

2 CBRNE DIARY

International CBRNE INSTITUTE

11\26

November 2026

Dedicated to Global First Responders

PART A

CBRN morgue

Hospital lockdown

Targeting FRs

Night operations

UAV CWA antidotes delivery

Freezer hacking

FPV drone googles trapped

Global cyberattacks

An International CBRNE Institute publication

C²BRNE DIARY ❁ 2026®

November 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)
Ex Editor @ ASPISMEDICAL, CTM-E (UK)
Epanomi, **Greece**

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

EDITORIAL TEAM

- **Bellenca Giada,** MD, MSc (Italy)
- **Bossis Mary,** PhD, Intern/EU Studies (Greece)
- **Hopmeier Michael,** BSc/MSc MechEngin (USA)
- **Khadra Joelle,** Lecturer, CBRN Women Project Leader (Lebanon)
- **Kiourktsoglou George,** BSc, Dipl, MSc, MBA, PhD (UK)
- **Marx Julien,** CCNurse, MSc, PhD cand | MoTransport (France)
- **Photiou Steve,** MD, MSc Em Disaster (Italy)
- **Tarlow Peter,** PhD Sociol (USA)

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

DISCLAIMER: The C²BRNE DIARY® (former CBRNE-Terrorism Newsletter), is a free online monthly publication dedicated to fellow civilian/military CBRNE First Responders worldwide. The Diary is a collection of papers and articles related to the stated thematology. Relevant sources/authors are included and all info provided herein is from open Internet sources. Opinions and comments from the Editor, the Editorial Team or the authors publishing in the Diary DO NOT necessarily represent those of the International CBRNE Institute (BE).

●▶ Occasional advertisements are free of charge

International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY



Topics that attracted attention!

EDITOR'S CORNER

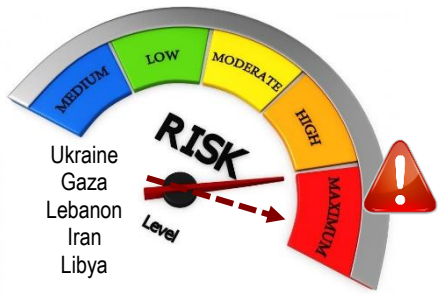




Editorial

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

Editor-in-Chief
ICI C²BRNE Diary



Dear Colleagues,

The global situation remains bloody stable, with a chance to become even worse! US offensive plans for Cuba and Somaliland are not forgotten, just put aside for the time being.



Congo: Data released today by the government of the Democratic Republic of the Congo show that the death toll from the Ebola virus has reached 5,683, while confirmed cases stand at 11,645 (CDC). Mortality: 48.7%. **First 9 cases in Nigeria; two deaths in Kenya!** Two vaccines—ChAdOx1, developed by the University of Oxford and the Serum Institute of India, and mRNA-1469, from the American company Moderna—will be added to the Tumaini clinical trial, which began on October 23 and employs the ring vaccination method, prioritizing individuals who have been in contact with confirmed cases. **Cholera:** 60,000 cases; 1,800 deaths. 80 attacks against healthcare facilities.

▶ A British healthcare worker infected with Ebola is being medically evacuated from the DRC to Britain for specialist treatment, according to an official document seen by Reuters. The patient has been sent to the DRC by a humanitarian organization to help support the response to the outbreak.



Ukraine: Ukraine's financing needs for 2027 amount to €115 billion, according to Volodymyr Zelenskyy in an interview with the Ukrainian media outlet TSN, as Kyiv seeks additional resources to cover defense costs and state budget requirements. The Ukrainian president noted that €45 billion has already been pledged by international partners; however, these funds have not yet been disbursed. Stop the f* war! NOW! We have better ways to spend our money!



▶Ukraine and Russia were hit by **fake nuclear threat alerts** just hours apart. It started in Ukraine, where the country's air raid warning app suddenly told people in Kyiv that radiation had been detected. But that wasn't all. More alerts followed, warning of a chemical attack, street fighting, and even a Russian Oreshnik missile heading toward Ukraine. The Ukrainian Air Force quickly told people there was no radiation threat and warned that the app had likely been hacked. And just hours later, Russia reported a similar attack. Its emergency alert app began sending fake nuclear warnings, with some messages reportedly telling people to stock up on supplies and



hide in basements. A Ukrainian partisan group called Atesh claimed responsibility for hacking the Russian app, although that claim hasn't been independently verified.



Sweden: Sweden opts for a coronavirus protein vaccine instead of mRNA. From the 2027/2028 season onwards, Sweden will use **only** a protein-based coronavirus vaccine (Nuvaxovid) for its national vaccination campaign. It is the first country in the world to say goodbye to mRNA vaccines. **Nuvaxovid** utilizes traditional recombinant DNA technology. It contains the virus's spike protein—produced in a laboratory—combined with an adjuvant that stimulates the immune system. The body is exposed directly to the protein, prompting the development of antibodies, without any interference with cellular mechanisms.

Germany: Iran warns Germany that its military bases and facilities across the region will be considered legitimate targets if Berlin openly joins a military operation against Iran, according to Fars News.

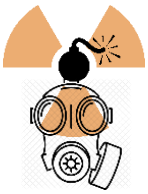
Russia: A Bulava ballistic missile was launched from a nuclear-powered submarine submerged in the Sea of Okhotsk—in the Russian Far East, north of Japan—with its warheads striking their target in the Russian Far North, near the border with Finland, after covering a distance of 8,300 km!
▶ US intelligence agencies, including the Defense Intelligence Agency (DIA), have expressed serious concern regarding the development of a Russian space-based anti-satellite weapon designed to carry a nuclear power source or a nuclear warhead into orbit, reports FoxNews.com. This system is not intended to strike ground targets; rather, it is designed to emit a destructive **electromagnetic pulse** (EMP). Such an event could blind or disable thousands of satellites in low Earth orbit (LEO), crippling global telecommunications, navigation systems, and financial transactions, and triggering a global, cascading economic collapse.

Afghanistan: Opium production in Afghanistan has seen a significant increase, despite the ban on opium poppy cultivation imposed by the Taliban in 2022. According to UN data, production has increased fivefold in a single year, as a growing number of farmers find ways to circumvent the restrictions. Opium production in Afghanistan rose by 400% year-on-year, based on figures released by the United Nations. Specifically, output climbed from 300 tonnes to nearly 1,500 tonnes—the first major surge since the Taliban's ban on opium poppy cultivation. During the same period, the area under cultivation expanded by 330%, growing from approximately 10,000 hectares in 2025 to over 43,000 hectares in 2026. Despite this striking rise, both production levels and the area under cultivation remain significantly lower than they were before the ban was implemented. At that time, opium poppy cultivation covered approximately 232,000 hectares, while Afghanistan accounted for nearly 80% of the global opium supply. It seems that the US occupation failed to transform Afghans into New Yorkers!



USA (TX): An extremely concerning dimension of Turkish penetration—and the use of the Islamic factor as a tool for foreign policy and espionage—has come to light in the United States. According to revelatory information that has sparked a political uproar, at least three Islamic mosques in the state of Texas are directly funded, staffed, and directed by the Turkish government. These mosques—located in Dallas (in the Richardson area), Houston, and Austin—are openly and officially linked to the notorious Diyanet (Turkey's Directorate of Religious Affairs) through its branch, "Diyanet America."

▶ The Federal Aviation Administration (FAA) issued a rare nationwide "ground stop" order, effectively closing the country's airspace to all takeoffs. More than 10,000 flights have been delayed, and over 3,000 have been canceled. The measure was imposed due to "extraordinary circumstances" and for serious "safety reasons." The cause? Earlier in the week, the implementation of a flight control system utilizing AI technology began. This initiative collapsed when it became apparent that many of the systems were incompatible! This occurred on the same day that Microsoft experienced a global email outage, and U.S. bases at RAF Lakenheath, Mildenhall, and Feltwell faced security alerts.



▶▶▶ US intelligence has reportedly identified detailed **Iranian plans** for potential attacks on US soil, including the use of unconventional weapons (RDD, CWA). CNN says the plotting is not considered evidence of an imminent attack, and sources say it is unclear whether Iran has operatives in place. The plotting picked up by the US has been very specific and includes locations (Washington DC) and targets. Provocation or reality?

Iran: Tehran designated two of the United Kingdom's primary military branches—the Royal Navy and the Royal Air Force—as terrorist organizations.

▶ General Mohsen Rezaei, Secretary of the country's Supreme National Security Council, stated that any potential new American military operation would trigger retaliation that would not be limited to U.S. facilities in the Middle East. Iran's hardline state-run newspaper *Kayhan*—published under the supervision of the Supreme Leader's representative—is calling for missiles to be launched against U.S. bases in Europe. It identifies **Germany, Britain, Albania, Greece, and Cyprus** as targets, stating that "the enemy will now hear the roar of the new missiles of the Revolutionary Guards' Aerospace Force."

▶▶ Iran declares Argentine Navy and Air Force as terrorist organizations.

▶▶▶ In an unprecedented diplomatic scandal that has sparked global outrage, Iran has managed to secure election—with 144 votes—to a key United Nations committee. This body is responsible for setting guidelines on issues including human rights, gender equality, disarmament, and counterterrorism. The very same regime that was expelled from the Commission on the Status of Women in December 2022 has now managed to get back in "through the back door," securing a seat on the Committee for Programme and Coordination (CPC) for the 2027–2029 term.





Israel: Israel is planning to drop a nuke on Iran's Pickaxe Mountain if the US refuses to do so, claims Yaakov Nagel, former Israeli National Security Adviser and intelligence official. The explosive claim is fueling fresh speculation over how far Israel could go to destroy Iran's underground nuclear facilities.



European airports: A total of seven **bomb threats** were recorded over the last two days involving aircraft heading to European airports; all proved to be false alarms, according to statements from the affected airport authorities. The threats concerned two flights to Warsaw—one from Copenhagen and another from London Heathrow—as well as a flight from Manchester to Murcia, and two others from Bergamo and Dublin to Sofia. These incidents follow an event a day earlier, in which a Wizz Air aircraft flying from Luton Airport in England to Sofia made an emergency landing in Budapest, escorted by two Hungarian fighter jets. On Sunday (November 1), an Austrian Airlines flight from Tel Aviv to Vienna was diverted to Bulgaria. No explosives were found on board the aircraft. On November 3, an incident occurred involving a SAS flight from Copenhagen to Warsaw Chopin Airport.





Nov 05: Bomb threats go viral across Europe against airlines, airports, and TV stations (RTE, Sky, NovaTV, TF1). ■ The top-secret internal communications network of the US National Security Agency (**NSA Net**) in Maryland has been taken offline,

KSA: The official spokesperson for the Coalition to Support Legitimacy in Yemen, Brigadier General Turki Al-Maliki, announces the interception and destruction of a drone in the Makkah Al-Mukarramah region. Zaydis (Shia) versus Wahhabis (Sunni)!
▶ The tallest skyscraper in Riyadh, Saudi Arabia, sustained serious damage following an attack by the Houthis of Yemen. According to Reuters, the target of the attack was the Public Investment Fund Tower (PIF Tower)—an 80-story skyscraper that houses the headquarters of Saudi Arabia's sovereign wealth fund. Perhaps they should reconsider the (in progress) Jeddah Tower project (1km high; 167 floors) since t seems that they cannot protect vertical constructions. Besides, who is going to buy a flat or an office or live there under current and future fragile situation?

Poland: Armed terrorist attack in Kraków, Poland (Nov 07). According to a statement by Kraków City Hall citing the Małopolska police, 10 people were killed (including the terrorist [the day after] - 3 at the perpetrator's home in Ostrowiec Świętokrzyski), and 16 were injured (8 in serious condition) in the attack near the Main Square. The terrorist (Michał Oksiński, a 24-year-old Polish citizen), who reportedly opened fire with an AR-15 rifle from a black Subaru, was shot and apprehended by police. Reports indicate that the perpetrator wore a patch belonging to the American tactical/training group Forward Observations Group (FOG), or that he had served as a volunteer/mercenary in the International Legion, fighting for Ukraine. The two police officers who were seriously wounded while attempting to stop the perpetrator were exceptionally fortunate. Two prominent surgeons from Kraków happened to be dining at a restaurant next to the scene of the shooting; they were captured on camera assisting the wounded immediately after the incident. In fact, one of the two surgeons—Professor Michał Pędziwiatr—later performed surgery on one of the officers at the hospital. The other physician, Dr. Mateusz Wierdak, is also considered a leader in his field. A similar **coincidence** happened during the fourth bomb of the 7 July 2005 London terrorist attacks that exploded directly outside the British Medical Association (BMA) House – approximately 15 doctors who were inside BMA House rushed outside to help. The building's courtyard was transformed into an improvised field hospital, where casualties received initial treatment before transportation to hospitals.



Korea: North Korea is amending its Constitution, recognizing South Korea as an independent state for the first time and abandoning the doctrine of "unification" of the peninsula—which means that Pyongyang is making peace with Seoul after 73 years!

Jordan: Three men in Jordan have been sentenced to death by hanging after being found guilty of a bloody attack on a Greek Orthodox church in the village of Hamoud, in the Karak Governorate, last October. The attack resulted in the deaths of nine people, while another 25 were injured. The three gunmen had entered the grounds of St. George's Church while a funeral service was taking place and opened fire on those present. According to the Catholic organization Aid to the Church in Need (ACN) and the Pew Research Center, approximately 220 million Christians are directly exposed to extreme persecution. The report "Persecuted and Forgotten? 2024-26" confirms a deterioration in conditions in 55% of high-risk countries, with the threat stemming from both Islamist extremist organizations and authoritarian state regimes.



