahead of today's event. Under the first effort, "building knowledge," the Army plans to recruit, develop and retain talent "to expand the pool of scientific, medical, and operational biodefense SMEs [subject matter experts] at all echelons," according to the strategy. This line also aims to

further include biodefense curriculum in training and education courses.

U.S. Army Command Sgt. Maj. Shelita Taylor, the command sergeant major of the 400th Military Police Battalion, U.S. Army Reserve, dons and clears her gas mask during a team-building ruck march held by the 200th Military Police Command during a 'CSM Huddle' in Scottsdale, Arizona, Sept. 16, 2017. During the huddle, the command sergeants major discussed critical topics relevant to their command and their units in order to increase readiness to deploy. (U.S. Army photo by Master Sgt. Michel Sauret)

The second line is "gaining situational awareness," under which the service plans to integrate biological sensors and analytical tools into existing platforms to "enable decision advantage" while also monitoring indications of adversaries using biological weapons.

Regarding the third line of effort — "managing information and communication" — the service wants to standardize biological information sharing systems across the joint force and with other agencies and allies. The Army also wants to counter misinformation and disinformation, which it plans to do by monitoring information spaces using artificial intelligence and machine learning tools.

"Building biodefense readiness" is the fourth line of effort. Through this, the Army wants to provide decontamination and protective equipment to mitigate biological threats and shift away from "treating biothreats as a purely medical problem to viewing them as operational constraints that affect warfighting functions."

Lastly, the fifth line of effort is "modernizing biodefense." According to the strategy, this will look like employing faster acquisition processes by leveraging AI, synthetic biology and additive manufacturing. The service also plants to update its doctrine by identifying "remaining gaps" in its current principles.

According to the strategy, the Army will prioritize lines three and five through 2028 as they will "create the necessary architecture for success across the other lines of effort." Lines one and two will be prioritized from 2028-2031 and the Army will focus on line four from 2031-2035.

Why Now?

Allison Tamasi, chief of USANCA's survivability and effects analysis division, told reporters there's "not a particular catalyst" for the new strategy but it comes after lessons learned from the COVID-19 pandemic, "the overall threat picture" and the "advancements in precision medicine" that "could be potentially also used against us." Kingery added that exercises in the Pacific and those in the US homeland have also helped inform the new strategy, but he did not provide any specific details on the exercises.

Col. Dennis Rufolo, deputy director for Force Health Protection at the Office of the Surgeon General and Army Medical Command, said more tools like mobile genetic sequencing devices have allowed soldiers in operational environments to test samples of "suspicious" looking wildlife remains or a strange, potentially harmful substance in as little as 24 hours. A few years ago, he said, this would have taken weeks as soldiers would have to send the samples back to the continental US to get tested. The updated speed helps to mitigate the risks of exposure, he said.

Further, the new strategy piggybacks off the service's 2021 biodefense

strategy, Tamasi said. The main differences between the two strategies is that the 2021 strategy was "focused very much on the Army getting those initial pieces in place," within its specific biology or chemistry shops whereas the new strategy includes guidance for how all of the Army can implement biodefense.

"It's no longer where if you see a group of dead wildlife, you just leave it to the surgeon team. Everyone has to have a part," she added. Rufolo echoed Tamasi's statement, explaining that now it's not only Army biologists or surgeons that will be responsible for tackling biodefense issues, but also intel professionals, protection professionals and more.

What's also different from the 2021 strategy is the proliferation of artificial intelligence, Rufolo said. The Army has been using AI to establish a "baseline" for diseases — referring to a benchmark that tells users how common and transferable a disease is based on different data sets. "So, from other nations, they're going to publish potentially data, and we could, through open sources, collect that information and be able to translate that and provide baselines. Where other information comes in, we can establish baselines. So when we have increases, we'll identify the concern potentially much faster with establishing a robust baseline through the utilization of AI, starting now onward," Rufolo said.

Flushing a Toilet Can Blast Germs Up to Your Breathing Zone, Study Finds

Source: https://www.sciencealert.com/flushing-a-toilet-can-blast-germs-up-to-your-breathing-zone-study-finds

Sep 11 – Few people go out of their way to touch a toilet. When we inevitably must, it's advisable to always wash your hands afterward, even if the toilet looks clean.

That's because a toilet's daily duties tend to leave it teeming with microbes, including potentially dangerous bacteria and viruses. If you leave those germs on your hands, you could sicken yourself and others. As a new research review highlights, however, washing your hands may not always be enough.

Flushing a toilet produces an upward plume of unsavory aerosols, which can rise into the breathing zone of adults and persist there for 20 seconds.

This plume could hold a wide array of microbial passengers, as previous research has shown, and seems capable of ferrying pathogens directly onto people or onto surfaces we might touch.

Yet while many studies have demonstrated the

existence of such plumes, and examined their contents and behavior, the evidence so far is still "fragmented and highly variable," the authors of the new review write.

Previous studies vary in experiment design, measurement methods, target microbes, and reporting, the researchers note, and have not consistently accounted for plume-influencing factors like bathroom ventilation or the physical and hydraulic characteristics of toilets.

Given what we do know about toilet germs and flush plumes, this phenomenon seems worth learning more about. It could already pose a hazard in places like hospitals, where many patients are more vulnerable to infection, and may play a wider role in some disease outbreaks.

In hopes of learning more, researchers from Australia conducted a systematic literature review, analyzing 22 studies of toilet-generated aerosols.

"Toilet flushing creates turbulence that can release aerosols into the surrounding air," says lead author Lira Adiyani from Flinders University. "Some studies detected these aerosols at adult breathing height, indicating a potential pathway for inhalation exposure."

Although the plumes are largely water, they can also feature bioaerosols – airborne particles arising from biological sources. Many of these are whole bacteria or viruses, and some can run amok inside a human nose or mouth. The danger depends on a variety of factors, Adiyani says, such as the volume and energy of a flush as well as a toilet's abundance of pathogenic microbes.

"The microbes can originate both from contamination of the toilet bowl during use, or from the water used for flushing," she says.

"The more microbes present in the toilet, the more bioaerosols may be released. Therefore, larger flush volumes generally produce more aerosols." The review included some studies in which researchers first "seeded" toilet water with microbes or fluorescent surrogate particles, as well as others conducted under more natural conditions.

Aerosol levels differed significantly among studies, the review found, depending on various experimental conditions, toilet properties, and sampling techniques.

In studies that involved seeding toilet water, higher concentrations of microbes in a toilet corresponded with higher concentrations of bioaerosols in its flush plume. Higher bioaerosol levels were often found closer to the toilet seat. This points to theimportance of toilet hygiene, Adiyani and her colleagues note. Regularly cleaning a toilet and nearby surfaces can curb microbial growth, which seems to reduce the prevalence of bioaerosols after you flush. The details of that flush matter, too, with forceful, high-volume flushes launching more microbes. This suggests we might limit bioaerosols by choosing toilets with lower flush volumes, or at least those with a lower-volume option.

The review did not find significant associations between aerosol levels and ventilation or lid position, but these are likely still worthwhile precautions, the authors say, as they could influence how aerosols move within a bathroom.

While ventilation may help disperse aerosols, some findings suggest closing the toilet lid can obstruct their ascent in the first place. A closed lid didn't seem to stop the plume entirely, but it did redirect aerosols outward through gaps between the lid and seat instead of sending them up.

"Based on the available evidence, I would recommend closing the toilet lid before flushing, where a lid is available, as a precautionary measure to minimize potential inhalation exposure – while recognizing that it does not completely prevent aerosols from escaping," Adiyani says.

This review helps shed light on toilet aerosols, but there's still plenty we don't know about how the plumes work and how to limit them, says environmental microbiologist Harriet Whiley, a professor at Flinders University and co-author of the review.

"Further research is needed to develop design

and engineering interventions that reduce toilet-generated bioaerosols, particularly in high-risk settings such as hospitals," Whiley says.

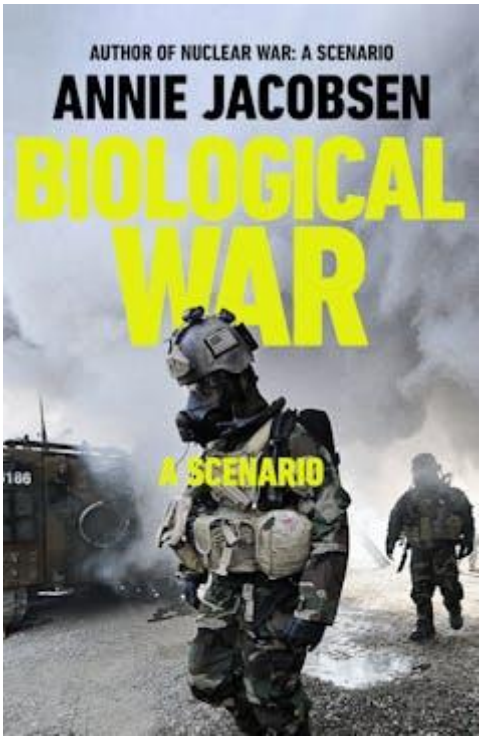
●▶ **The study was published in** *Science of the Total Environment*.