Ireland: A pro-Palestinian activist broke into Shannon Airport in Ireland on April 11 and damaged a U.S. National Guard C-130 Hercules aircraft valued at $60 million. The perpetrator carried several capsules of gallium—a highly corrosive metallic chemical element capable of corroding aluminum within minutes—noting that the aircraft in question was constructed primarily of aluminum. Hope that the plane was insured!



Brave adults: In 2025, 589 million children, almost one out of four children worldwide, lived in conflict zones. Since 2005, the UN has verified 442,241 grave violations against children in conflict. In 2025 alone, 38,967 violations were verified. 171,712 children have been killed or maimed since 2005. More than 70 per cent of cases were committed against children in five countries: Palestinian territory, Afghanistan, Somalia, Syria, and Yemen.



The Nethelands: The Netherlands has now openly become a target for Moscow, following boasts by the Dutch defense company Destinus that its RUTA missiles and drones struck the Crimean Bridge. **Einstein was so right!**



Kaliningrad: For the first time, the Ukrainians have launched a drone attack in Western Europe—specifically against the Russian region of Kaliningrad, located between Poland and Lithuania. The target is the city of Baltiysk, the region's port, which houses not only anti-aircraft missile batteries but also surface-to-surface missile systems. According to initial assessments, the **drones were launched from a vessel positioned off the coast**. Kaliningrad—Russian territory since 1945—is heavily militarized with nuclear capabilities and can strike Ukraine within minutes! This is a development of particular significance, given that Kaliningrad serves as a Russian exclave in the Baltic, situated between Poland and Lithuania. **Some fools are pushing us toward catastrophe!**



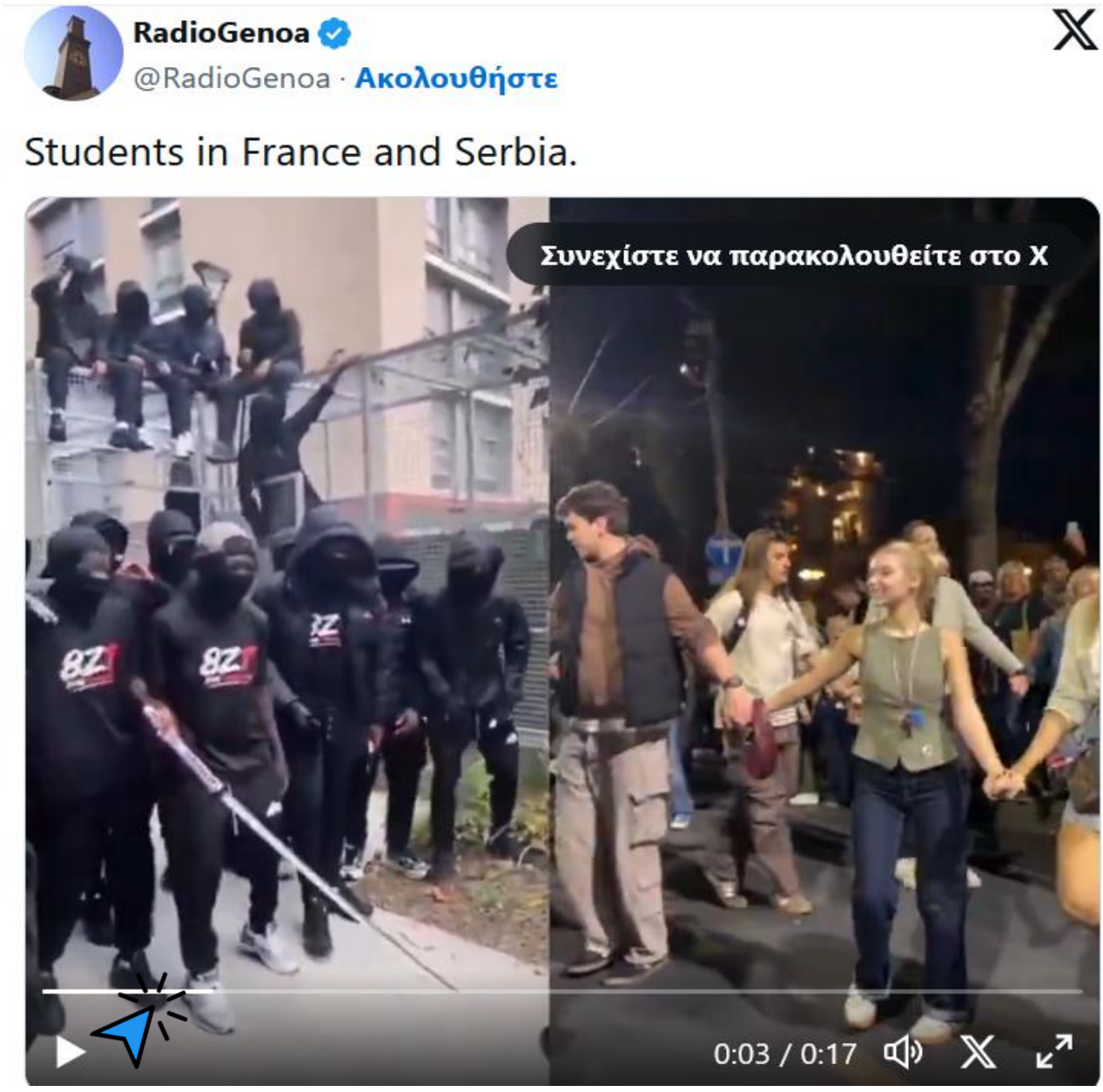
ASPISMEDICAL: After 19 months and 93 out of 111 articles published, I put an end to the collaboration with *CounterTerrorism Medicine – Europe* (UK) as the Editor-in-Chief of the ASPISMEDICAL monthly e-journal, due to incompatibility of characters and lack of consistency.

The Editor

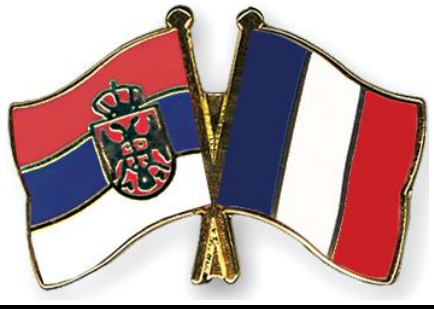



To Rigas

Students in France and Serbia



The cultural differences are stark, as evidenced by the above footage—circulated by numerous accounts on X and garnering millions of views—which contrasts "French" "students" brandishing machetes and knives while dancing to drill and trap music with young Serbian women performing traditional dances. This is the fundamental distinction noted by many users, whose comments offer a scathing critique of the direction in which France is heading, in contrast to Serbia, which continues to maintain strong ties to its own traditions.



Without comments!



Fethiye Expat Forum · Γίνετε μέλος
Victoria Slabir · 18 ώρ. ·

Hello 👋 we are a Scottish family with 2 children at school here. We went to the Independence Day school show today. We were really shocked that they had children dressed in the UK, Greek and Indian flags with demon masks on. They were put in a circle and covered in the Turkish flag while my British children had to sit and watch. Has anyone experienced anything like this?



The "integration" of Turks and Islamists into Germany's security forces has not gone very well… A Berlin police officer (who himself has a migrant background!) describes to his lawyer, Christiane Meusel, what goes on within the Berlin Police force. Colleagues of Turkish and Arab origin hurl insults at him, as well as at other Germans. Remarks such as "Luckily, we're going out to shoot today without any Germans along" or "Thank goodness that German bastard isn't here today" are heard regularly. During police training, one participant openly declared: "I will take revenge on the Germans." German colleagues remain silent; they allow themselves to be intimidated and do not speak up. The State Security service is now investigating these allegations, while other personnel have reported similar incidents. One Islamist police officer even refused to go on patrol with a woman! In a case involving domestic violence, he showed leniency toward the abusive man, operating under the rationale that "it's the woman's fault." At the academy, some trainees appeared wearing *fezes*, while others refused to participate in a swimming lesson because a female classmate was supposedly menstruating. A trainee asked his instructor whether he could defend his family's honor using his service weapon! All of this may also be linked to the fact that the Berlin police force is finding it increasingly difficult to recruit a sufficient number of suitable candidates. Approximately 40% of applicants fail the German language test, training positions remain unfilled, and the proportion of personnel with a migrant background has been rising for years. In certain sectors, 70 out of 170 employees already have a Turkish or Arab background. Armed personnel—paid for by the German taxpayer—who speak about their own population in such terms. The policy of quotas and diversity does not seem to be working…

It seems that Iran is still holding . . .



Oooops!



Front cover of the Iranian state-owned newspaper Hamshahri

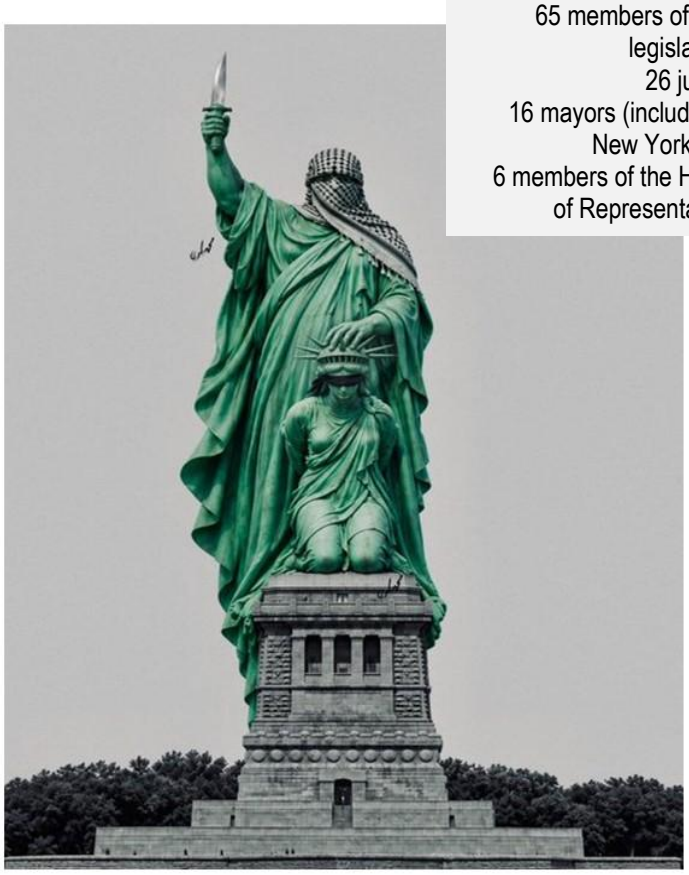
Iran threatens missile strikes on Europe if the US resumes attacks The Islamic regime in Iran has explicitly threatened direct missile strikes on European soil if the United States uses its bases in Europe to attack Iran. “Any act of sabotage or military aggression by the US and Israel would trigger an Iranian response, with missiles capable of reaching targets in Europe,” said Islamic regime parliament lawmaker Hossein-Ali Haji Deligani. Islamic regime media named Germany and Italy as primary targets due to their concentration of U.S. bases. A published map highlighted 15 bases across Europe, including RAF Fairford in the UK and Bezmer Air Base in Bulgaria. IRGC forces also declared that Iran will target critical subsea fiber-optic cables in the Strait of Hormuz to disrupt international internet connectivity. Defense analysts note that Iran’s actual capacity to strike deep into Western Europe remains highly restricted. Most of its ballistic missiles are limited to a self-declared 2,000 km range, which is enough for parts of Southeastern Europe (Greece, Bulgaria, Romania) but short of Western or Northern Europe. To hit distant targets like Diego Garcia earlier this year, Iran used heavily stripped-down warheads. Firing a limited payload over well-defended NATO airspace makes a successful deep strike into Europe very unlikely. The more realistic risk is Iran firing at U.S. bases in Southeastern Europe, missing, and hitting civilian areas, which could trigger a NATO Article 5 response.

EDITOR’S COMMENT: Can you imagine **just one** missile out of nowhere in a European city or capital? Israel knows the feeling, but the US is far away and is quite safe to care.

Houston we have a problem!

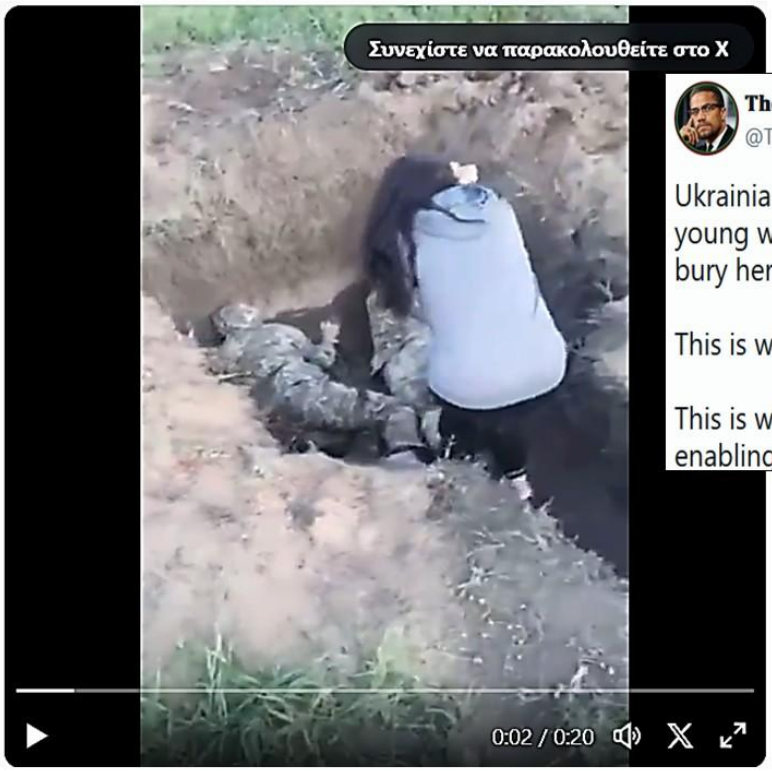
Muslims have been elected in 26 U.S. states:
114 city council members
90 education officials
65 members of state legislatures
26 judges
16 mayors (including in New York City)
6 members of the House of Representatives





"Michigan is the capital of Arab America," stated Senator-elect Abdul El-Sayed.