EDITOR'S COMMENT: A reminder from the pandemic era!

The threat of biological warfare is real – a new book describes the potential devastation

By Thomas Jeffries | Senior Lecturer in Microbiology, Western Sydney University
Source: https://theconversation.com/the-threat-of-biological-warfare-is-real-a-new-book-describes-the-potential-devastation-288934

Aug 30 – Annie Jacobsen's Biological War: A Scenario is a factually grounded book that reads like a thriller.



It tells the story of a hypothetical but realistic pathogen, built to cause maximum destruction, that is leaked from a research laboratory. The pathogen quickly causes anarchy and mass casualties around the world. The book follows the same format as Jacobsen's previous bestseller, Nuclear War: A Scenario, combining investigative journalism with speculative history, but in this case the enemy is invisible, difficult to detect and less well known than nuclear weapons.

Jacobsen's hypothetical scenario plays out day-by-day across the world. The point of view shifts between labs, Pentagon bunkers, city streets and military facilities. These scenes are interspersed with "history lessons" that describe previous biological weapons events, pandemics and government policies. The narrative structure keeps the reader glued to the page, taking in the ensuing horror. The language can sometimes be hyperbolic – for example, "military-grade DNA amplification technology" (this doesn't exist) – adding to the thriller-like tone. But the strength of the book is its sources. It is based on interviews with ex-military and government experts, defected Russian biological weapons engineers, and even the chief executive officer of OpenAI, Sam Altman. These add credibility to an otherwise too-scary-to-be-believable story.

An airborne plague

The first section of Jacobsen's book covers the history of biotechnology and biological weapons development. It starts with the 1925 Geneva Protocol outlawing their use, then notes subsequent violations of the protocol during the second world war and Cold War. The Biological Weapons Convention, which came into force in 1975, required the destruction of all such weapons. But a loophole allowing "defensive" or predictive research ensured many countries continued to engineer biological weapons, under the guise of developing vaccines or detection capabilities for hypothetical pathogens. This "dual-use" research has expanded recently. Researchers have sought to engineer possible future pandemic candidates.

The aim is to get one step ahead of naturally occurring outbreaks. But the same protective research can also be used to create pathogens for malicious use.

This research has led to an increase in the number of biosafety laboratories with the highest biological risk rating. Despite their strict safety guidelines, these facilities increase the risk of accidents such as lab leaks.

It is in one such laboratory – the real-life Vector Institute in Koltsolvo, Siberia – that the book's hypothetical leak occurs. After a sobering description of the historical Cold War era research conducted at this facility, Jacobsen moves into a blow-by-blow account of her hypothetical pandemic and its consequences.

A scientist responsible for a fire at the lab, riddled with guilt, seeks confession at the local church, unwittingly infecting a traveller. He then takes himself out in the woods to end his life. He is found by a group of hunters.

These primary contacts then spread the disease. The airborne fever, which kills quickly, reaches Los Angeles via a cruise ship, then spreads rapidly around the globe.

Jacobsen introduces us to a dizzying array of acronyms for United States military departments responsible for the real-time monitoring of satellite, chemical and communications data on a global scale. They receive information about the decontamination of the Russian lab site, as well as a mass vaccine roll-out and government cover-up, suggesting the catastrophic release of a biological weapon. When the plague appears in the homeless encampments of Los Angeles, however, authorities patronisingly believe it to be caused by a bad batch of fentanyl and fail to respond with any measure of personal protection or quarantine. By the time they realise their mistake, it is too late. Hospitals and clinics are overrun. There are mass casualties and gun violence.

Jacobsen populates her story with a full modern cast of influencers, YouTubers, conspiracy theorists and anti-vaxxers. Statistics not even relevant to biological warfare – about the large number of US citizens dying from opioid overdoses and the lack of faith in government institutions – are given in this section, adding to the gloom.

The portrayal of the belligerent and impatient US president and the self-obsessed podcasting California governor in this scenario is perhaps tongue in cheek. Another controversy is skirted when Jacobsen refers to the discredited theory that the COVID pandemic began with a lab leak in Wuhan, without explicitly stating whether this is a conspiracy theory or a realistic interpretation.

Devolution

Testing conducted by the Center for Disease Control and the military, which is described in detail in Jacobsen's book, reveals the pathogen responsible for the pandemic to be a form of the *Yersinia pestis* bacterium, which causes the plague. In this case, it is in its pneumonic (airborne) form, rather than the bubonic form known to history as the Black Death. This version of the bacteria, however, has been genetically engineered to be resistant to antibiotics. It responds to their application by releasing a toxin that causes encephalitis (swelling of the brain), leading to mania. It also produces a feeling of euphoria when a person is first infected, aiding its spread. This would seem like science fiction if it wasn't based on actual research conducted in Soviet biowarfare labs during the Cold War and tested, successfully, on animals – and in one case, accidentally on a human.

In Jacobsen's hypothetical scenario, the final response is to declare martial law. Citing the Insurrection Act, the US government attempts to use military force to

protect the insufficient roll-out of medical supplies antibiotics and vaccines, which are probably not effective against the disease anyway.
We are introduced to the actual "devolution" plans that exist to ensure the continuity of the US government in the event of an extinction-level catastrophe. Jacobsen describes how these measures would be put in place, leading to a world where a select group of people are isolated in bunkers as society collapses above ground.

An ongoing threat

After the initial spread of the pathogen, Jacobsen tends to ignore the world outside the US. This understandable given her expertise and intended audience, but it would be have been good to have a little more global context. Biological War is very much intended as a warning to governments to increase vigilance and policy effectiveness against the very real threat of biological weapons. The book ends in a post-apocalyptic landscape, where those who are the least altruistic, but had the best respiration masks, have survived in isolation. The president sits alone, pondering the nature of evil and the evolutionary basis for war.
In showing us what such a global catastrophe might look like, **Biological War is a reminder that we should not ignore the loopholes and dull legislation around biological weapons, biosafety and biosecurity. Our future depends on it.**

AI and the New Age of Bioweapons

Preparing for a World of Synthetic Pathogens

By Elizabeth Sherwood-Randall

Foreign Affairs | September/October 2026

Source: https://www.foreignaffairs.com/united-states/ai-new-age-bioweapons-elizabeth-sherwood-randall

Pathbreaking scientific discoveries can create transformational possibilities. They can also create catastrophic risks. The integration of artificial intelligence, biotechnology, and bioengineering is already enabling life-changing achievements, from combating disease to supercharging agricultural productivity to solving energy challenges. But it is also generating capabilities that can be weaponized more easily than ever by a growing number of actors. The United States is unprepared for these threats.
In the foreseeable future, a terrorist group with minimal skills could access a jailbroken AI model (one that has evaded safety controls) trained on the world's most comprehensive biological data set. The group could use the model to design a new strain of H5N1 avian influenza that is more lethal and more easily spread from animals to humans than

existing strains. Connecting remotely to one of the new generation of fully equipped, contract-for-service "cloud" labs, it could anonymously arrange for the virus to be built and tested and then sent to a biomanufacturing facility to be produced at scale. From there, the group could stealthily disperse the new strain through air-handling systems at major livestock farms across the United States.

Before long, the American poultry, beef, and dairy industries would suffer massive losses. When the virus inevitably jumped to the human population, it would cause severe illness and could result in hundreds of thousands or even millions of deaths. The response from U.S. public and private institutions—lacking both an integrated strategy and adequate tools—would be too slow, too uncoordinated, too underresourced, and too overwhelmed to stop the spread and mitigate the consequences. And soon, the virus would also cross borders, triggering food insecurity, widespread sickness, and mass casualties around the world.

U.S. policymakers have long contended with the possibility of biological attacks from hostile nation-states. Along with surveillance and global risk-reduction initiatives, Washington successfully deterred such attacks with the threat of significant retaliation, including the use of nuclear weapons. Yet that strategy was effective because only a small number of governments were developing the most dangerous biological weapons. It no longer works in a world in which AI allows more actors—rogue states, terrorist groups, even individuals—to develop new bioweapons of their own.

In this new threat landscape, biological attacks are unlikely to be prevented entirely, given the proliferation of biological capabilities and the fact that some actors cannot be deterred by traditional means. Policymakers need a new strategy in response—one that accepts that biological attacks are likely and prepares to contain the harm, helps the country recover more quickly, and uses new tools to identify and hold perpetrators accountable. Ultimately, this resilience to biological attacks could dissuade malicious actors from attempting to use them in the first place, knowing that the effects will be minimized—a strategy of deterrence by resilience.

Consider the attack scenario described above, but with a comprehensive strategy in place. The U.S. government would use a sophisticated biological monitoring system to provide early warning of the emergence of a new viral pathogen. Employing many of the same technologies that enable the threat in the first place, federal laboratories would determine its origin from telltale signatures in the AI model used to design the virus—enabling prompt efforts to track and target the perpetrators. Public health authorities would have the tools to integrate scientific and intelligence data to suppress the disease's spread. Based on pre-negotiated contracts to provide surge capacity, the biomanufacturing sector would accelerate the production of diagnostics, therapeutics, and vaccines. Although the crisis would not have been prevented entirely, its effects would be speedily and effectively contained: vulnerable human and animal populations protected, contagion minimized, agricultural production recovered, public confidence restored.

Such bioresilience is far from today's reality. In 2024, H5N1 bird flu spread from poultry to dairy and beef herds and eventually to more than 70 humans. As the White House homeland security adviser at the time, I coordinated the federal response to this potentially catastrophic threat. The virus was naturally occurring, not the result of a deliberate attack. It nevertheless showed that even in this base case, there were considerable weaknesses and gaps in U.S. prevention, monitoring, attribution, and response systems. Data on disease incidence and spread were hard to acquire and exasperatingly incomplete. Mobilizing sufficient preventive action by the poultry and cattle industries proved difficult and slow. And in order to deliver sufficient

quantities of human vaccines to protect the American people, we needed to provide substantial new federal funding to rapidly create an mRNA vaccine and divert U.S. pharmaceutical industry production lines to make it at scale, and there would still have been inadequate drug supplies for many months. The United States urgently needs a new system to generate resilience against AI-enabled biological threats. The reality of this technology means that the very innovation that drives the revolutionary discoveries also creates the new threats—and the same tools that make those threats so dangerous are also essential to countering them. That system, accordingly, will depend on leveraging advances at the intersection of AI, biotechnology, and bioengineering—and staying ahead of adversarial exploitation of the very same advances.

BRAVE NEW WORLD

During the Cold War, U.S. security experts warily monitored the Soviet Union's biological weapons programs. Their concerns focused on the possible weaponization of rare but known pathogens such as anthrax, Marburg virus, and Variola virus (which causes smallpox) that could be used against American forces in combat—or even against U.S. civilians. After the Soviet empire collapsed, I oversaw the Pentagon's efforts to reduce the threats posed by its arsenal of weapons of mass destruction. We closely tracked and worked to eliminate legacy stockpiles of deadly pathogens in Russia and other newly independent states.

For decades, Washington relied on deterrence to counter the possibility of adversarial biological attacks—but, notably, not by threatening biological attacks of its own. Indeed, in 1969, U.S. President Richard Nixon officially forswore the research, production, and use of offensive biological weapons. Instead, American doctrine was based on credibly threatening nuclear retaliation.

As the Cold War receded and Moscow and Washington shrank their nuclear arsenals through cooperative threat reduction initiatives, national security experts began questioning whether it was moral or effective to threaten the use of nuclear weapons to deter biological attacks. Nevertheless, across multiple administrations, the United States retained deliberate ambiguity on this front. The most recent U.S. Nuclear Posture Review, in 2022, concluded that "our nuclear strategy accounts for existing and emerging non-nuclear threats with potential strategic effect for which nuclear weapons are necessary to deter." It added that the "fundamental role" of nuclear weapons is to deter nuclear use against the United States and its allies, but it did not go so far as to assert that nuclear deterrence is the "sole purpose" of the arsenal. The current Trump administration has thus far decided that another nuclear posture review is not necessary, pointing to the adequacy of the doctrine promulgated by the first Trump administration in 2018. That review stated that nuclear weapons could be used against "non-nuclear strategic threats," which, although not specifically referring to biological attacks, is understood to include them.

Given technological changes at the intersection of AI, biotechnology, and bioengineering, changes that substantially lower the bar to lethal pathogen production and wide diffusion to uses beyond secret state laboratories, this doctrine is no longer fit for purpose, if it ever was. A decade ago, leading experts began to focus on novel pernicious uses of biology. In late 2016, for example, the President's Council of Advisors on Science and Technology issued the first thorough, unclassified warning about the potential national security risks posed by biotechnology. Those risks, the council wrote, were "real and will only grow as biotechnology becomes more sophisticated in the years ahead."

The report's authors went on to explain why. "Biothreats," they wrote, "differ in significant ways from nuclear or chemical threats in that the initial creation of biologically engineered organisms requires much

more modest resources and smaller facilities that cannot be readily distinguished from ordinary research labs. Work undertaken with malevolent intent is thus harder to distinguish from work undertaken for benevolent purposes." The report highlighted the gene-editing tool CRISPR, in particular, for its revolutionary positive and simultaneously pernicious potential. CRISPR enables DNA sequences to be quickly cut and modified, giving users the capacity to eradicate hereditary diseases but also to insert changes in the genome that could affect a specific group of individuals—or even alter the human germline, which determines the genetic inheritance of future generations. CRISPR is also, as the advisory report emphasized, a dual-use tool (one with both civilian and military applications) that can be employed without massive investment or expertise.

The brave new world of synthetic biology, in other words, is radically democratizing and dispersing access to the tools used to make bioweapons. Rapid DNA sequencing and synthesis capabilities have collapsed the cost of reading and writing genetic information, just as tools such as CRISPR have broadened the availability of precise genome modification. Now, AI systems trained on biological data can design proteins and predict a multiplicity of interactions at scales previously unimaginable. AI systems and advanced computing also enable generative biology, which makes possible the construction of synthetic biological systems. Finally, digital designs are being linked to increasingly automated laboratory processes, facilitating the production of digital instructions in the real world. All this innovation is powering immensely positive discoveries across multiple sectors, the most obvious of which is health care. But it is also evaporating the barriers that until now have made it very hard to engineer dangerous biological agents. Performing complex biological work is no longer limited to people whose advanced education and professional occupations would impress on them the gravity of their responsibilities to do no harm. Today, a much greater variety and number of people, including those with little or no formal training, have access to sophisticated AI-enabled biological tools. This dramatic widening of usability—"uplift," in the parlance of artificial intelligence experts—has become a key measure of how much improvement an AI system provides over what a human being can do without it. And American frontier AI models have rapidly advanced the material uplift available to nonexperts who want to acquire biological knowledge or lab skills to complete scientific tasks. Three years ago, large language models failed simple biology tests. But by April 2025, a group of university and nonprofit researchers found that large language models consistently outperformed Ph.D.-level virologists on tests of the knowledge needed to conduct laboratory experiments. This fact might be less concerning if large language models and other leading-edge biological tools were cloistered in government labs. But they are not. They are widely distributed, and AI science agents are now available for hire and are ready to accompany their clients on creative journeys, whether benign or malign.

For now, turning a digitally designed pathogen into a real-life threat is restricted by the fact that, in the United States, the work is still done by human beings in traditional "wet labs," where the physical production of digital orders takes place. But the human role is now increasingly accompanied by robots and automation, in particular with the advent of "cloud labs," which can receive digital orders, design and execute experiments based on them, and evaluate the outcomes, combined with specialized contract manufacturers that provide biotech production services. Right now, there are no regulations governing any of this activity.

SCIENCE FICTION TO SCIENCE FACT

Today, public officials and private-sector leaders need to be concerned not

only about sophisticated states developing and using bioweapons but also about organized nonstate groups, including terrorists, criminal syndicates, and mercenaries, as well as lone wolves. In addition, well-intentioned people might cause a dangerous accident because they do not fully understand the powers they wield.

There are innumerable scenarios for which Washington needs to be prepared. For example, malicious cyber-hackers seeking to wreak havoc could use AI to corrupt the pharmaceutical manufacturing process, creating dangerous, tainted drug products. The results could exacerbate illnesses or cause deaths—and could damage confidence in products more generally, destabilizing the market for American medicines or deleteriously affecting national health care through a reluctance to use previously respected therapeutics.

In another plausible scenario, a politically motivated, loosely organized anarchist network could use an open-source large language model to figure out how to deliver a highly pathogenic virus into large human populations. It might order what appear to be benign fragments from multiple commercial DNA synthesis providers. A member with relevant expertise could then assemble those fragments into a deadly new virus and possibly release that virus into a major American urban area, such as New York or Los Angeles, where it would spread rapidly. In such a scenario, many deaths would precede conclusive diagnoses, treatments would not be readily available, and health-care systems would be overwhelmed. Emergency response mechanisms would be unable to react fast and at scale. Mass panic would ensue.