The right side of history



The Empire Watch
@TheEmpireWatch · Ακολουθήστε

Ukrainian soldiers from the Azov Battalion execute a young woman with her hands tied behind her back, then bury her in a mass grave alongside other fallen soldiers.

This is what American taxpayers are funding.

This is what the European Union is financing and enabling. Εμφάνιση περισσότερων



One photo, a thousand words



No polite commends . . .





France: a sick country on a sick continent

By Guy Millière
Source: https://el.gatestoneinstitute.org/



Nov 15 – “Who didn’t expect that? Oh, yeah... the politicians," remarked "The Great Gates" on X.

The French government was reportedly “surprised” when students began revolting about two weeks ago to protest conditions — overcrowded classes,

dilapidated buildings, pests and rats, lack of heating and air conditioning, a lack of teachers — in their schools.

“But,” writes U.S. journalist Michael Schelenberger, “French schools now have more money per student than ever before. [...] [...] The French government spends 4.5% of gross domestic product for educational institutions, while Germany spends 3.7%.

The violent unrest, which began in Il-de-France, Paris and spread across the country, appears, according to investigations, were instigated by the French political party *LaFranceInsoumise* (Rebellious France), led by Jean-Luc Mélenchon, a far-left candidate in the French presidential election scheduled for spring 2027. *LaFranceInsumise* denies the accusations —however, according to Schellenberger, “evidence clearly shows that *LaFranceInsoumise* (LFI) [...] instigated and led the protests.”

> "The protest was attended by elected officials of the party insubordinate France and collectives of the extreme left," an unnamed security official told Le Point. In a report on the prime minister’s emergency meeting on ηOctober 1, which he handed over to Reuters by a person close to his entourage, the movement is described as “an operation organized by the LFI (La France Insucumise) party and its representatives on the far left,” according to a “joint assessment” of the secret intelligence.
>
> "Parents, activists of the Insubordinate France, mobilize to oppose the brutality of the police," Mélenchon said, accusing the police, not students of violence.
>
> In Marseille, hundreds of young people forced firefighters to leave their vehicle outside a high school, and then set him on fire. In Paris, about ten protesters chased a police lieutenant, threw her to the ground and kicked her screaming "kill her!"
>
> "We are not entirely sure they are even high school students," the French justice minister said of the people arrested ... "
>
> The French left has declared war on schools while creating an alliance with Islamist leaders hoping to radically transform them. For both sides, the fight starts in schools.
>
> "It is clear that religious and politico-religious organizations "affect" these pupils, sometimes already from primary school, as well as their families, their social environment and their neighbourhood, while some are trying to turn them against the school," said the report of the Ministry of Education's review held in June 2004 on religion in schools.
>
> What unites the Islamists and the revolutionary left is their intention to destroy Western civilization. The French Interior Ministry report compiled in May 2025 on the Muslim Brotherhood described the movement's plan in France as "a long process of political conquest" with "systematic priority in investment at the local level."
>
> The children of Muslim immigrants are often more radical than their parents. “There is, first of all, a revolt of the new generations,” wrote Olivier Roua, a French scholar of Islam in 2015, referring to the French jihadists.
>
> The LFI openly seeks the vote of Muslim voters, and a parliamentary inquiry said this makes it a target for Islamist networks [...].
>
> “The LFI’s commitment to a strategy of clientelism toward the Muslim electorate may have made this movement a privileged goal,” said Mathieu Bloch, rapporteur for the National Assembly’s research on parties and Islamist networks in December 2025.
>
> “All polls show that Mélenchon will suffer a crushing defeat in a second round against Le Pen,” επισήμανεthe BBC said.

So far, about 2000 students have been arrested, and more than 1000 schools have been affected. Incidents of violence include "schools that were torched and teachers who were beaten and doused with petrol."

French President Emmanuel Macron, who is in his second term and cannot run again, is concluding his presidency by facing a broad rejection from the public. According to a recent poll, only 21 percent support their policies, although that figure has risen from 19 percent a few months ago.
Macron's percentages are not surprising. He has repeatedly shown contempt for the poorest members of French society.
A few weeks after the start of his first term, which began in May 2017, he spoke of "those who succeeded" and "those who are nothing." Less than a year and a half later, in November 2018, citing man-made climate change, it raised France's already outrageous taxes on gasoline, a move that immediately sparked the Yellow Vest movement, when thousands of French citizens said they could no longer afford either fuel to move to work or food to feed their families. Macron replied that while some people may face financial difficulties, he must take care of something more important: "the danger of being faced with the end of the world."



Municipal workers clean the area around the "Marcel Sembat" middle school in Rouen, France, on October 1, 2026, after the building was set on fire by rioters. (Photo: Guillaume Saligot/AFP via Getty Images)

The "Yellow Vest" movement lasted more than a year —and only fell in January 2020 with the start of the COVID-19 pandemic. Throughout the movement, Macron remained contemptuously, responding to the grievances of nonviolent protesters with police attacks that caused deaths and amputations. In the meantime, he allowed leftist rioters who had infiltrated the movement to cause riots and commit arson, without asking the police to intervene. Many in France found that Macron could be merciless at people who expressed their anguish, but leniently towards criminals, as long as they had the political direction he preferred.

During the pandemic, Macron put in place some of the most authoritarian measures in Europe. The French were forced to stay in their homes and go out only for one hour a day—in a radius of eight hundred metres— provided they would fill in a form in which they would indicate their name, address and departure time. The police, who were ubiquitous, arrested thousands of people and imposed heavy fines on them simply because they were slightly removed beyond the permitted distance or remained outside a little more than an hour. All outdoor conversations were strictly prohibited.

The years of Macron's rule were further marked by a deep economic downturn in France and a severe decline in living standards. In the last decade, France's per capita wealth has fallen below the EU average, and is now lagging behind that of Cyprus. Ten years ago, in 2016, France's GDP per capita ranked 23 percent ⁿworldwide, while it is currently in 33 ⁿthe place. The unemployment rate, which currently stands at 8.3%, is rising. For people aged 15 to 24, this percentage is extremely high, reaching 21.1%.

Deindustrialization continues unabated. Ex-secret regulations have led to factory closures. These are not replaced by other businesses, but by an increasingly costly welfare system, which currently accounts for more than 40% of total public spending. In 2025, France's poverty rate rose to 15.4 percent, a figure of 9.8 million people living on an income of less than 60 percent of national average income, and they struggle every month just to meet their basic needs.

At the same time, successive French governments have increased unrestricted spending. While GDP growth in France from 2016 to 2026 totaled 13.17%, public spending growth in the same period was 35.6%. This huge difference means that the government continues to spend much more than it collects. Public debt, which is constantly rising, reached 117.5% of GDP in January 2026 and will reach 119.3% by the end of the year. Interest payments on debt are devouring an increasing share of the country's annual budget and, like the United States, now go beyond the national defense budget. The difference is that the U.S. may still be able to get out of this impasse through economic growth —$40 trillion, with interest of $7.1 billion a day — while France, crushed by overregulation, cannot.

On the other hand, while Macron, in 2020, condemned "Islamist separatism," he has done nothing to prevent, or at least slow France's Islamist conquest. For a decade now, the country's unabated Islamization has continued unstoppable. Millions of people from the Muslim world have settled in France, both legal and illegal. Around 2016, the approximate number of Muslims and foreign Muslims living in France was 5.7 million (8.8%). Today, officially, it is estimated that they probably amount to 7 million in a population of about 67 million, but the real numbers are undoubtedly higher. Most Muslims in France are not assimilated, and a growing proportion — about 38% — it sets Islamic sharia law above the laws of the Republic (this figure, 57%, is highest among Muslims aged 15 to 24).

The laws against illegal immigration are not enforced. Every year, only 7% of illegal immigrants in France, to whom the police have imposed an obligation to leave the country — through OQTF (Omfault of French Territory) — are deported. This laxity means that over 93% remain in the country. Many of them are criminals. Some of the most heinous killings that occurred in France during Macron's tenure were committed by illegal immigrants who had ignored the OQTF that had been imposed on them. Twenty-year-old Lola Davidier, for example, was raped, tortured and murdered in an apartment in Paris by an Algerian thief and occasional prostitute, Dabia Benkired. On August 21, 2022, Benkirid had been arrested, OQTF had been imposed, and then she was released. Two months later, on October 14, he murdered the 12-year-old.

Forbidden zones, dominated by radical imams and Muslim gangs, have increased since 2016. They now appear in the suburbs of the great cities of France. Members of Muslim gangs carry out raids and looting several times a year, especially when a French football team is held, and recently during the 2025 World Cup. Police have

orders to intervene only in a short place. If they injure or kill a Muslim criminal, police officers know that their career and life may be destroyed. On June 27, 2023, Nahel Merzuke, a young Muslim criminal, refused to obey a police officer, who then accidentally shot him. The riots, which broke out across the country, only began to calm down when the police officer, Florian M., was remanded in custody and charged with first-degree murder. He now faces up to 20 years in prison.

"Right" anti-Semitism has almost disappeared and has been replaced by an extremely venomous Islamic and left anti-Semitism.

After the massacre committed by Hamas on October 7, 2023 in Israel, Islamic and left-wing demonstrations in favor of Hamas and the "Palestinian resistance" were organized in a few days. *The La France Insumise* party described ηςthe October 7 carnage as an "armed attack by Palestinian forces," without mentioning at all the fact that Hamas is a terrorist organization. One of the leaders of the LFI, Rima Hassan, a French citizen, defines herself as "French-pallastinia" and not as a French woman. Israel is constantly and falsely accusing Israel of "genocide," and claims that "the actions of Hamas are legal."

The massive upsurge in anti-Semitic attacks, threats and insults continues to this day.

In recent years, Macron has also increasingly aimed at freedom of expression, using Arcom to this end —a body he founded in 2022 to regulate and control French audiovisual media. In 2025, Arcom closed the C8 TV channel: the official reason was the "lack of pluralism" and the fact that too many conservatives had been invited to speak. On June 15, 2026, another TV channel, CNews, received an official notice from Arcom, which also accused it of "lack pluralism." CNews may also close soon. It is the last major television channel in France that still invites right-wing commentators, whom the other channels no longer invite. CNews was fined twice in 2026: one because a guest said that man-made global warming does not exist, and the other time because one guest said that "history shows that Islam is still a religion of conquest."

In December 2025, France called for sanctions by the European Union to be imposed on two commentators — Jacques Bond and Xavier Moreau — because of their "pro-Russian statements." Bank accounts and their assets within the EU froze, while their credit cards were cancelled. They are no longer allowed to travel within the EU. Any financial assistance provided to them by anyone will be subject to sanctions. These measures are out-of-court, but there is no possibility of appeal or appeal.

In May 2024, Macron's political party, the *Αναγέννηση*"Renaissance", was defeated in the European Parliament elections. While France's main right-wing party, the "National Coalition" (*Rassemblement* National), garnered 31.37% of the vote, Macron's party received only 14.6 percent. He spoke angrily about the outcome, dissolved the National Assembly and called early parliamentary elections. In the first round, the "National Coalition" garnered more than 33% of the vote and was ready to win the majority of seats in the second round. Macron quickly created an alliance of all other political parties with the aim of defeating the "National Coalition." He spoke of a "republican front" and hinted that the "National Coalition" poses a danger to democracy. Voters who supported candidates from the centre or moderate right were encouraged to vote for a left-wing candidate, as long as he had the best chance of winning. Voters who supported left-wing candidates were encouraged to vote for a centre or moderate right-wing candidate for the same reason. The result was that the National Coalition secured the largest percentage of votes, but the "republican front" parties received the largest number of seats in the National Assembly, which was fragmented into several parties, none of which was able to form a cohesive majority. Since then, the country has experienced several powerless governments, and no major decision has been allowed to be made. Macron made the country ungovernable.