There are also pernicious potential nation-state applications of AI-enabled biology. For example, a technologically sophisticated foreign adversary could leverage AI, biological design systems, and biomanufacturing tools to engineer a stealthy respiratory pathogen. Through advanced bioengineering, the disease's symptoms might not emerge until six months after infection. The adversary could surreptitiously release the pathogen near several American military bases, both across the U.S. homeland and elsewhere, as part of a broader plan to launch a military campaign that coincides with emerging mass illness. Simultaneously, under the guise of an annual domestic flu shot program, the adversary country could secretly inoculate its own population against the pathogen. American troops and the civilians with whom they have been in contact would eventually start coming down with severe symptoms, disrupting the U.S. military mobilization and deployment required to respond to the adversary's initiation of overt hostilities.

And there are possibilities extending beyond human disease vectors. For example, an ideologically motivated American terrorist organization could genetically modify a plant pathogen so that it destroys a key crop such as rice, corn, or wheat in the United States. This would rapidly disrupt domestic food supply and the agricultural economy on which so many livelihoods depend, resulting in food insecurity at home and famine in regions of the world that depend on U.S. crop exports.

These scenarios are not science fiction, and the United States is underprepared to handle any of them. The U.S. biological monitoring and attribution architecture is a patchwork of systems with significant gaps. Its various components are not always interoperable, and the country has no real-time capability to integrate and analyze diverse streams of data at scale. The American monitoring system is designed to diagnose, recognize, and report existing pathogens, but it cannot yet recognize new ones that may be created by AI-enabled biotechnology. Meanwhile, the country's system for fielding countermeasures to treat and prevent diseases is not primed to move quickly, and it has relatively little surge capacity. The global response system is even more deficient. The early warning network for international biological threats—akin to the national missile defense

early warning system—that the United States established and championed over the last two decades across multiple presidencies, including an expansion to more than 50 pivotal countries during the Biden administration, was largely dismantled by the Trump administration in 2025. These scenarios also vividly demonstrate that with new biothreats, the long-standing U.S. deterrence-by-punishment concept designed for a small number of state-level adversaries—threatening the imposition of pariah status and the prospect of employing nuclear weapons against a biological attack—is no longer adequate. Today's AI-enabled biotechnology challenge upends reliance on punishment for four reasons. First, the bio-risk club is already large and will inevitably become much larger than the nuclear club. Biodeterrence needs to shape the behavior of numerous countries and, more consequentially, private-sector and individual actors who are likely to be much less sensitive to state-level interests. Because the building blocks of biological threats are most often dual-use technologies and because they have immense upside, it is not possible to fully prevent the generation of potentially harmful materials or lock them down in government-controlled laboratories and sites, as has been done with nuclear fissile materials. Ultimately, it is not a plausible strategy to threaten to use nuclear weapons against the full array of risks and threats posed by AI-enabled biology, so the threat of nuclear-scale punishment loses credibility. Second, given the role that AI-enabled biotechnologies already play in multiple sectors of the economies of Washington's allies and partners, extended deterrence will not be plausible. The United States cannot offer them protection in exchange for forbearance as it has done in extending its nuclear umbrella to protect European and Asian allies. The benefits of bioconvergence—the synergy of advances in AI, biotechnology, and bioengineering—matter too much to each country's economic and societal well-being. Third, it is highly doubtful that Washington can either persuade or compel U.S. competitors and adversaries to reliably withhold development of AI-enabled biotechnology capabilities in the same way that it managed the nuclear arms race with the Soviets because nuclear weapons had no other market value than deterrence and warfighting. Bioconvergence, by contrast, promises and indeed is already delivering immense positive potential, and the AI-enabled biotech economy is global.

Fourth, and relatedly, the Trump administration has episodically sought to make it harder for other countries to access and use American frontier AI models, including in June 2026, when it suddenly imposed export controls on Mythos and Fable—cutting-edge Anthropic products that provided AI capabilities to the United Kingdom and the European Union. The controls resulted in an abrupt and total cutoff of access to any foreign user, including allies and U.S.-based individuals. This draconian action was subsequently reversed, but it is likely to stimulate even more international interest in developing domestic AI capabilities, including at the intersection of AI and biotechnology, because dependence on the United States may create vulnerability.

DETERRENCE BY RESILIENCE

Given the near inevitability of natural, accidental, and weaponized biological incidents in the future, anxiety about growing risks is warranted, and it is magnified by the absence of a strategy to effectively manage those risks. The American people are not powerless in the face of this epochal challenge, but it requires a comprehensive plan of action and a sustained commitment to adaptive implementation, both of which must leverage the vibrant U.S. innovation ecosystem to manage biological risks—including those that may be existential.

As a foundational capability for biological risk management, the United States needs a nationwide monitoring system that can provide early warning of emerging

pathogens, whether naturally occurring or synthetic. This requires federal and state investments in building the underlying sensing and collection infrastructure, such as wastewater surveillance, and in establishing a distributed laboratory network to rapidly process the data this infrastructure generates. Those tools would undergird the effort to quickly identify pernicious actors, which would be essential in establishing deterrence. Although some attackers, such as lone wolves, are unlikely to be responsive to threats of punishment, if state-level or state-sponsored adversaries believe that biological attacks will never be attributed to them, they can act with impunity. It is therefore a matter of national security that the United States develop the capacity to quickly determine which hostile adversary is the source of a biological agent.

A new, resilient ecosystem will depend on a backbone of rapid data access, integration, and analysis that should be owned by the federal government but managed as a collaborative consortium with private-sector partners. This will ensure that the United States can absorb, fuse, and evaluate AI and biological data streams from across the country and, optimally, around the world. This enterprise would serve national and homeland security missions, including being able to continuously identify emerging biothreats and understand what they are and what they can do—such as recognizing engineered pathogens that do not match any list of known organisms—and rapidly develop targeted responses. It must feature the capacity to do work in a classified context that provides dedicated computing power and infrastructure for training and evaluating frontier biological models and for managing sensitive biological data.

Detection and attribution, of course, will not stop the spread of disease on their own. In the event of an attack, Washington must be ready to instantly respond to save lives and preserve the economy. After the 9/11 attacks, U.S. President George W. Bush created a national "critical infrastructure" designation, applied to 16 sectors such as chemicals, financial services, energy, and transportation, that enables the federal government and private companies to securely share information and develop thorough plans for effective crisis management. The biotechnology industry should now be designated as a critical infrastructure sector. As part of this designation, Washington should establish a coordinating council for the biotechnology sector that includes DNA synthesis providers, AI model developers, genomic data platforms, cloud lab operators, and high-containment laboratories. The group should exercise regularly with federal, state, and local government partners for biological incident responses, just as the electricity sector does to strengthen grid security and build resilience against all hazards.

Leveraging additional capabilities in the private sector to enable a "warm start"—in which the bio-innovation ecosystem is primed to surge its tools in response to an emerging biological crisis—the United States should establish a national strategic readiness reserve for handling biothreats. This can be modeled on the Civil Reserve Air Fleet, which enables the federal government to promptly make use of commercial planes and pilots when a military aircraft shortage emerges. In the context of a biological threat, similar, preestablished arrangements would assure the federal government of emergency access to the computing power, laboratory facilities and personnel, and production capacity needed for accelerated discovery, design, and development of diagnostics, therapeutics, and vaccines, along with scalable biomanufacturing capacity to make urgently needed tests, medicines, and inoculations. Although the Defense Production Act could enable government access, it does not provide the flexibility needed to prepare for long-term resilience, and invoking it in the midst of a crisis can cost the country precious, potentially life-saving time.

As part of its readiness efforts, the United States must fix the federal clinical trials process, which is far too slow and cumbersome to effectively address a biological crisis. This major bottleneck already limits U.S. biotech competitiveness and diverts activity to China, creating supply chain dependencies with potentially ominous implications for American security. The United States would benefit right now from a reformed clinical trials process, which would help U.S. companies regain their competitive edge—and help Washington demonstrate to would-be attackers that it can move fast to field countermeasures.

Without a comprehensive technological edge, the United States will not be able to rapidly discern the nature of a biological attack, determine where it came from, and quickly figure out how to mitigate its harms by fielding targeted diagnostics, therapeutics, and vaccines. That capability is essential for reducing adversaries' confidence in their use of biological weapons, for shaping global norms, and for responding effectively when prevention fails.

Unlike in previous eras, the U.S. government alone cannot maintain the country's technological supremacy. The ability to characterize and attribute threats, develop countermeasures, and respond rapidly to novel pathogens will depend heavily on the private sector, which needs to be not only a supplier but also an enduring national security partner. The United States must therefore maintain a strong private-sector AI and biotechnology ecosystem that is aware of emerging dangers and incentivized to work with the government to reduce them.

Meeting this challenge requires a sustained, deliberate effort to rebuild and protect the United States' capacity for biotechnology innovation. Over the last five years, American companies have become increasingly dependent on China for the components used in many drugs sold in the U.S. market and for access to the latest research in therapeutic molecules that can treat or cure diseases, creating substantial supply chain risks. The U.S. pharmaceutical industry is also acquiring a large number of Chinese biotech assets—buying the intellectual property and rights to develop Chinese drugs—particularly in innovative therapeutics. At the same time, it is competing to sell pharmaceutical products into the gigantic Chinese domestic market despite deep concerns that Beijing is stealing intellectual property.

Washington can tackle this challenge and strengthen American firms by revitalizing federal funding for basic science and investing in the human talent to win the biotech race. To do so, Congress should enact legislation that reduces growing dependencies on China and supports the U.S. biotech and pharmaceutical industries via targeted subsidies, public investment in research and development, tax incentives, and other measures. This bill might be modeled, in part, on the 2022 CHIPS and Science Act, which invested hundreds of billions of dollars in research and manufacturing for strategically important sectors. These actions should be paired with measures that expand protections for the United States' biotech innovation infrastructure, including the strengthening of a national security review process governing foreign investment in the sector. Incentives for collaborative development and production with aligned foreign partners should also be prioritized. In addition, Congress should immediately pass legislation to mandate that DNA synthesis companies screen customers and the sequences they order to prevent malicious actors from abusing this technology; this action needs to be synchronized with comprehensive efforts to strengthen the U.S. biotech innovation sector that can counterbalance the potentially onerous burden of such requirements.

MEET THE MOMENT

Pathogens know no borders. All countries should share the responsibility for preventing terrorists and

rogue actors from developing and using AI-enabled biology to perpetrate mass harm. But without American leadership, it will not be possible to build the global institutions, regimes, norms, and practices that advance U.S. interests in prevention and effective crisis response and help protect the entire world from AI-enabled biological attacks. To that end, the United States, in collaboration with close international partners, should launch a series of global biosecurity summits modeled on the four international nuclear security summits that took place from 2010 to 2016. The agenda could include setting common standards for DNA synthesis screening, generating market incentives for secure and resilient AI-biotech tools and systems, conducting pathogen surveillance, ensuring supply chain resilience, and pursuing responsible AI-enabled biotechnology development. Whether within this framework or parallel to it, China and the United States should establish a high-level, technically sophisticated dialogue on AI-enabled biological risk management.

On the home front, American frontier AI companies, such as Anthropic, Google, and OpenAI, have committed to testing their models and ensuring novice users cannot employ them to generate biological weapons. But these undertakings remain voluntary, their effectiveness has not been proved, and these companies' private incentives will inevitably diverge from public interests. The U.S. government should work concertedly with frontier AI companies and biotechnology developers to establish a framework for tiered access to the most sophisticated of AI-enabled bio models: an AI model trained not on words and text but on sequences of DNA that can predict, edit, and design novel proteins, cells, and viruses. They should also collaborate to establish and enforce specific guardrails for what these models can generate. This includes embedding safety features that prevent malign bioweapons development and embedding mechanisms that enable such misuse to be easily detected. It also includes establishing guardrails around what biodesign tools that facilitate the construction of novel proteins and cells are permitted to do—and how autonomous laboratories are allowed to operate, specifically with respect to whether human beings must remain in the loop to prevent abuse. Given the pace of innovation, responding to this multidimensional challenge will be an ongoing and iterative process. But this is not the first time the United States has tackled an emerging and potentially existential security threat. In the early 1990s, Indiana Senator Richard Lugar, a Republican, and Georgia Senator Sam Nunn, a Democrat, came together to enact landmark legislation that enabled the United States to prevent the proliferation of nuclear weapons and fissile materials after the collapse of the Soviet Union. Congress authorized and appropriated funds for a comprehensive and consequential series of actions—some unilateral and some cooperative—at home and around the world that ensured that the Soviet Union's nuclear legacy did not create multiple new nuclear nations and that terrorists could not access Soviet nuclear weapons or the essential components to build their own bombs and delivery systems.

With similarly visionary bipartisan action today, the United States can position itself to excel in developing hugely beneficial commercial applications of biotechnologies while also effectively monitoring, attributing, and responding to biological threats. This will require synergy and deft management between private-sector innovation and public interests. But the United States is capable of balancing these two imperatives. If a nationwide biological monitoring network that depends on private companies to provide services is established, it will offer continuous benefits, including early warning and attribution for a variety of risks. If the clinical trials system can be transformed, it will benefit consumers by strengthening the competitiveness of U.S. industry and onshoring more biotech production.

Coupled with investments and incentives for the American biomanufacturing sector, these measures will build up the infrastructure necessary to secure Americans against biological risks. That, in turn, will enable the country to respond promptly in the event of a deliberate attack and make it less vulnerable to supply chain disruptions. The United States will establish deterrence and therefore reduce risks, creating a virtuous cycle in which Americans can begin to have greater confidence in a bioresilient future.

Elizabeth Sherwood Randall is Ashton B. Carter Visiting Professor at the Harvard Kennedy School of Government and Founder and Director of the Initiative on Bioconvergence, Biosecurity, and Bioresilience at the Kennedy School's Belfer Center for Science and International Affairs. She served as White House Homeland Security Adviser and Deputy National Security Adviser from 2021 to 2025.

Building a Defense-in-Depth Biosecurity Strategy for the AI Era

Source: https://www.homelandsecuritynewswire.com/dr20260919-building-a-defenseindepth-biosecurity-strategy-for-the-ai-era

Sep 19 – The convergence of artificial intelligence (AI) and biology offers great promise for medicine and public health, including the potential to yield transformative societal benefits. Yet this same convergence could introduce serious global health and national security risks. As capabilities continue to advance, AI-enabled biotechnology might lower the technical, operational, and motivational barriers to creating biological weapons. It might also enable high-consequence attacks involving enhanced or novel pathogens. The dual-use nature of biotechnology requires proactive mitigation measures to counter these threats.

In a new report from RAND, the authors develop a defense-in-depth mitigation strategy that is robust, complementary, and deployable across a wide variety of threat scenarios. To create the strategy, the authors assessed the capabilities of various actor types across different steps of the bioweapon-development pathway prior to an attack, from ideation to weaponization. They also examined how different mitigations could add friction to primary milestones that nefarious actors must bypass to successfully execute an attack using AI-enabled biological weapons.

The authors describe a network of nine mitigations, each with their own strengths and weaknesses and areas of mutual reinforcement, and propose next steps for how decisionmakers in the public and private sectors can work collaboratively to advance this strategy.

Key Takeaways

- **Different threat actors require different prevention mechanisms.** Resource-constrained individuals might be thwarted at material or information access chokepoints. However, technologically sophisticated or well-resourced groups, such as state actors, might be immune to access controls and therefore require deterrence through elevated perceived costs and a degraded expected utility of attack.
- **Prevention must evolve beyond access controls alone.** Although restricting dual-use information and materials remains necessary, determined actors with sufficient resources can circumvent these barriers. An effective strategy, therefore, requires a complementary detection architecture that identifies and disrupts misuse patterns in digital and physical domains before they culminate in harm, shifting the paradigm from denial to integrated monitoring and early response.

- **Aggregate signals matter.** Threat actors operating across multiple nodes of the AI-biology ecosystem—probing different models, querying multiple synthesis providers, sourcing materials from separate vendors—produce signals that appear ambiguous when observed individually but form identifiable patterns of concern when analyzed collectively. Realizing this aggregate value requires centralized information-sharing infrastructure that no entity can provide alone.
- **Invest early.** Implementing this strategy's mitigations will require investments in new research, institutional adaptation, legal clarification, and international coordination. Waiting until more-advanced biological threats are undeniable will be waiting too long.

25 Years After Amerithrax: The Changing Landscape of Biosecurity – Analysis

By Aayushi Sharma and Ajey Lele
Source: https://www.eurasiareview.com/21092026-25-years-after-amerithrax-the-changing-landscape-of-biosecurity-analysis/

Sep 21 – The deadly attacks of 11 September 2001 were followed by another critical terrorist incident in the United States, wherein anonymous letters laced with the deadly anthrax spores were sent to several media companies and post offices. The attacks claimed the lives of five people through the inhalation of anthrax and infected several others who came in contact with the postal envelopes. The Federal Bureau of Investigation (FBI) codenamed the investigation 'Amerithrax'.[1] The 'Amerithrax Task Force' was created to determine the source of this terrorist attack. The FBI subsequently released an 'Amerithrax Investigation Report' detailing the course of the investigation.[2] The investigation focused primarily on scientists associated with the US biodefence establishment, especially the US Army Medical Research Institute of Infectious Diseases (USAMRIID) at Fort Detrick, Maryland.