Macron may want a successor who will continue his programs, whatever they may be, but that doesn't seem to happen. Marine Le Pen, for the first time in her

political career, is leading the polls, which show that in 2027 she could win. The other candidates belong to parties now linked to the disaster in which France has been plunged into.
Le Pen διώχθηκεwas even prosecuted for allegedly allowing her party's parliamentary advisers to work in Paris on behalf of MEPs who had hired them. When centrist candidate Francois Bayrou and leftist Jean-Luc Mélenchon were charged with the same offence, the charges against both were dropped. But not for Le Pen. On March 31, 2025, she was sentenced to four years in prison and a five-year ban on public office, apparently to be averted for her nomination.
After appealing the decision on 7 July 2026, her sentence was reduced to three years in prison — of which one year was due to be served under house arrest, wearing an electronic monitoring bracelet — and a 45-month ban on public office, of which 30 months were suspended. The new decision allows her to run for office. He has appealed to France's highest court, and the enforcement of the decision has been suspended. He will not have to wear the electronic surveillance wristband during the election campaign. The court is expected to issue its ruling on its appeal before the election, and may overturn its original ruling. In this case, Le Pen will be required to wear the electronic watch bracelet in the final days of her election campaign and, if elected, at the Presidential Palace of the Elysee upon taking office.
All of her legal problems, however, seem to have affected her constituents at all, who seem to understand that justice in France has now been politicised.
If Le Pen is elected president in the spring, the implications will be felt across Europe. A Le Pen presidency would mean victory for a political party that defends the values of Western civilization — a party that every sitting leader in Western Europe, with the exception of Italian Giorgia Meloni, seeks to keep away from power by any means possible.
The economic, financial and social situation that Le Pen would face in the event of her victory would be difficult. All available evidence shows that France is almost in bankruptcy at almost every level. Recovery will be extremely complex and difficult.
Most LFI leaders have already said they will refuse to accept a Le Pen victory: if she wins, they will call for εξέγερσηrebellion. Several political analysts believe that, in such a case, widespread unrest may break out across the country, involving left-wing groups and Islamist gangs.
Several other French politicians trying to spread panic will do so with increasing tension until the election day. It is far from certain that these obstructions would be enough to beat Le Pen.
A recent poll conducted on behalf of the centre-right Foundation for Political Innovation shows that 78 percent of voters believe that "French lifestyle, traditions and habits are under threat." The available evidence shows that, unfortunately, this is true. Another recent poll shows that 85 percent of voters consider France to be in decline. They are absolutely right. France is in abrupt decline, and the vast majority of French people understand this.
The situation in France differs little from the general situation elsewhere in Western Europe. The policies pursued in most other Western European countries are not substantially different from those adopted by Macron — and lead to the same results.
Many other Europeans are just as unhappy with their leaders, as the French. Everyone understands the economic disaster, the continued Islamization of their countries, the threat from China to undermine their automakers, as well as the growing inability to discuss certain issues without being demonized or brought to trial.
Many Europeans see Islamism gaining ground in their countries and enjoying the support of Marxists: everyone believes that the other will bring him to power. They see their leaders doing nothing to fix a situation becoming increasingly worrying. They seem to prefer to protect and save their Western civilization. Political parties in Western Europe with programs approaching that of Le Pen's "National Rally," such as the German *"Antalis for*

Germany" (AfD), are gaining ground despite the efforts of leaders in power and the media to demonize them.

On September 6, 2026, in the regional elections in Saxony-Anhalt, Germany, the AfD won 43.8% of the vote — twice as much as five years earlier. In May 2025, German Chancellor Friedrich Merz took power as the head of a large coalition government, which was united solely by a desire to stem the rise of the AfD. His coalition did nothing to counter Germany's deep industrial recession and the growing isolation of Muslims living in the country. The situation is now worse. Merz is now more unpopular in Germany than Macron in France (only 14% of Germans consider him worthy to hold the office of chancellor). The AfD is now the most popular party nationwide in Germany. A recent poll puts his support at the record of 30 percent.

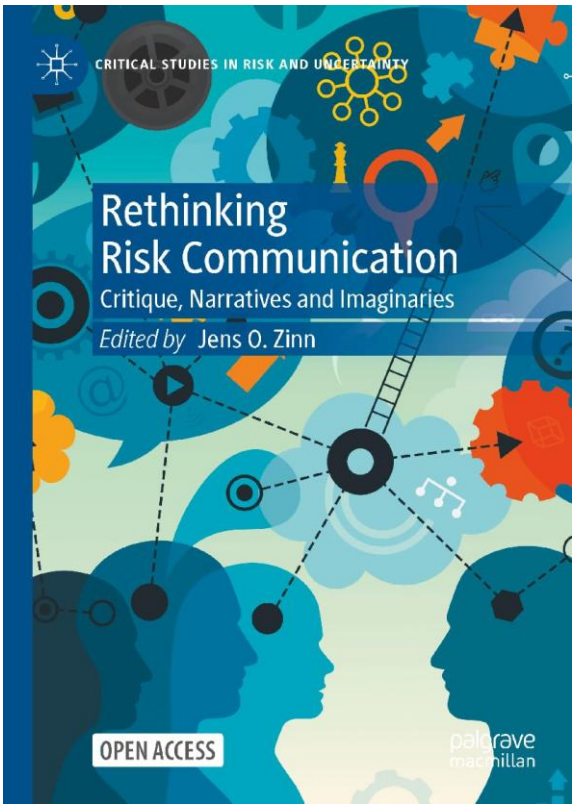
In the UK, in May 2026, the Reform Party won many local and municipal elections, bringing heavy defeats to both the ruling Labour Party and the Conservative Party. Recent polls show that, if parliamentary elections were held today, the Reform Party would secure the highest number of seats. A political wave is taking shape in Western Europe. Most mainstream media commentators scornedly characterize it as "populist."

"What they call populism," wrote Eric Zemmour, a former columnist and chairman of the right-wing party "Recapture," "is the cry of people who don't want to die."

Dr. Guy Millière is a professor at the University of Paris, is the author of 27 books on France and Europe.

Rethinking Risk Communication: Critique, Narratives and Imaginaries

By Jens O. Zinn (Editor)
Source: https://link.springer.com/book/10.1007/978-981-92-5082-0



This open access edited volume provides a unique interdisciplinary study of risk communication, presenting both innovative conceptual frameworks and new empirical data. Risk communication cannot be fully understood without considering not only scientific knowledge and values but also cultural imaginaries, embodied experiences, and power relations. This book therefore sheds light on risk communication as a complex social process involving a wide range of individual and organized actors including political decisionmakers, journalists, writers, NGOs, profit organizations and people in everyday life, who interact across various settings.

With contributions by scholars in sociology, human geography, philosophy, literary studies, science and technology studies, social theory, security studies, and health studies, this volume demonstrates how risks are framed, negotiated, and contested in society. Exploring emerging challenges, it presents strategies to address national security risks, the difficulties of predicting extreme weather events, and the politics surrounding public engagement. This book also

addresses previously underrepresented issues—such as the role of literature in shaping collective imaginaries, the limitations of citizen science, the strategic use of rhetoric by institutional actors, and the interaction between media discourses and political or economic interests. The intended audience includes both students and scholars in sociology of risk and uncertainty, risk studies, risk communication, and STS, as well as practitioners (such as those in disaster prevention) and policymakers interested in the broader social aspects of risk.

OMG!

At the center of remarks by professor and politician Victor Gao was a recent statement by the High Representative of the Union for Foreign Affairs and Security Policy, Kaja Kallas, regarding Russia and China and their roles in the Second World War.



Kallas overlooked the fact that Russia and China contributed to the victory over the Nazis. As Gao stated:



"I would tell Ms. Kallas to go back to elementary school and study history from the beginning. It is absolutely shocking that a European leader claims not to know what role China played in the defeat of fascism.

China sacrificed more than 35 million lives to defeat Japanese fascism.

And while the American war against fascist Japan and Nazi Germany lasted less than four years, China's struggle against Japanese aggression spanned 14 years—at a cost of 35 million lives." "Therefore, Ms. Kallas, go back—even to kindergarten, if necessary—to study history and refresh your knowledge regarding the heroic sacrifices and the heroic struggle of the Chinese people—who never agreed to capitulate—which led to the definitive defeat of Japanese fascism. Never let such nonsense pass your lips again."



Gao's statement comes as a direct response to remarks by Kaja Kallas that downplayed or ignored the contributions of China and the Soviet Union to the victory over the Axis powers.

The Chinese analyst pointed out that China's struggle against Japan began as early as 1931 and lasted for 14 years, resulting in massive human casualties, whereas American involvement in the Pacific War was significantly shorter.

This confrontation highlights the fact that, in recent years, individuals with no background in history have ascended to high-ranking positions—suggesting a deliberate agenda to revise history.




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

Guess the working organization of this person!



Terrorism's impact on global security

By Josef Dishan

Source: https://dailynews.lk/2026/10/28/general-opinion/1047173/terrorisms-impact-on-global-security/

Oct 28 – Globally, terrorism will add to instability and drive international security interventions, especially in the Middle East and Africa. The threat from terrorism will remain high and worsen over the next five years, despite strong counter-terrorism measures. Extremists will continue to exploit fragile and violence-prone states, including in Southeast Asia. New technologies could make it easier for terrorists to make advanced biological or chemical warfare agents. Extremist narratives will continue to inspire violence globally. The terrorism threat in Southeast Asia is increasing because of links between local extremists and terrorist groups. Terrorism significantly reduces foreign direct investment and capital formation, leading to economic instability. In 2023, the number of terrorist attacks worldwide surged to 3469

Yemeni Houthi rebels have launched an escalating wave of missile, drone, and projectile strikes against Saudi Arabia, intensifying

a renewed phase of cross-border conflict. Saudi Arabia has one of the largest defense budgets in the world, and its armed forces are equipped with advanced fighters and air-defense systems. But the Houthis have indigenous missiles and drones to effectively counter Saudi military strengths. Pakistan and Egypt have condemned attacks by the Iran-backed Houthi movement on Saudi Arabia, reaffirming their support for the kingdom's sovereignty, amid escalating regional tensions. The Gulf Cooperation Council (GCC) foreign ministers have called for a return to dialogue and diplomacy to resolve the crisis involving Iran and safeguard regional security and stability, urging a political solution.

Rather than a "war on terror," what is needed is to transform security itself. Democracy provides opportunities for conflict prevention, conflict management and conflict resolution as well as opportunities of political participation. The word "terrorism" is politically and emotionally charged, and this greatly compounds the difficulty of providing a precise definition. **What is terrorism to one group may connote a freedom fight to another group.** Terrorism, in the modern sense, is violence against civilians to achieve political or ideological objectives by creating fear. Terrorists also attack national symbols to show their power and to shake the foundation of the country or society they are opposed to. This may negatively affect a government's legitimacy. The United Nations Global Counter-Terrorism Strategy reaffirms the links between human rights and security, and places respect for the rule of law and human rights at the core of national and international counter-terrorism efforts. Terrorism is a transnational threat that cannot be addressed by a single country alone.

EDITOR'S COMMENT: The sentence in **red** might sound logical to many, but if you think of it, it denotes that the ignition of terror is just fine, similar to any other feeling we experience in our lives. **IT IS NOT!**

Transnational threats

The international order is also being contested in other ways. Some states have increased their use of 'measures short of war' to pursue political and security objectives. Such measures include the use of non-state actors and other proxies, covert and paramilitary operations and media manipulation. In parts of the Indo–Pacific, China's power and influence are growing to match (in some cases exceed) that of the United States. The future balance of power in the Indo–Pacific will largely depend on the actions of the United States, China and major powers such as Japan and India.The quality and quantity of missile forces in the Indo–Pacific are rising, including ballistic missiles.

Al-Qaeda operates from several safe havens around the world, one of which is Iran. Its alleged Iran directly supports al-Qaeda with weapons and funding. But their religious and ideological differences, a Shia Iran and a Sunni al-Qaeda, limit direct commitment to each other's political objectives. The core of their relationship is centred on disrupting US interests in the region. On the other side, a threat has grown. Extreme Right-Wing Terrorism (ERWT) describes those involved in Extreme Right-Wing activity who use violence in furtherance of their ideology. These ideologies can be broadly characterized as Cultural Nationalism, White Nationalism and White Supremacism.

Terrorist attacks can be broadly categorized into two categories: focused and indiscriminate. Historically, terrorism has largely fallen under the former category. In terms of the use of violence and force by terrorists, this also ranges across a wide spectrum- from individuals with military training and experience and "throwaway" operatives, who are sent untrained on suicide missions. Their use of violence also illustrates the slow evolution of terrorist tactics and strategies, including traditional assassination, bombings, arson, hostage-taking, hijacking sabotage and suicide

bombings. More recent tactics include unconventional forms of terrorism, including nuclear terrorism (fabricating a dirty bomb, attacking a nuclear reactor, etc.) and high-tech terrorism involving cyberattacks.

Asian theatre

Despite the apparent decline in Al Qaeda and ISIS in the Middle East, violent extremism linked to the two terrorist organisations continues to pose an ideological and security threat to Southeast Asia. ISIS' growing footprint in this region can increasingly be felt. Extremist networks in Southeast Asia often exploit policy gaps and security loopholes between nations to operate, recruit members and secure funding.

The first is the significant growth in terrorist attacks by ISIS-inspired, self-radicalised individuals. The March 2021 'lone wolf' attack on the Indonesian National Police Headquarters by a young female college student, shows the danger of radicalized domestic terrorists. She was reportedly radicalised online by ISIS propaganda. Since 2023, Indonesia has experienced a period with no large-scale terrorist attacks. Far from signaling the end of terrorism, it reflects an evolving threat which is moving online to radicalise lone-wolf actors.