The investigation subsequently went through a series of phases which were deemed controversial. Several scientists were designated as 'persons of interest' and came under surveillance and investigation. In several cases, the suspects also pushed back against the allegations of deliberately releasing anthrax. One known suspect, Steven Hatfill, a pathologist and a biological weapons expert, ultimately received a large government settlement after pursuing legal action over being falsely accused in connection with the attacks.[3] In 2008, another biodefence scientist, Bruce Ivins, a senior biodefence researcher at USAMRIID who was identified as the principal suspect, died by suicide.[4] The FBI formally closed the investigation in 2010, concluding that Ivins was the actual culprit and that he had acted alone. However, an independent scientific review found that the evidence was consistent with Ivins being the culprit, but still inadequate to conclusively establish his responsibility.[5]

Along with the rapid investigations, the anthrax attacks also triggered a major national public health and law enforcement response, widespread disruption to postal services, and extensive decontamination efforts. Executed only a week after one of the worst terrorist attacks in modern history, the anthrax attacks added to the already heightened threat perceptions regarding terrorism. As a result of these attacks, biological terrorism emerged as a public health, law enforcement, intelligence, and national security problem, highlighting the need for an integrated approach to addressing the threat. Biological terrorism or bioterrorism, however, was not a novel phenomenon. There have been numerous accounts of non-state actors using or attempting to use hazardous

biological materials as weapons to create widespread harm.[6]

This brief addresses response mechanisms, bio-surveillance, and emerging technology challenges to contextualize where the world stands today on bio-preparedness, 25 years after the 2001 Anthrax attacks. It explores the critical implications and opportunities for the Biological Weapons Convention (BWC) in shaping the future of global biosafety and biosecurity. The brief evaluates how two-and-a-half decades of science, technology, and policy evolution have shaped our preparedness against biological and toxic threats, and the challenges that persist.

Biodefence and Response Mechanisms

Response mechanisms and biodefence are a critical interdisciplinary field focused on protecting human life and agriculture. Key organisations involved include laboratories studying biological science, agricultural research centres, medical sciences, public health agencies, pharmaceutical companies, and national security agencies. Over the last 25 years, states worldwide have developed specific agencies associated with biological threats. Some states have developed advanced biodefence strategies and institutional mechanisms, while others are still working on them. It is also important to recognise that this threat has always been dynamic, so continued attention is required when deciding on response mechanisms and biodefence practices.

When it comes to addressing the risks posed by biological weapons, it is important to focus on the unique characteristics and vulnerabilities regarding biological agents. These agents include infectious pathogens and biotoxins that are non-transmissible. These weapons often have delayed effects and variable incubation periods, which add to the challenges of building robust response mechanisms for such threats. The case of anthrax attacks in the US made it fundamentally clear that investigations into biological weapons attacks are often met with attribution challenges. The challenge of effective attribution persists and is often exacerbated by rapid advances in biotechnology and easily accessible biological design tools.

The fragmented nature of biological weapons dissemination also challenges preparedness and response. While in the US, anthrax spores were dispersed through the postal mail, such agents can also be disseminated through aerosols or even contamination of important resources such as crops or water supplies, causing widespread damage. Therefore, as these threats rapidly evolve, delivery mechanisms for such agents are easily accessible to non-state actors, further complicating attribution.

The 2001 anthrax attacks exposed massive vulnerabilities in the public health detection and response systems, intelligence gathering, and inter-agency coordination mechanisms in the US. The US hence worked to build national capacities through the Public Health Security and Bioterrorism Preparedness Act of 2002 to strengthen prevention, preparedness, and response mechanisms against biothreats and to develop stringent standards for securing dangerous biological agents. The Act also imposed strict regulations on the possession, use, and handling of specific biological agents. To build on these response capabilities, Congress enacted the Project BioShield Act in 2004, which incentivised companies to research, develop, and stockpile medical countermeasures against CBRN threats.[7] Incentivising research in medical countermeasures also heightens capabilities to address novel bio-risks and leverage technological advancements to improve detection and response mechanisms.

Globally, funding surged for biodefence and preparedness research, as well as for high-containment facilities, to build scientific, defence, and policy capabilities to counter such threats.[8] The preparedness gaps to deal with bioterrorism threats were significantly highlighted in the

aftermath of the anthrax attacks. The World Health Organization (WHO) developed the International Health Regulations in 2005 to legally require signatory countries to build national capacities for detecting, analysing, and surveilling public health emergencies of international concern.[9]

Additionally, the Global Health Security Initiative (GHSI) emerged in 2001 as a cross-regional multilateral grouping to improve cooperation in public health preparedness mechanisms to respond to CBRN terrorism threats, with WHO as the technical advisor.[10] The anthrax attacks thus led to growing attention on improving biodefence, international coordination in public health preparedness, and response capabilities, not just within the US but worldwide.

Thus, in 2001, bioterrorism emerged as a pressing challenge requiring coordination across public health, national security, and law-and-order agencies. However, contemporary issues relating to emerging technologies, AI integration, dual-use research of concern (DURC), and the evolving capabilities of biotechnology are creating new pathways to biological misuse and redefining the biosecurity landscape.

Bio-Situational Awareness and Intelligence Gathering Mechanisms

One of the most effective ways to address novel threats is to build robust disease surveillance systems that track unusual occurrences that may signal a public health emergency. Disease surveillance is therefore a key pillar of early recognition and detection. Bio-surveillance essentially involves gathering and analysing relevant data to provide periodic information on biological threats affecting human, animal, plant, and environmental health. Strong bio-surveillance systems build bio-situational awareness and early detection, improving national and global capacities to address bio-risks.

Various approaches may be used to develop such systems, such as syndromic surveillance, which involves gathering data through public health officials reporting on suspected threats based on the reported symptoms of a given population, or event-based surveillance, which involves a wider range of information systems involving newspaper reports, social media, or publicly reported incidents.[11] Epidemiological studies have also become central to early detection by understanding disease patterns and transmission.

However, the anthrax attacks revealed that public health surveillance may not only deal with accidental bio-risks but also deliberate attacks. The resulting policy shift led the US to treat biological risks as a national security problem. The Department of Homeland Security created the BioWatch system as a direct result. BioWatch served as an early-warning system to detect the aerosolised release of certain pathogens through a network of sensors.[12]

Gathering public health data and developing bio-situational awareness is beneficial not only in the context of deliberate biothreats but also accidental ones. Therefore, even after 25 years of terrorist attacks using anthrax, efforts are underway to develop global bio-surveillance mechanisms to build transnational capacities to tackle such threats. Integrated bio-surveillance efforts would require simultaneous data collection from several sources, including public health institutions, high-containment laboratories, pharmacies and wastewater facilities.[13] Current efforts extend surveillance beyond public health data to include animal, plant, and environmental health. This One Health approach to bio-surveillance and intelligence gathering requires active global cooperation frameworks that go beyond national implementation.[14]

To build global coordination mechanisms, organisations like the WHO have worked to develop early warning detection systems and transnational response systems to address the threats posed by pathogens with pandemic potential. WHO has

several initiatives, including the International Pathogen Surveillance Network (IPSN) and the Global Outbreak Alert and Response Network (GOARN), which provide technical coordination to identify and respond to public health emergencies.

The Epidemic Intelligence from Open Sources Initiative (EIOS) and the WHO Hub for Pandemic and Epidemic Intelligence also provide technical assistance to countries to improve detection and monitoring capabilities.[15] While these initiatives exist, building an integrated approach to intelligence sharing and data gathering, along with inter-agency coordination, such as the World Organisation for Animal Health (WOAH) and the Food and Agriculture Organization (FAO), for a One Health framework remains a challenge.

Translating these bio-surveillance capabilities into effective early warning systems also comes with its own set of nuances. For global early warning systems to work well in deliberate and accidental disease outbreaks, capacities need to be built towards interoperable systems capable of operating in diverse demographic and geographic settings.[16] One major driver of continued efforts to build better, more integrated bio-surveillance, early warning, and detection systems is the increased perception of biological risk in recent years. Even after more than two decades of anthrax attacks, the challenge of keeping biological weapons capabilities out of the hands of non-state actors persists due to the novel risks posed by artificial intelligence (AI) as well as developments in biotechnology.

Emerging Technologies: Boon and Bane

Rapid advances in biotechnology, synthetic biology, gene editing, AI and related technologies are strengthening biodefence while simultaneously lowering barriers to biological misuse. Developments in biotechnology continue to offer immense potential to enhance biological defence capacities by supporting research into rapid detection, diagnosis, and improved medical countermeasures, including vaccine development and other prophylactic treatments. Advances in life science research capabilities have also expanded the potential of gene sequencing methods such as metagenomic sequencing to provide simultaneous, independent analysis of the total genetic material in a sample.[17]

Biotechnology developments, when considered alongside accessible AI integration, also present opportunities to improve drug discovery, vaccine development, and other pharmaceutical interventions. AI models can also help with biological data analysis, as well as structuring and synthesising large databases to support research. Targeted attention is also being paid to improving medical measures against drug-resistant bacteria and viruses through frontier AI models along with improved gene editing capabilities.[18] Therefore, a case can be made for responsible and governed use of AI in biotechnology and life science research. This integration could help address longstanding concerns and improve the biosecurity landscape.