In 2020, the Philippines passed an anti-terrorism act. The act considerably expanded the definition of terrorism to include activities that incite terror and extremism, such as provocative speeches and proclamations. The Abu Sayyaf Group, originally devoted to the establishment of a radical Islamic state in the Philippines through terrorism, has been fragmented by the bold Philippine military response. However, by virtue of its maritime capability, it is an important part of the maritime terrorist threat facing Southeast Asia. The Abu Sayyaf Group (founded in 1991) remains a violent extremist and terrorist threat in the southern Philippines. Although ASG has historically aligned itself with al-Qa'ida and Jemaah Islamiyah, some ASG sub-groups have pledged allegiance to Islamic State. The continuous entry of foreign jihadists to the southern Philippines only compounds these issues, as radical foreigners subvert the minds of the locals.

The strategic geographic location of India in foreign trade, combined with its natural resources spread across land and coastal areas, mandates a multi-faceted security apparatus. These long borders present multiple security challenges- illegal immigrants, insurgency, cross-border terrorism and illicit drug trade. India's separatist landscape is shaped by a complex interplay of ethnic, religious and regional factors, particularly evident in regions such as Punjab, and Kashmir. India prudently subdivides terrorism into five major groups: ethno-nationalist terrorism, religious terrorism, ideological, narco-terrorism and state-sponsored terrorism.

Europe

Europe could be more directly affected. Over the past decade, intelligence data collected shows that Iran increased its collaboration with criminal networks in Western countries to commit violence and target journalists, politicians, Jewish communities, and Iranian dissidents. Iran's previous weaponization of criminal networks has targeted Jewish communities and synagogues, particularly in Europe, considering them legitimate extensions and representations of Israel. Iran also directly engages in state-led terrorism with agents deployed around the world that can be activated when necessary. Some of these agents act as interlocutors with Organised Crime Gangs (OCG) and terrorists in Europe. Recent attacks in the EU demonstrate the intent and capability of jihadist terrorists to inflict mass casualties on urban populations.

The main concern of Member States is jihadist terrorism and the closely related phenomenon of foreign terrorist fighters who travel to and from conflict zones. The right-wing terrorism threat in Europe also remains a

serious and evolving security challenge. Foreign terrorist fighters (FTFs) are individuals who travel to a state other than their state of residence or nationality to commit, plan, or receive training for terrorist acts. They continue to pose an evolving threat to global security. The European Parliamentary Research Service estimated 4,000 citizens from European Union (EU) member states (mostly from Belgium, France, Germany and the United Kingdom) left to participate in the Syrian civil war, with over 30 per cent having returned to Europe.

Drone terror

In the past few years, terrorist groups have begun employing drones. Both can be harnessed to respond effectively to multiple security challenges. Uncrewed aerial systems (UAS) have been identified as one of the key terrorist threats by the United Nations (UN) Security Council Counter-Terrorism Committee. UAS are remotely piloted airborne vehicles. They are also referred to as unmanned aerial vehicles (UAVs), or more commonly drones.UAS are attractive for terrorists because they are affordable and require minimal training.

Terrorists have deployed drones to attack state military assets, diplomatic sites, international trade, energy infrastructure, and civilian centres. State sponsorship of terrorist groups has also helped increase the number of drone attacks. Globally, drones can travel up to 1,500 km, ideal for attacks on military targets deep within state territory. In 2015, a drone with radioactive sand targeted the roof of the Japanese Prime Minister's office. Governments worldwide will also face a significant national security threat. Drones also perpetuate the psychological dimension of terrorism by spreading fear. Countries need extensive defence cooperation and intelligence sharing to mitigate terrorism.

Books on Intelligence That Upgrade Homeland Security, Terrorism and Counterterrorism Studies: October 2026, Volume 1, No. 3

By Dr. Joshua Sinai

Source: https://www.hstoday.us/books/books-on-intelligence-that-upgrade-homeland-security-terrorism-and-counterterrorism-studies-october-2026-volume-1-no-3/

Oct 28 – The disciplines of homeland security, terrorism and counterterrorism (CT) are continuously being upgraded by the latest advances in intelligence analytic technologies, such as geospatial, data mining, and link analysis software, as well as artificial intelligence (AI) applications. This review essay covers a representative sample of 22 books about the application of structured intelligence analytic methodologies and technologies in homeland security, terrorism and CT subjects.

Note that some of these books on intelligence analytic methods and technologies also cover other homeland security topics such as cybersecurity, critical infrastructure protection, emergency security management, and disinformation, which are not primarily covered in this review essay.

The books below are listed in alphabetical order, according to the authors' last names. The listing is followed by the books' capsule-reviewed coverage arranged by topic.

—

Jonathan M. Acuff, et al., **Introduction to Intelligence: Institutions, Operations, and Analysis** (Thousand Oaks, CA: SAGE/CQ Press, 2022), 440 pages, $80.54 [Paperback], ISBN: 978-1-54437467-3.

Richard M. Adler, **Bending the Law of Unintended Consequences: A Test-Drive Method for Critical Decision-Making in Organizations** (Cham, Switzerland: Springer, 2020), 328 pages, $79.99 [Hardcover]. US $54.99 [Paperback], ISBN: 978-3-0303-2716-3.

Patrick T. Biltgen, **AI for Defense and Intelligence** (Chantilly, VA: Tallaios, 2025), 379 pages, $69.99 [Hardcover], ISBN: 979-8-2183-5148-9.
Robert M. Clark, **Geospatial Intelligence: Origins and Evolution** (Washington, DC: Georgetown University Press, 2020), 320 pages, $149.95 [Hardcover], $49.95 [Paperback], ISBN: 978-1-6471-2011-5.
Robert M. Clark, **Intelligence Analysis: A Target-Centric Approach** [8th Edition] (Thousand Oaks, CA: SAGE/CQ Press, 2025), 528 pages, $169.00 [Paperback], ISBN: 978-1-0719-5192-7.
Thomas E. Copeland**, Fool Me Twice: Intelligence Failure and Mass Casualty Terrorism** (Boston, MA/Leiden, The Netherlands: Martinus Nijhoff Publishers, 2007), 292 pages, $156.62 [Hardcover], ISBN: 978-9-0041-5845-0.
William Costanza, **Treason, Terrorism, and Betrayal: Why Individuals Cross the Line** (Boulder, CO: Lynne Rienner Publishers, Inc., 2025), 279 pages, $115.00 [Hardcover], ISBN: 978-8-8961-6017-5.
Erik J. Dahl, **Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond** (Washington, DC: Georgetown University Press, 2013), 256 pp., $29.95 [Paperback], ISBN: 978-1-5890-1998-0.
Jack Dangermond, **The Power of Where** (Redlands, CA: Esri Press, 2024), 300 pages, $36.50 [Paperback], ISBN: 978-1-5894-8606-5.
Mustafa Demir, **Criminal Intelligence: Collection and Analysis** (Dubuque, IA: Innovative Publishing, 2026), 166 pages, $130.00 [Paperback], ISBN: 979-8-3197-3617-8.
Theresa Fanelli and Anthony Moscato, **Terrorism and National Security: A Student Investigative File** [Revised First Edition] (San Diego, CA: Cognella Academic Publishing, 2023), 100 pages, $145.42 [Hardcover], $51.95 [Paperback], ISBN: 978-1-7935-8383-3.
John A. Gentry and Joseph S. Gordon, **Strategic Warning Intelligence: History, Challenges, and Prospects** (Washington, DC: Georgetown University Press, 2019), 296 pages, $103.29 [Hardcover], US $33.89 [Paperback], ISBN: 978-1-6261-6655-4.
Erik Kleinsmith, **Intelligence Operations: Understanding Data, Tools, People, and Processes** [Second Edition] (San Diego, CA: Cognella Academic Publishing, 2026), 422 pages, $99.95 [Paperback], ISBN: 979-8-8233-1055-0.
Robert Mandel, **AI & Early Warning Systems: Technology Innovation for National Security** (Bouilder, CO: Lynne Rienner Publishers, 2025), 279 pages, $115.00 [Hardcover], ISBN: 978-1-9625-5168-7.
Colleen McCue, **Data Mining and Predictive Analysis** [Second Edition] (Boston, MA: Elsevier/Butterworth-Heinemann, 2015), 422 pages, $78.89 [Paperback], ISBN: 978-0-1280-0229-2.
Patrick McGlynn, **Taking Intelligence Analysis to the Next Level: Advanced Intelligence Analysis Methodologies Using Real-World Business, Crime, Military, and Terrorism Examples** (Boca Raton, FL: CRC Press, 2023), 350 pages, $187.19 [Hardover], $81.59 [Paperback], ISBN: 978-1-0321-3673-8.
Thomas L. Norman, **Risk Analysis and Security Countermeasures Selection** [Second Edition] (Boca Raton, FL: CRC Press, 2015), 483 pages, $126.00 [Hardcover], ISBN: 978-1-4822-4419-9.
Randolph H. Pherson and Richards J. Heuer Jr., **Structured Analytic Techniques for Intelligence Analysis** [3rd Edition] (Thousand Oaks, CA: SAGE/CQ Press, 2021), 385 pages, $123.95 [Paperback], ISBN: 978-1-5063-6893-1.
Katherine Hibbs Pherson and Randolph H. Pherson, **Critical Thinking for Strategic Intelligence** [4th Edition] (Thousand Oaks, CA: SAGE/CQ Press, 2026), 558 pages, $90.00 [Paperback], ISBN: 978-1-0719-0228-8.

Hank Prunckun, **Methods for Inquiry for Intelligence Analysis** [Third Edition] (Lanham, MD: Rowman & Littlefield, 2019), 248 pages, $121.00 [Hardcover], US $60.00 [Paperback], ISBN: 978-1-5381-2587-8.
Julian Richards, **The Art and Science of Intelligence Analysis** (New York, NY: Oxford University Press, 2010), 197 pages, $69.28 [Paperback], ISBN: 978-0-1995-7845-0.
Itai Shapira, **Israeli National Intelligence Culture: Problem-Solving, Exceptionalism, and Pragmatism** (New York, NY: Routledge, 2025), 270 pages, $140.00 [Hardcover], ISBN: 978-1-0327-7811-2.

Lessons From Government Intelligence Agencies' Failed Anticipation of Surprise Adversarial Attacks

As a category of asymmetric warfare, with a small insurgent group or lone actor targeting its larger country adversary, terrorists operate covertly with their violent operations taking the form of surprise attacks against their adversaries. The surprise nature of their unexpected attacks increases the likelihood that their targets will be accessible. The role of government intelligence agencies in anticipating surprise attacks by their terrorist adversaries is crucial, as they provide critical strategic, operational, and tactical warnings and insights that can preempt or prevent such incidents.
Understanding the historical context for examples where terrorists carried out successful surprise attacks, or were preempted from carrying them out, therefore, is important for counterterrorism analysts. The authors who discuss this subject include Erik J. Dahl's **Intelligence and Surprise Attacks: Failure and Success from Pearl Harbor to 9/11 and Beyond**, whose theory of preventive action posits that the key to success in preempting surprise attacks is the acquisition of precise, tactical level intelligence combined with the decision makers who listen to and follow-up on the warnings they receive from their intelligence staff (p. 176). In **Fool Me Twice: Intelligence Failure and Mass Casualty Terrorism**, Thomas E. Copeland examines the surprise terrorist attacks against the World Trade Center (2003), the 1995 bombing of the Murrah Federal Building (Oklahoma City), the Khobar Towers bombing, the bombings of the U.S. Embassies in Kenya and Tanzania, and the 9/11 attacks to examine the questions concerning the nature of the surprise, were details of the event foreseeable?, what was the threat environment at the time, were the successful attacks the product of intelligence failures or policy failures, and were the surprises preventable (pp. xii-xiv).
In **Israeli National Intelligence Culture**, Itai Shapira examines the failure of the Israeli intelligence agencies to anticipate Hamas's planning to launch its devastatingly successful surprise cross-border attack against Israeli on October 7, 2023. One factor was its "fixated analytical paradigm according to which Hamas was deterred from initiating a war with Israel" despite contradictory intelligence-derived information that was considered as "weak signals" (p. 239). This resulted in "groupthink and fixation" overtaking contrary assessments (p. 239).
To avoid failures by intelligence services to anticipate major surprise attacks by their terrorist adversaries, the intelligence analytic discipline utilizes strategic warning methodologies. As explained by Julian Richards in **The Art and Science of Intelligence Analysis**, the potential points of failure in the intelligence cycle begin with the inadequate setting by policy-makers of collection requirements, which require appropriate information/data gathering, which is followed by effective analysis (including the formulation of alternative future scenarios), and then the efficient dissemination and implementation of response measures by decision-makers (p. 33).
As part of the strategic warning analytic process,

as explained by John A. Gentry and Joseph S. Gordon in **Strategic Warning Intelligence**, this serves to alert national leaders to the emergence of significant future threats and the measures required to address them (p. 11). These are framed as alternative future threat scenarios that are assessed as possible or plausible, and as inflicting high- or low-impact (p. 132).

Textbooks on Intelligence Analytic Methodologies

The academic discipline of intelligence analysis in the form of textbooks encompasses a spectrum of approaches and methodologies. In Jonathan M. Acuff, et. al. (Eds.), **Introduction to Intelligence: Institutions, Operations, and Analysis**, the volume's chapters on intelligence analysis and analytic methods are especially pertinent as they cover the topic of prediction (short-term) and forecasting (long-term) of likely future incidents by applying an estimative probability methodology consisting of almost no chance, very unlikely, unlikely, roughly even chance, likely, very likely, and almost certainly (p. 263). It also discusses software-based analytic techniques such as network analysis, which graphically represents relationships in an adversary's network (pp. 282-284), and indicators, which serve as drivers of future events (pp. 286-288).

In **Methods of Inquiry for Intelligence Analysis**, Hank Prunckun discusses significant intelligence methodologies to examine adversarial threats, some of which are discussed by the other volumes, as well. These consist of qualitative analytics, such as SWOT analysis (strengths, weaknesses, opportunities, and threats), Pest analysis (political, economic, social, and technological), analysis of competing hypotheses, which are outlined in a matrix, and network analysis, in which a matrix is applied to outline associations among adversarial subjects. Quantitative analytics consist of organizing intelligence-type data according to numbers that analysts attribute to them for statistical testing, which are applied to four levels of measurement: nominal data, ordinal data, interval data, and ratio data (p. 113). The volume also discusses the key parts of a target profile in terms of personal details, criminal record, and target planning (pp. 139-152), as well as conducting risk assessments and producing national security policy assessment reports.

Critical Thinking for Strategic Intelligence by Katherine Hibbs Pherson and Randolph H. Pherson, is a comprehensive textbook for developing intelligence analytic methodologies and techniques. These include structured analytic techniques, such as the cross-impact matrix, network analysis, multiple scenario generation, quadrant crunching, and the complexity manager. The chapter on portraying probability levels of confidence compares how they are defined and scaled by the United States, Canada, and the UK, as well as how quantitative data should be used in intelligence reports. The textbook is complemented by the handbook **Structured Analytic Techniques for Intelligence Analysis**, Randolph H. Pherson and Richards J. Heuer Jr., which features sixty-six analytic methodologies and techniques employed in intelligence agencies. These include matrices, process maps, gantt charts, mind maps, Venn analysis, network analysis, chronologies and timelines, alternative competing analyses, deception detection, key drivers' generation, indicators generation, critical path analysis, decision trees, and complexity manager.

Robert M. Clark's **Intelligence Analysis: A Target Centric Approach** examines the intelligence cycle, intelligence collection and analysis, intelligence targeting, assessing adversarial denial, deception and signaling, anticipatory analysis and alternative future scenarios, geospatial modeling and analysis, and providing finished intelligence products to government customers. Also discussed are significant advances in the application of artificial

intelligence in conducting intelligence collection and analysis.

Erik Kleinsmith's **Intelligence Operations: Understanding Data, Tools, People, and Processes** covers significant topics in the study and practice of intelligence operations. These include defining intelligence and the disciplines of intelligence; an overview of current threats; threat analysis (defining a threat, threat patterns, and hybrid threats); the application of data and information (evaluating data, signals and technical data, imagery and geospatial intelligence, and human-based intelligence); intelligence tools (data mining, evaluating intelligence tools); the intelligence operations process (understanding intelligence requirements); threat profiling (threat profiling methods and applications); delivering intelligence (understanding the customer); generating intelligence products to support intelligence operations (levels of analysis and intelligence collection operations). Also covered is the requirement to manage insider threats, leakers, and whistleblowers (which is legitimate).

Regarding the counter-intelligence challenge of addressing insider threats, including foreign espionage, William Costanza's **Treason, Terrorism, and Betrayal: Why Individuals Cross the Line** examines the factors that compel such susceptible individuals to engage in espionage on behalf of a foreign country and how their activities can be detected during the pre-incident phases.

In the related discipline of criminal intelligence, Mustafa Demir's **Criminal Intelligence: Collection and Analysis** covers subjects such as foundational concepts (e.g., intelligence collection and analysis), tactical, operational, and strategic types of criminal intelligence; the criminal intelligence cycle, intelligence collection techniques (e.g., HUMINT, OSINT, SIGINT, GEOINT, and others), information evaluation assessments; network analysis techniques, structured intelligence analytical techniques, assessing analytical results, and preparing intelligence reports and their dissemination.

In another aspect of criminal intelligence, in this case, its application to counterterrorism, is Theresa Fanelli's and Anthony Moscatos **Terrorism and National Security: A Student Investigative File**. It discusses the methodologies used to investigate terrorism within the context of national security. The chapters cover topics such as the criminal justice system and national security, fact patterns, professional record keeping, and report writing, court and legal considerations, group versus individual racketeering, major designations of terrorism and hate crimes.

Patrick McGlynn's **Taking Intelligence Analysis to the Next Level** includes a chapter on the analysis of strategic futures. Forecasting, the author explains, is "an objective estimation technique used to predict future data as a function of past known data" (p. 164). He adds that quantitative forecasting can predict future data (or event cycles) when past numerical data is available, while qualitative forecasting is a subjective technique, which is applied to potential intermediate or long-range events, through the Delphi, alternative future scenario, futures wheel, horizon scanning, and other forecasting methods (pp. 164-195).

Security Risk Management

The integrated application of security risk management (SRM) frameworks is considered an important component of effective government counterterrorism campaigns. With security risk management a function of the correlation of threat (the potential to be attacked by a threat actor), vulnerability (to be attacked), and consequence (of being attacked), operationalizing it can reveal a country's level of risk tolerance, which can enable it to prioritize mitigation measures to lower the overall risk to terrorist attacks.

Thomas L. Norman's **Risk Analysis and Security Countermeasure Selection** is considered one of the leading handbooks on security risk management.

It covers topics such as an overview of risk, assessing threat, vulnerability and consequence analysis, estimating probability to be attacked and prioritizing the threat actors, and implementing countermeasures. Among the SRM frameworks, it also discusses the widely used adversarial target selection known as CARVER, the acronym for criticality, access, recuperability, vulnerability, effect on the population, and recognizability. The handbook's discussion is operationalized by numerous tables, matrices and checklists.

In **Bending the Law of Unintended Consequences: A Test-Drive Method for Critical Decision-Making in Organizations**, Richard M. Adler arranges risks into the three categories of strategic, preventable, and external. With risk assessment encompassing quantitative and qualitative dimensions, he calculates risk according to the formula of Risk = likelihood of occurrence plus economic value of loss [to which we might add the value of the human loss of life – JS], with the management of risk falling into the four categories of avoidance, sharing, reduction, and acceptance (pp. 192-195). To manage a risk reduction portfolio (which also applies to a government's counterterrorism campaign), he posits as performance effectiveness metrics four outcomes: reduction of risk, residual risk (the remaining level of risk following a risk reduction campaign), cost, such as in the form of a return-on-investment (ROI), and time efficiency, such a effectiveness in reducing risk "sooner rather than later" (p. 198).

Risk assessment is also discussed in Prunckun's **Methods of Inquiry for Intelligence Analysis**, with the equation of risk = likelihood + consequence operationalizing the process of managing risk (p. 202). It also features tables outlining the rankings of risk likelihood, consequence, and overall risk to a variety of hazards.

Geo-Spatial Analytics

With terrorists operating clandestinely and difficult to locate, the application of geospatial analytics is beneficial to terrorism and counterterrorism analysts, as it enables them to map, predict, and potentially prevent terrorist operations and incidents against their targets in a spatiotemporal context.

In **The Power of Where**, Jack Dangermond, the co-founder and President of Esri, a major geo-spatial corporation, explains that digital mapping technology and online geospatial data have created a "global geospatial nervous system" through "an array of instruments, satellites, sensors, and cameras [that – JS] measure on a continuous basis almost everything that can be detected" on the earth's various surfaces (p. 2). GIS, the author explains, integrates and synthesize such disparate data, which enable 'previously hidden views of the world' (p. 2). Geographic data, not only captures major geospatial data categories such as the environment, critical infrastructure, and boundaries, but people, as well, such as the incidences of crime and terrorism (p. 52). Geospatial modeling tools such terrain analysis, site suitability analysis, and 3D analysis (pp. 168-173).

Robert M. Clark's **Geospatial Intelligence: Origins and Evolution** examines the field of GEOINT as the synthesis of geography, cartography, remote sensing, photogrammetry, geopolitics, and geographic information systems (GIS). The chapter on the tools of geospatial intelligence terms them as geomatics, GIS, geo-visualization, big data, data analytics and visual analytics, and geospatial simulation modeling. Future trends in geo-spatial analytics, the author writes, include applying graphic techniques to create and update layered digital maps in real time, applying techniques of virtual reality to create a computer image of the real world, and equipping drones and autonomous vehicles with remote-sensing artificial intelligence technologies to search for items of interest from distant regions (pp. 304-310).

Artificial Intelligence in Intelligence Analysis

The application of artificial intelligence (AI) systems

are prevalent in supporting intelligence analysis, with this new technology enabling faster processing of vast datasets. While it has not transformed traditional methods of intelligence analysis, it is being applied in predictive analytics (utilizing historical data to forecast future trends), prescriptive analytics (recommending actions to achieve specific objectives), and anomaly detection (identifying potentially anomalous activities in datasets).

Colleen McCue's **Data Mining and Predictive Analysis** was one of the earliest books to examine the algorithmic technology that became artificial intelligence and how it was being used in intelligence and security analysis. It discusses how advanced analytics in the form of algorithmic-based data mining is applied to risk and threat assessment, social network analysis, and geospatial tools, including surveillance detection and the behavioral analysis of violent crime.

In **AI & Early Warning Systems: Technology Innovation for National Security**, Robert Mandel observes that "AI can perform anomaly detection, classification, clustering, continuous estimation, data generation, optimization, ranking, and recommendation and is especially adept at identifying relevant alternative explanations, disruptive discontinuities, underexplored trends, unrealized risks, and missed data interconnections" (p. 48).

The advanced analytical capabilities of AI are further examined in **AI for Defense and Intelligence**, by Patrick T. Biltgen. He notes that what is termed Artificial General Intelligence (AGI), a self-++learning machine capable of performing human tasks, in national security "could be utilized for tasks like information extraction, automated report generation, or threat detection" (p. 333). In intelligence missions, the author observes, AGI could upgrade what is currently a time-consuming process to identify connections by analyzing vast quantities of disparate data into a rapid process "to provide more accurate and timely intelligence, helping to anticipate threats and providing strategic advances" (p. 337).

The application of AI in upgrading intelligence analysis is also discussed in the previously listed books by Robert M. Clark's **Intelligence Analysis: A Target-Centric Approach** (Chapter 23, "An AI-Enabled Version in the Target-Centric Approach"), in Patrick McGlynn's **Taking Intelligence to the Next Level (**Chapter 12, "Trends in Intelligence Analysis," pp. 267-311), and in the chapter on "How Do Models and Artificial Intelligence Help My Analysis?" (pp. 109-140) in **Critical Thinking for Strategic Intelligence**, by Katherine Hibbs Person and Randolph H. Pherson.

Conclusion

This capsule-based overview of selected textbooks, handbooks, and general books about the application of intelligence analytic methodologies and technologies to examine homeland security, terrorism and counterterrorism is intended to provide a representative snapshot of the vast published literature on these subjects. As terrorists, whether as organized groups, loosely affiliated networks, and lone actors incorporate technological innovations in their warfare, government counter-terrorism agencies are also innovating analytically and technologically in their response measures. This is reflected in the new publications which are continuously being published on these issues.

Dr. Joshua Sinai is Professor of Practice, Intelligence & Global Security Studies, at Capitol Technology University, in Laurel, MD. Throughout his professional career, he has worked as a contractor for the Department of Homeland Security (National Operations Center, Science & Technology Directorate, Active Shooter Prevention Training Program, and the Federal Protective Service Training Division), as well as at the FBI's Foreign Terrorist Tracking Task Force (FTTTF). Dr. Sinai's publications include several

articles and book chapters on the insider threat, as well as Active Shooter – A Handbook on Prevention (ASIS International, 2016, 2nd edition, which is being revised and updated for a third edition).





Article Key Points

- MCI survivors among clinicians may develop persistent trauma triggers years later.
- MCI training improves knowledge/confidence, but many courses remain low-fidelity.

- Real-world MCI response needs adaptable triage; one-size-fits-all training may fail.
- Post-event support gaps are common; peer support + tailored psychiatric first aid helpful.
- Cumulative microtrauma may contribute to suicidality; longitudinal support needed.

Terrorists and Weapons of Mass Destruction: A History of Hype and the Possibility of a Dystopian Future

By Peter Bergen

CTCSENTINEL | September 2026, Volume 19, Issue 9
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.