While the opportunities presented by AI and biotechnology are widely recognised, they are also accompanied by concerns about potential risks, especially in the absence of integrated governance and regulatory frameworks. Improvements in biotechnology capabilities over the years have also created space for faster, cheaper, and more accessible DNA synthesis technologies, driving market expansion among DNA synthesis providers. However, screening protocols for ordered DNA sequences have not been implemented to the same extent.

These capabilities require structured, standardised, and uniform screening regulations to verify customer identities comprehensively. These regulations are crucial for ensuring that DNA sequences of potentially dangerous pathogens are only provided to legitimate

research facilities with adequate institutional biosafety standards in place. Currently, DNA providers primarily belong to the International Gene Synthesis Consortium, a commercial group of providers in the global market.[19] The Consortium has established the Regulated Pathogen Database (RPD) to verify given orders and detect the sequences of concern.[20]

They may either conduct customer screening to establish the identity of the ordering parties or screen the sequences ordered to identify potentially dangerous and controlled pathogens or biotoxins. However, without a legal mandate within the Consortium, screening DNA synthesis orders before fulfilment is largely voluntary. This staggered safeguards landscape creates gaps in screening and contributes to biosecurity concerns about unregulated access to hazardous biological materials.

The integration of AI into this biotechnology landscape therefore adds another layer of complexity. While certain frontier AI models may be instrumental in synthesising large datasets to aid biological research, they may also lower technical thresholds, especially open-source large language models (LLMs), by disseminating information on biological design.[21] A study auditing 32 LLMs found that most complied with requests to design and generate novel toxin sequences.[22] Similarly, recent scientific research shows that generative AI models can develop genome sequences for novel viruses that target bacteria resistant to natural bacteriophages.[23] This development also raised concerns about diverting these capabilities to engineer drug-resistant, human-infecting viruses.

Safeguards on the end of AI developers also become significant in this case. Anthropic's newer models have safety classifiers in place, with evaluations conducted on refusal benchmarks to assess the models' ability to handle prompts related to the hazardous use of biological weapons.[24] However, despite these mechanisms, Anthropic's recent threat assessment report revealed several attempts to bypass the safety classifiers and retrieve questionable information on gene editing of infectious pathogens and toxin design.[25] Thus, in the context of deliberate biothreats, greater access to bio-design tools and open-source AI platforms equipped with the requisite knowledge are among the most pressing challenges in the current global biosecurity discourse.

Strengthening Global Norms for Biosecurity

Biosecurity is a crucial pillar of the international security architecture. Considering the broad spectrum of biological risks, ranging from natural and accidental outbreaks to deliberate weaponisation of infectious pathogens and biotoxins, the global norms on biosecurity are embedded in various institutional mechanisms. Major international frameworks on deliberate biothreats include the Biological and Toxin Weapons Convention (BTWC) and UNSCR 1540, while the WHO sets norms for public health issues such as biosafety standards, disease surveillance, detection, preparedness, and response mechanisms. The voluntary export control groupings such as the Australia Group are significant in managing transnational trade in controlled substances with relevance to chemical and biological weapons.

The 'biological weapon taboo', or the perceptions against the use of biological materials as weapons, was recognised through the prohibition of use under the 1925 Geneva Protocol.[26] This development was further strengthened and legally enforced through the Biological and Toxin Weapons Convention (BTWC), which entered into force in 1975.[27] While the BTWC has largely succeeded in establishing the norm against biological weapons, contemporary challenges relate to enforcing these norms through practical frameworks that adequately address emerging risks.

The Convention legitimises the use of

biological materials for peaceful life science research while prohibiting any use not intended to be peaceful. In theory, this may seem like a significant qualifier for what the regime permits and prohibits. However, questions and uncertainties arise as the dual-use characteristics of life science research and subsequent AI integration in biotechnology take shape. With frontier AI models, scientists are increasingly studying capacity-building in medical countermeasures to address drug-resistant pathogens, which requires careful use of gene-editing technologies. However, the same capabilities can also be diverted towards more lethal use of genetically engineered pathogens for harmful purposes. Therefore, without international verification mechanisms, determining the legitimacy of biological research for peaceful purposes becomes a mammoth challenge for the existing regime.

Current structural challenges in the Convention also include the lack of a Science and Technology Advisory Body to monitor and routinely conduct a scientific review of the treaty. This development would be necessary to adequately assess the Convention's capacity to address emerging biosecurity risks. The ongoing working group discussions to strengthen the Convention are a significant step forward in this regard. The Convention's scientific capacities can also be enhanced by developing networks of high-containment laboratories with strong biosafety standards.

The Organisation for the Prohibition of Chemical Weapons (OPCW) has provided a precedent for such a structure, with designated biomedical and environmental facilities also in place.[28] Such a network for the BTWC could facilitate independent, regulated research into sequencing novel pathogens and toxins to develop stronger verification mechanisms for the treaty. Building effective regulatory practices without infringing on or curtailing scientific progress is a pressing challenge for the BTWC.

Alongside laboratory security measures, research verification, international cooperation and compliance, efforts to prevent misuse by non-state actors are also significant to strengthening global biosecurity norms. The anthrax attacks of 2001 widened the perceptions around biosecurity to include the threats posed by non-state actors as well as inadequate regulatory oversight of research facilities. Hence, stronger norms backed by practical frameworks are essential for improving biosecurity in response to bioterrorism threats.

Deliberations at BWC review conferences signal a careful yet staggered recognition of the threat of bioterrorism. The final declaration of the seventh review conference of 2011, for the first time, condemned terrorism 'in all its forms and manifestations' in the context of using biological agents, further highlighting the role of UNSCR 1540.[29] In the absence of verification and implementation mechanisms for the Convention, instruments such as UNSCR 1540 and its oversight mechanism through the 1540 Committee provide important frameworks for advancing global security protocols against bioterrorism.[30]

Given the plethora of emerging challenges surrounding synthetic biology, open-source AI models, and rapidly evolving biotechnology capabilities, institutionalising appropriate safeguards and building an integrated approach is essential to strengthening biosecurity normative frameworks.

While the anthrax attacks presented a case of deliberate use of biotoxins to inflict harm, hence a biological weapons attack, the experience of COVID-19 presented the need to consider pandemic preparedness and response as an international security issue.[31] Many response and biodefence capabilities that support defence against accidental biothreats and natural outbreaks also support defence against deliberate threats. Thus, lessons should be learned from the COVID-19 pandemic of 2020, and the institutional inadequacies that hindered global coordination should be addressed to build international capacity.

Conclusion

The anthrax attacks of 2001 revealed that mitigating biological threats requires an integrated approach towards bringing together public health, law enforcement, bio-surveillance and national security frameworks. Twenty-five years later, amid a rapidly advancing emerging risk landscape, the reality remains the same. The COVID-19 pandemic of 2020 is particularly significant in this regard. The pandemic exposed gaps in current detection and preparedness capabilities and underscored that global biodefence mechanisms must support robust, transnational early detection and response.

Developments in biotechnology, synthetic biology, gene editing, and AI models offer immense opportunities to advance life science research. Still, they also heighten concerns about access to biological materials, lowered technological thresholds, and deliberate misuse. While AI integration in biotechnology cannot replace tacit laboratory knowledge, institutions need to strengthen biosafety mechanisms and regulatory oversight to prevent accidental exposure and outbreaks. Similarly, safeguards around DNA synthesis acquisition and screening mechanisms are essential to reduce perceived threats around the availability of controlled and high-risk sequences.

Additionally, effective bio-surveillance mechanisms become important for improving early-warning systems, preparedness, and detection capabilities. While national frameworks for addressing bio-risks exist in practice, existing international frameworks are still essential for building multilateral and transnational capacity against these risks. Efforts are underway to address longstanding issues in the BTWC, especially regarding legally binding verification mechanisms, international assistance and cooperation, and stronger compliance.[32] While these developments largely reflect state obligations, continued deliberations on threats posed by non-state actors are also crucial within the Convention.

After more than two decades, the anthrax attacks provide a strong vantage point to evaluate the priorities of the existing biosecurity landscape. The experience of anthrax and COVID-19 indicates that biological threats cannot be treated simply as low-probability possibilities. Sustained investment in prevention, detection, attribution, medical countermeasures, and international cooperation remains essential.

Aayushi Sharma is a Research Analyst at Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), New Delhi.
Group Captain (Dr) Ajey Lele (Retd.) is the Deputy Director General, MP-IDSA. Earlier, he was a Senior Fellow at the Manohar Parrikar Institute for Defence Studies and Analyses and a part of its Centre on Strategic Technologies. He started his professional career as an officer in the Indian Air Force and took early retirement from the service to pursue his academic interests. He has a Master's degree in Physics from Pune University, and Master's and MPhil degrees in Defence and Strategic Studies from Madras University.