Citations

[1] "Human Cost of Post-9/11 Wars: Direct War Deaths in Major War Zones," Watson School of International and Public Affairs, Brown University, September 1, 2021.
[2] "U.S. Military Casualties – Operation Iraqi Freedom (OIF) Casualty Summary by Casualty Category (As of August 31, 2026)," Defense Casualty Analysis System, accessed September 1, 2026.
[3] "The 9/11 Commission Report," 2004.
[4] "IRAQ: Weapons of Mass Destruction," Council on Foreign Relations, February 3, 2005.
[5] "A mystery unravelled," *Economist*, Agust 7, 2008; Sarah Pruitt, "When Anthrax-Laced Letters Terrorized the Nation," History.com, October 4, 2018.
[6] "Amerithrax or Anthrax Investigation," FBI.Gov, n.d., accessed August 18, 2026.
[7] Peter Bergen, *All the Presidents' Wars: Twenty-Five Years of America's War on Terror* (New York: W.W. Norton & Company, 2026), pp. 58-59.
[8] Seyed Hossein Mousavian, "Globalising Iran's Fatwa Against Nuclear Weapons," *Survival* 55:2 (2013): pp. 147-162.
[9] Mark Mooney, "Cheney Thought He Had Lethal Anthrax Dose," ABC News, July 14, 2008.
[10] "Aum Shinrikyo: The Japanese Cult behind the Tokyo Sarin Attack," BBC, July 6, 2018; "Global Proliferation of Weapons of Mass Destruction: A Case Study on the Aum Shinrikyo," Senate Government Affairs Permanent Subcommittee on Investigations, Staff Statement, October 31, 1995.
[11] Author interview, Charles Faddis, January 2010; Peter Bergen, "Al Qaeda's Track Record with Chemical Weapons," CNN, May 7, 2013.
[12] Columb Strack, "The Evolution of the Islamic State's Chemical Weapons Efforts," *CTC Sentinel* 10:9 (2017).
[13] Ibid.
[14] Rukmini Callimachi, "The ISIS Files," *New York Times*, April 4, 2018.
[15] Megan Friedman, "Georgi Markov and the Umbrella Gun," *Time*, February 17, 2010.
[16] Florian Flade, "The June 2018 Cologne Ricin Plot: A New Threshold in Jihadi Bio Terror," *CTC Sentinel* 11:7 (2018).
[17] Animesh Roul, "Ricin Threat and the Jihadist Conspiracy against India," MP-IDSA Commentary, November 13, 2025.
[18] Peter Bergen and Swati Pandey, "The Madrassa Scapegoat," *Washington Quarterly* 29:2 (2006): pp. 115-125.
[19] Diego Gambetta and Steffen Hertog, *Engineers of Jihad: The Curious Connection between Violent Extremism and Education* (Princeton: Princeton University Press, 2018), p. 8.
[20] Ibid.
[21] Clive Cookson, "AI Creates First Synthetic Viruses," *Financial Times*, August 6, 2026.
[22] Fabio Urbina, Filippa Lentzos, Cédric Invernizzi, and Sean Ekins, "AI in Drug Discovery: A Wake-up Call," *Drug Discovery Today* 28:1 (2023).
[23] Audrey Kurth Croin, "Biology's Tectonic Shifts and Novel Risks," *CTC Sentinel* 15:5 (2022).
[24] "Department of Homeland Security Report on Reducing the Risks at the Intersection of Artificial Intelligence and Chemical, Biological, Radiological, and Nuclear Threats," U.S. Department of Homeland Security, April 26, 2024.
[25] Daniel Byman and V. S. Subrahmanian, "Artificial Intelligence and the Future of Terrorism," Audio Briefs, CSIS, July 10, 2026.
[26] Andrew Glazzard, David McIlhatton, and Paul Martin, "Will Generative AI Fundamentally Change Terrorist Threats?" *CTC Sentinel* 19:5 (2026).
[27] Benjamin Mueller, William K. Rashbaum, and Al Baker, "Terror Attack Kills 8 and Injures 11 in Manhattan," *New York Times*, October 31, 2017.
[28] "Ohio Man Pleads Guilty to 29 Federal Hate Crimes for August 2017 Car Attack at Rally in Charlottesville," U.S. Department of Justice, March 27, 2019.
[29] "New Orleans Attack: Driver Acted Alone in ISIS-Inspired Rampage That Killed 14, Authorities Say," NBC News, January 2, 2025.
[30] Dustin Volz and Eric Schmitt, "How Terrorist Groups Are Using A.I. to Gain an Edge in Battle," *New York Times*, July 15, 2026.
[31] Jocelyn Kaiser, "NIH Says Grantee Failed to Report Experiment in Wuhan That Created a Bat Virus That Made Mice Sicker," Science, October 21, 2021.
[32] Kevin Collier and Jasmine Cui, "ChatGPT Safety Systems Can Be Bypassed to Get Weapons Instructions," NBC News, October 10, 2025.

[33] Adam Hadley, "Feature Commentary: Guardrails Under Test: Terrorist Misuse of AI Models and the Open-Weight 'Abliteration' Problem," *CTC Sentinel* 19:7 (2026).
[34] "Preparing for future AI capabilities in biology," OpenAI, June 18, 2025.
[35] "AI Executives Make Rare Collective Warning on Bioweapons Threat," Semafor, June 4, 2026; "In Support of Mandatory Nucleic Acid Synthesis Screening and Recordkeeping," dj.com, June 2026.
[36] Thomas C. Schelling in Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Redwood City, CA: Stanford University Press, 1962), p. vii.

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).

ISIS's Pakistan Province Releases Second Issue of English-Language Magazine Which Advocates for Joining ISIS in Pakistan, Lone-Actor Attacks

Source: https://www.counterextremism.com/press/extremist-content-online-media-group-linked-isis-pakistan-province-launches-new-online

On October 30, a propaganda group linked to ISIS's Pakistan Province released the second issue of *Invade*, an English-language web magazine. In a February 2026 post, the group claimed the magazine was meant to reach new online audiences. The 61-page second issue included articles calling for lone-actor terrorist attacks and a wallet address to donate Monero, a privacy cryptocurrency. The magazine also included the .Onion address of the newly created Al-Karrar Network.



The magazine's foreword encouraged steadfastness and faith in response to hardship and noted the current war between the U.S. and Iran, the ongoing conflict in Yemen, and listed ISIS and ISIS-inspired attacks around the world.

The first article called for the reader to immigrate to ISIS-held territory. The second main article provided a short history of the Muslim conquest of the Iberian Peninsula in the 8th century, the establishment of Al-Andalus, the golden age of Cordoba, and the subsequent Reconquista. The article claimed that specific lessons from the 8th-century invasion should be applied to ISIS fighters and supporters today, specifically that victory is only possible with faith, religiously mandated fighting is the path to victory, unity among fighters and factions is required for success, strength and preparation are obligatory, and that one should not be distracted by worldly luxuries.

Another main article called on the Pakistani people to fight, pledge their allegiance to ISIS, and institute religious law. The article claimed that issues such as corruption and violence against women and children were impossible to fix in a democratic system where people lived under human-made laws. The authors argued that security, justice, and prosperity could be achieved only by adopting religious law. The article noted that the Pakistani people have overwhelmingly chosen democracy and insulted ISIS, condemning the latter as Khawarij, terrorists, or agents of foreign powers.

Additional articles questioned whether unjust rulers invalidated religiously mandated fighting, condemned Jama'at Nusrat al-Islam wal-Muslimin (JNIM) in the Sahel region, and condemned Europe, the United States, and Russia for imperialism, modern policies in Africa, and the history of slavery and domestic anti-black racism.
The final major article consisted of the biography of a Pakistani man who joined al-Qaeda in Somalia before pledging his allegiance to ISIS after the declaration of the Caliphate in 2014, subsequent imprisonment by al-Qaeda, and eventual ISIS media work and death in a U.S. airstrike.



Why are so many teens being treated as terrorists?

Panic over boys being radicalised by the right is warping the UK's counter-terror response.

JOANNA WILLIAMS
COLUMNIST

1st November 2026

spiked

Women & Criminal Justice, 29: 181–187, 2019
© 2019 Taylor & Francis Group, LLC
ISSN: 0897-4454 print/1541-0323 online
DOI: 10.1080/08974454.2019.1633612

Routledge
Taylor & Francis Group

Check for updates

Introduction: Women, Gender, and Terrorism: Gendering Terrorism

Cyndi Banks

Associate Vice President of Student Success, Capilano University, North Vancouver, BC, Canada and Emeritus Professor of Criminology, Department of Criminology and Criminal Justice, Northern Arizona University, Arizona, USA

Terrorism and Political Violence Journal
Research Article

Gendering Terrorism: Comparing Female Versus Male Terrorism Offenders Using Closed-Source Data

Jonathan Kenyon, Maura Conway, Jens Binder & Christopher Baker-Beall

Published online: 27 Oct 2026



Abstract

This article addresses persistent gaps in terrorism studies by drawing on closed-source UK government risk assessment reports on 543 convicted extremists in England and Wales (2010–2023) to systematically compare female and male offenders, providing a gender-aware analysis of especially women's involvement. While prior scholarship has offered valuable insights, it often lacked empirical breadth and systematic comparison, leading to partial accounts shaped by gendered assumptions. Using quantitative and qualitative methods, this study examines offence histories, psychopathology, radicalisation pathways, online activity, motivations, roles, and assessed levels of engagement, intent and capability. Findings show women were more often categorised as affiliates, had fewer prior convictions, and were influenced by intimate partners; men engaged more in online learning and propaganda dissemination, while Islamist women relied heavily on the internet for radicalisation and attack planning. Notably, while many fewer in number, female attackers' plots progressed to execution at higher rates, challenging assumptions of women's lower threat. These findings highlight the need for gender-informed approaches to how terrorism is both studied and responded to.

The Terrorism Map Has Changed. Has Washington's Counterterrorism Strategy Kept Pace?

By Mahmut Cengiz

Source: https://www.hstoday.us/subject-matter-areas/counterterrorism/the-terrorism-map-has-changed-has-washingtons-counterterrorism-strategy-kept-pace/

Nov 03 – For more than two decades after September 11, 2001, American counterterrorism strategy was largely shaped by threats originating in Afghanistan, Pakistan, Iraq, Syria, and the broader Middle East. These regions became central to U.S. military operations, intelligence collection, terrorist-financing investigations, and international security partnerships.

That focus produced significant achievements. Al-Qaeda's central leadership was severely weakened, ISIS lost its territorial caliphate in Iraq and Syria, and numerous terrorist plots against the United States and its allies were disrupted. Yet the global terrorist threat has not disappeared. It has become increasingly decentralized, geographically dispersed, and operationally adaptive.

Today, some of the most persistent terrorist threats are emerging from Africa and South Asia, where organizations affiliated with al-Qaeda and ISIS continue attacking military installations, targeting civilians, exploiting weak governance, and expanding their operational capabilities.

The question facing Washington is no longer simply how to prevent

another September 11. It is whether American counterterrorism priorities adequately reflect the changing geography of terrorism.

The terrorist attacks and counterterrorism operations documented throughout 2026 in *Frontline Watch*, the biweekly monitoring series published by GTSC's *Homeland Security Today*, provide a compelling reason to revisit that question.

Africa is No Longer a Peripheral Counterterrorism Theater

Across the Sahel, the Lake Chad Basin, and the Horn of Africa, terrorist organizations have demonstrated remarkable resilience despite sustained military operations.

Jama'at Nusrat al-Islam wal-Muslimin (JNIM), an al-Qaeda-affiliated coalition, continues to conduct attacks against government forces and security installations in Mali and neighboring countries. Islamic State Sahel Province operates across parts of the central Sahel, while Boko Haram and Islamic State West Africa Province (ISWAP) remain active around northeastern Nigeria and the Lake Chad Basin.

These organizations are not merely surviving. They are exploiting local grievances, weak state institutions, porous borders, and political instability to maintain operational networks.

The September 15–29 edition of *Frontline Watch* documented JNIM attacks against Malian government forces and Russian Africa Corps personnel around Sévaré and Konna on September 20. The group claimed to have inflicted substantial casualties and damaged military equipment. Although its casualty claims were not independently verified, the reported attacks illustrated the continuing vulnerability of security installations in central Mali.

Subsequent reporting documented another JNIM explosive attack against a military convoy in Mali's Mopti Region on October 5.

In Nigeria, the October 6 attack against a military base in Kukawa, Borno State, demonstrated ISWAP's ability to organize coordinated assaults against defended positions. According to *Frontline Watch* reporting, at least ten Nigerian soldiers were killed, while Nigerian forces reportedly eliminated more than 25 militants while repelling the assault.

These incidents illustrate a persistent operational challenge: terrorist organizations continue to threaten military forces despite repeated counterterrorism campaigns.

For Washington, the implications extend beyond the immediate security of African states. Persistent terrorist activity can undermine regional governance, destabilize neighboring countries, threaten economic infrastructure, and create opportunities for transnational extremist networks.

Somalia Demonstrates the Limits of Geographic Containment

The Horn of Africa presents another important example.

Al-Shabaab has remained one of al-Qaeda's most durable affiliates, maintaining operational capabilities despite years of Somali, regional, and international counterterrorism pressure.

Its activities extend beyond Somalia's internal conflict.

The September 15–29 edition of *Frontline Watch* documented suspected al-Shabaab attacks against Kenyan security forces in Garissa and Lamu counties. On September 19, suspected militants reportedly attacked a Kenya Defence Forces patrol supporting security along the Lamu Port–South Sudan–Ethiopia Transport corridor.

The October edition subsequently documented an October 9 roadside explosive attack in Garissa County that killed two Kenyan police officers. Although al-Shabaab was suspected, organizational responsibility had not been conclusively established.

These incidents illustrate how militant activity can threaten border security, transportation infrastructure, and regional economic development.

At the same time, counterterrorism

operations continue. On September 17, U.S. Africa Command reported conducting an airstrike against an al-Shabaab weapons-storage facility in Somalia's Sanaag Region.
The operation demonstrated continuing American engagement, but it also raises a broader strategic question: Is U.S. involvement structured primarily around periodic military disruption, or does it sufficiently support sustainable regional security capabilities?
Airstrikes can destroy weapons and disrupt operational planning. However, long-term security also depends on capable local institutions, reliable intelligence networks, border cooperation, and effective governance. A strategy focused exclusively on eliminating militants risks overlooking the political and institutional conditions that allow terrorist organizations to regenerate.