Are countries making bioweapons? 'Bioaudits' could help find out

By Filippa Lentzos

Source: https://thebulletin.org/2026/09/are-countries-making-bioweapons-bioaudits-could-help-find-out/

Sep 18 – More than half a century after the Biological Weapons Convention (BWC) entered into force, it still has no standing system for verifying compliance. Since the last major attempt at closing that gap failed 25 years ago, the need for a verification provision is becoming harder to

ignore. Biotechnology is more powerful, more widely distributed, and increasingly digital. A backdrop of geopolitical mistrust makes allegations about prohibited biological activities harder to resolve—and confidence in compliance is becoming harder to sustain on national assurances alone.

It has always been a high bar to expect a BWC verification system to deliver a binary "compliant" or "non-compliant" judgment—all biotechnology has permissible and beneficial uses. But properly assessing compliance has become even more challenging than it might have been in 2001, when states parties made significant headway on verification. Back then, verification proposals could still center largely on declarations and visits to identifiable physical facilities, such as biodefence laboratories and vaccine-production plants. Now, in a time of rapidly developing biotechnology, a digital genetic sequence might pose as much of a potential bioweapons threat as a live virus sample.

Still, BWC member states see the need for

A biology lab in the United Kingdom. Financial-style audits of biological governance and infrastructure are a tool that countries could use to help verify compliance with the Biological Weapons Convention. Credit: John Sotton via Wikimedia Commons. CC BY-SA 2.0.

treaty verification. And next year they could approve a formal working group to explore the contours of a future regime. And when they do, they should seek to build a verification scheme that generates robust, independently acquired and mutually intelligible evidence.

Allegations of treaty violations have often been colored by geopolitical tension as adversaries cast suspicion on one another's biological activities. By developing a trusted source of factual information on compliance issues, treaty compliance discussion can rise above political distrust. Through the use of tools like financial-style audits of biological governance and infrastructure, they can become more than just easily dismissed assertions.

A complex effort

States last began to try and close the verification gap in the 1990s. An organization known as the Ad Hoc Group spent several years negotiating a legally binding protocol built around declarations of relevant facilities and activities, clarification procedures, visits and investigations. By 2001, a detailed composite text existed, but disputes persisted over how intrusive the system should be, whether it could reliably detect cheating, and how to protect sensitive commercial and national-security information. In July 2001, the United States rejected the draft protocol, arguing that it would not provide meaningful confidence in compliance and could expose sensitive information; later that year it also opposed continuing the Ad Hoc Group's mandate. The process collapsed.

Recent momentum to revisit verification is emerging as BWC states parties have been negotiating recommendations on how to strengthen the treaty. The current strengthening process is broader than verification, with states also examining—among other topics—how the treaty should keep pace with scientific and technological change,

how to improve confidence-building, and how to strengthen international cooperation.

Now states parties are weighing whether to create a new working group on compliance and verification issues. Its remit could include declarations, on-site and off-site approaches, scientific and technological developments, institutional arrangements, investigations, and, importantly, how different verification measures might complement one another. Whether to establish such a working group will ultimately be decided in 2027, when BWC delegates meet for the once every-five-years treaty review conference. Instead of trying to resurrect a verification architecture designed for the biotechnology of the 1990s, states could ask a more fundamental question: What should verification mean for the biology we actually have today?

Biology is different

The BWC does not prohibit bacteria, viruses, fermenters, DNA synthesizers, laboratories, or vaccine plants. Almost everything that could contribute to a biological weapons program also has legitimate peaceful applications. The treaty's central organizing principle is therefore what's known as the "general purpose criterion": Biological agents and toxins are prohibited when their type or quantity cannot be justified for prophylactic, protective, or other peaceful purposes. Ultimately, the distinction between permitted and prohibited activity turns on purpose.

That has always made verification difficult. Today it is harder still. Biotechnology is becoming more widely distributed, and capabilities relevant to biological weapons increasingly reside not simply in pathogens or specialized pieces of equipment but in data, automation, engineering expertise, artificial intelligence, and distributed manufacturing. There is consequently no biological equivalent of simply counting nuclear warheads or accounting for tons of declared chemical agent.

Compliance is ultimately an assessment of evidence that must be interpreted in context.

At present, transparency under the BWC rests largely on annual confidence-building measures, through which states provide information on matters including relevant laboratories, biodefense programs, unusual disease outbreaks, national implementation measures, past biological weapons programs, and vaccine-production facilities. These measures can reduce ambiguity and suspicion, but they rely on information supplied by states themselves and do not constitute verification.

As BWC delegates consider the issue, they should consider what role "bioaudits"—an idea raised in a 2025 Hoover Institution report—could play. Under this concept, professional, independent third parties would scrutinize university laboratories, biotechnology companies, and government facilities for weaknesses in biosafety, biosecurity, dual-use governance, and operational compliance—with the auditors themselves being accredited and held to common professional standards.

In the corporate world, financial regulators do not conduct financial audits because they assume every company is dishonest—but neither do investors, regulators, or markets simply take corporate claims on trust. Independent scrutiny creates a reason for confidence. Bioaudits would take a similar form to financial auditing.

The report also briefly proposes coupling bioaudits to the BWC. My argument here is broader: Bioaudits could become one component of a layered BWC verification system. They could help to generate independent evidence on which justified judgments can be built, building what I call "justified compliance."

Crucially, an audit would not establish categorically that a state is complying with the BWC. After all, a laboratory could pass a rigorous biosecurity audit

while a clandestine program operated elsewhere. And a state deliberately violating the BWC is hardly likely to volunteer its secret weapons facilities for inspection by a third-party auditor. These objections, however, are not arguments against bioaudits. Instead, they tell us where bioaudits fit in the bigger picture. Effective, biological verification should be constructed in layers.

One layer is routine transparency. This would involve things like engaging in BWC confidence-building measures, declarations, voluntary visits, and releasing publicly available information. Bioaudits would serve as a layer to provide assurances about how biologically-relevant institutions are operating. Another layer would comprise national regulation, licensing of labs, and inspection of facilities. Above that might sit a layer of international verification measures, including declarations, visits, and technical assessments. The most coercive layer might be mechanisms for investigating suspected non-compliance or alleged biological weapons use. None of these layers would answer every verification question, but together they can generate something much stronger. A bioaudit could, for example, substantiate information contained in a national declaration. Internationally recognized audit standards could make information about laboratories more comparable across countries. Audit findings might reveal anomalies requiring regulatory attention.

Conversely, evidence that facilities conducting specified categories of work are subject to credible independent scrutiny could increase confidence in a state's national implementation system.

Voluntary to mandatory?

Developing a bioaudit system raises many difficult questions.

Who sets the standards? How is auditor independence protected? How much information is reported publicly or internationally, and how much remains confidential? How are conflicts of interest and "audit shopping"—where organizations attempt to seek a favorable auditor—prevented? How could developing countries participate without bioauditing becoming another costly condition attached to biotechnology? And which activities are sufficiently consequential that governments might eventually require audits rather than simply encourage them?

Indeed, participation could initially be voluntary at the BWC level while becoming mandatory domestically for defined classes of institution or activity. Financial auditing again offers a useful analogy: Audits are optional for some organizations and legally required for others. "Voluntary," therefore, need not mean weak.

A sensible first step could be modest. Interested BWC states, scientific organizations, standards bodies, laboratories, and professional auditors could begin developing and testing common audit methodologies. States could explore what minimal information from an audit—its scope, standard, accreditation, outcome, and remediation status, to name a few examples—might usefully accompany national BWC reporting without exposing proprietary or security-sensitive information.

If states eventually agreed to a mandatory verification framework, accredited bioaudits could become one required component for defined categories of facilities or activities.

Bioaudits would not be a substitute for declarations, international inspections, or investigations. Ideally, they would provide independent assurance about what actually happens inside the laboratories and organizations performing modern biotechnology. They may turn out to be an important missing layer.

The verification debate now opening in Geneva should therefore resist the temptation to ask which single instrument can "verify the BWC." The better question is what combination of independent, mutually reinforcing measures can

make confidence in compliance progressively more justified. Twenty-five years after the last attempt at BWC verification failed, that would be a genuinely new place to start.

Filippa Lentzos is an associate professor in Science & International Security at King's College London, where she leads research projects on global biolabs, disinformation, responsible science, and BWC verification. She is an associate senior researcher at the Stockholm International Peace Research Institute in Sweden, and a non-resident scholar at the James Martin Center for Nonproliferation Studies in the United States. Lentzos chairs the WHO Technical Advisory Group on the responsible use of the life sciences and dual-use research, and she is a member of the WHO Health Security Interface–Technical Advisory Group. She is also a rostered expert for the UN Secretary-General's Mechanism for Investigation of Alleged Use of Chemical or Biological Weapons, and serves as NGO Coordinator for the Biological Weapons Convention.

Rue de la Vacherie, 78 | B5060 SAMBREVILLE (Auvelais) | Belgium
https://www.ici-belgium.be/