South Asia Remains a Major Source of Terrorist Innovation

While Africa's security challenges deserve greater attention, South Asia presents a different but equally important threat environment.
Pakistan continues to face violence involving Tehreek-e-Taliban Pakistan (TTP), while Islamic State Khorasan Province (ISKP) remains a significant concern in Afghanistan and the wider region.
Recent *Frontline Watch* reporting demonstrates that militant organizations are adapting their tactics.
On October 3, 2026, TTP militants reportedly attacked police checkpoints in Pakistan's Dera Ghazi Khan District using explosive-laden drones. Additional incidents during early October involved quadcopter attacks against police positions and civilian areas in Khyber Pakhtunkhwa.
On October 5, an attack involving a drone in North Waziristan reportedly killed a child and injured seven others. The perpetrators were not conclusively identified.
These incidents matter not only because of their immediate consequences but also because they reveal the spread of inexpensive attack technologies.
Commercially available drones and modified unmanned systems can allow militants to threaten security installations and civilian targets without relying on more traditional methods of attack.
The increasing availability of these technologies creates challenges for local police forces, border-security agencies, and military units that may lack adequate detection and defensive capabilities.
South Asia also remains important because of the potential for terrorist organizations to maintain cross-border networks, exploit unstable border regions, and inspire attacks beyond their immediate operating environments.
Washington cannot assume that geographic distance eliminates the possibility of transnational threats.

The Middle East Still Matters, but the Threat Has Diversified

Reassessing counterterrorism priorities does not mean abandoning the Middle East.
ISIS networks remain active in Iraq and Syria, while the Houthis and other armed organizations continue threatening regional security and critical infrastructure.
The September 15–29 edition of *Frontline Watch* documented ISIS-linked attacks against Iraqi security personnel and an attempted attack against a power transmission installation in Saladin Province. These incidents demonstrate that the Middle East remains a consequential counterterrorism theater. However, the strategic environment has changed since the years when al-Qaeda's central leadership and ISIS's territorial caliphate dominated international counterterrorism planning. Terrorist organizations now operate through geographically dispersed affiliates, locally embedded insurgencies, online networks, and increasingly adaptable operational structures.

The United States therefore faces a more complicated challenge: maintaining capabilities against established threats while developing partnerships and intelligence coverage in regions where terrorist violence remains persistent.

Washington Needs a More Geographically Adaptive Strategy

The United States should consider five adjustments.

First, align intelligence priorities with evolving threat patterns. Intelligence collection and analysis should regularly incorporate developments in the Sahel, Lake Chad Basin, Horn of Africa, and South Asia rather than relying primarily on historical threat geography. Second, strengthen regional intelligence-sharing partnerships. Cooperation among neighboring countries is essential when terrorist organizations exploit international borders. The September 2026 announcement of a Kenya–United States–United Kingdom counterterrorism reporting initiative offers one example of how multinational cooperation can improve information collection. Third, invest in local institutional capacity. Training, investigative expertise, financial intelligence, border security, and judicial capabilities can help partner governments sustain gains beyond individual military operations. Fourth, anticipate tactical innovation. Counter-drone capabilities, infrastructure protection, digital investigations, and monitoring of terrorist financing should become increasingly important components of regional security cooperation. Fifth, evaluate outcomes rather than operational activity alone. Washington should assess whether its partnerships reduce attacks, weaken terrorist organizations, improve civilian protection, and strengthen local institutions over time.

These adjustments do not necessarily require a major expansion of American military deployments. In many cases, intelligence cooperation, technical assistance, targeted capacity building, and sustained diplomatic engagement may offer more practical and durable benefits.

A Changing Threat Requires Changing Priorities

The United States has spent 25 years developing sophisticated counterterrorism capabilities. Those investments have prevented attacks, disrupted organizations, and strengthened international cooperation.

But terrorist organizations have also learned to adapt.

They have decentralized their structures, developed regional affiliates, exploited political instability, and adopted new technologies. In several African and South Asian theaters, they continue demonstrating the ability to conduct attacks despite substantial counterterrorism pressure.

The incidents documented in *Frontline Watch* are not, by themselves, sufficient to establish a global statistical shift in terrorism. They do, however, provide concrete illustrations of the persistent and geographically dispersed threats that counterterrorism policymakers must assess.

Washington should not wait for another major international terrorist attack before reassessing where its intelligence, partnerships, and preventive capabilities are most needed.

The geography of terrorism has evolved. American counterterrorism strategy must be able to evolve with it. The objective should not be to replace one regional priority with another, but to build a flexible, intelligence-driven approach that responds to terrorist capabilities wherever they emerge.

Dr. Mahmut Cengiz serves as Managing Editor for Counterterrorism at GTSC's Homeland Security Today and Chair of its Counterterrorism Advisory Board. He is also Professor of the Practice in Criminal Justice at the University of Kansas, where he leads the Global Crime concentration, and Senior Advisor at the International Coalition

Against Illicit Economies (ICAIE). He is a member of the Global Initiative Against Transnational Organized Crime (GI-TOC) Network of Experts and a Fellow at Small Wars Journal–El Centro. His expertise focuses on terrorism, transnational organized crime, illicit economies, terrorist financing, intelligence analysis, and the convergence of criminal and terrorist networks. Previously, Dr. Cengiz served as an Associate Professor and researcher at George Mason University's Schar School of Policy and Government and the Terrorism, Transnational Crime and Corruption Center (TraCCC). From 2018 to 2025, he served as Academic Director and Co-Principal Investigator of the U.S. Department of State-funded Global Terrorism Trends and Analysis Center (GTTAC), overseeing research and analysis of more than 64,000 terrorist incidents worldwide and leading a multidisciplinary team of researchers and analysts. Dr. Cengiz brings extensive international experience in law enforcement, capacity building, and security cooperation across the Middle East, Asia, and Europe. His professional background combines operational experience with academic research and policy analysis, providing a practitioner-oriented perspective on emerging security threats. He has authored or co-authored nine books and numerous scholarly articles, policy studies, and security analyses. His publications include Typologies of Terrorist Organizations (2025), Murder by Mail (2024), The Illicit Economy in Turkey(2019), and the forthcoming Military Coups and Fragile Democracies (Bloomsbury, 2027). Dr. Cengiz holds two master's degrees and two doctoral degrees, including a Ph.D. in Public Policy from George Mason University and a Ph.D. in Sociology from Ankara University.

Terrorism facts

Cars and Blades

For all the attention on new technology, the attack methods that have killed people in crowded places over the past two years are old ones. On 25 July 2026 a 21-year-old drove a rented van into crowds at Berlin's Christopher Street Day celebration, then continued the attack with a blade. One person died and 29 were injured. German authorities called it an Islamist terrorist attack. The attacker had been given a suspended juvenile sentence for planning an attack only two months earlier.

The pattern repeats across jurisdictions and motives. A vehicle was driven into pedestrians in Derby in March 2026, injuring seven. In Modena in May, a driver rammed pedestrians and stabbed a bystander; Italian authorities ruled out terrorism and pointed to psychiatric illness. In Vancouver, the man accused of killing 11 people with an SUV at the Lapu Lapu Day festival in April 2025 has just pleaded not guilty, with trial set for 2027. In London, the Golders Green attack in April was a knife attack in an ordinary street.

WHY THESE ATTACKS PERSIST

Low-sophistication attacks need no network, no training and no materials that trigger alerts. They require only a crowd and access to it. For lone actors, young offenders and people with mixed or unclear motives (see article 4), they are the default choice. And because the motive is often ambiguous for hours or days, the first responders on scene are nearly always venue staff, stewards and the public, not police.

WHERE THE VULNERABILITIES ACTUALLY SIT

1.Temporary and linear events. Parades, festivals, markets and fan zones are the hardest to protect with permanent hostile vehicle mitigation. The Christmas market season, now beginning, is a known high-risk period.

2.The edges. Attacks are frequently launched at the perimeter, in queues and dispersal routes, where security is lightest and crowds are densest.

3.Gaps in temporary barriers. Emergency and service vehicle access points are a recurring weak point; a closed road is only as good as its controlled gap.
4.Time to intervention. In marauding knife attacks, the outcome is often decided by what bystanders and staff do in the first minutes.

THE PROFESSIONAL VIEW

There is no technology fix. The defences that work are layered and unglamorous: properly specified and installed vehicle security barriers (to IWA 14 or the earlier PAS 68), controlled vehicle gates staffed by people with authority to stop traffic, crowd management that avoids dense static queues on open roads, and staff trained to run, hide, tell and to give first aid. Martyn's Law will make several of these expectations explicit for qualifying sites and events from 2027.

Hoax Threats

On Monday 2 November 2026 a Wizz Air flight from London Luton to Sofia diverted to Budapest after a bomb threat. The next day at least seven European flights received threats, including two departing the UK, from Heathrow and from Manchester, which landed in Poland and Spain. Warsaw's Modlin airport closed temporarily, and Italian Eurofighters escorted aircraft into Rome Fiumicino. A cruise ship was also targeted. No explosives were found. The UK government described the incidents as malicious hoax threats. Further fighter scrambles followed on 5 November.
An analyst at Osprey Flight Solutions called seven confirmed threats against flights in a single day exceptional. No one has yet been identified as responsible, and investigators have not established that the threats were coordinated.

WHY THIS MATTERS BEYOND AVIATION

The aviation wave is the most visible example of a broader pattern. The same week, refrigeration systems at supermarkets across seven European countries were sabotaged remotely (see article 11). Some analysts see both as part of a campaign of low-cost, deniable disruption; others caution that copycat behaviour and online subcultures can produce the same clusters. Either way, the security effect is the same.
A hoax achieves several things an attacker values:
1.Disruption at almost no cost. A message or call can ground aircraft, empty a stadium or close a shopping centre.
2.Reconnaissance. Every evacuation shows how a site responds: how long it takes, where people gather, where police deploy, which exits are used.
3.Erosion of trust. Repeated false alarms create fatigue among staff and the public, which slows the response when a threat is real.
4.Status. For young offenders in online communities, causing an evacuation is itself the reward (see article 4).
The ICCT has also warned that automated tools could be used to generate threats at a volume that overwhelms security services and businesses.

THE PROFESSIONAL VIEW

The default reaction to a bomb threat, total evacuation, is not always the safest. UK protective security guidance has long favoured a structured assessment by a trained, named decision-maker, using the content and context of the threat, a search of the site, and a choice between evacuation, invacuation and continued operation. Evacuating several thousand people into an unsearched assembly point next to a road can create the very crowd an attacker wants.

Martyn's Law will require qualifying premises to have procedures for evacuation and invacuation. Bomb threat handling should sit squarely within them.

Younger, Faster, Less Ideological

The Home Office's latest Prevent statistics, published on 6 August 2026, recorded 10,293 referrals covering 9,957 individuals in the year to September 2025. That is a 39 per cent rise on the previous year and the highest annual figure since the series began in 2015. Where age was known, 11 to 15-year-olds were the largest group at 36 per cent; 393 referrals concerned children aged ten or under. Extreme right-wing concerns accounted for 20 per cent of referrals with a recorded concern type. Only 18 per cent were adopted as Channel cases.

The Home Office itself attributes the shape of these figures to an increasingly fragmented ideological picture, in which vulnerable individuals are less fixed in any one position. Practitioners have a shorthand for it: mixed, unclear or unstable ideology.

THREE SHIFTS THAT MATTER

1.Age. Analysis drawing on the 2026 Global Terrorism Index suggests young people and minors accounted for 42 per cent of terrorism-related investigations in Europe and North America in 2025, roughly three times the 2021 share. The UK is legislating for youth diversion orders, a civil route for people aged 21 or under, precisely because arrest and prosecution were not designed for 14-year-olds.

2.Nihilism as a motive. In the US, the FBI now classifies the most dangerous actors in online networks such as "764" (part of a wider ecosystem known as "the Com") as nihilistic violent extremists. These groups groom and extort young people into self-harm, animal cruelty and violence, and glorify mass-casualty attacks. The Justice Department brought its first terrorism charge against an alleged 764 member in 2026, and the FBI reports investigations into more than 300 people linked to the network.

3.Speed. Researchers describe radicalisation timelines measured in weeks, sometimes days, driven by gaming platforms, Discord servers and encrypted chats rather than recruiters or mosques or rallies.

WHY THIS REACHES THE PRIVATE SECTOR

The security implications are not confined to schools and social services. Young people are a large share of the workforce in hospitality, retail, events and contract security. Venue operators face a would-be attacker who may have no group, no clear cause and no prior record, and whose target selection is driven by notoriety rather than symbolism. And a growing number of hoax threats, swatting incidents and bomb threats are traced back to minors acting for status in online communities.

THE PROFESSIONAL VIEW

The old screening question, "what does this person believe?", is the wrong one. Behavioural threat assessment asks "what is this person doing, and is it moving towards violence?" Fixation on previous attackers, research into weapons or targets, leakage of intent online, and a sudden collapse in personal circumstances are better indicators than any ideological marker.

The Executive as Target

The killing of UnitedHealthcare chief executive Brian Thompson outside an investor conference in Manhattan in December 2024 changed boardroom attitudes to executive protection almost overnight. Two years on, the data shows it was not an isolated event but part of a curve.

WHAT THE NUMBERS SAY

The Security Executive Council's Executive Targeting Report, published in February 2026 with Mercyhurst University, analysed 424 open-source incidents worldwide from 2003 to October 2025. It found that 2025 incident volumes effectively doubled those of 2024. CEOs were the target in 64 per cent of cases, but attacks on other senior executives are growing, and incidents involving female executives have doubled since 2021. According to analyses of the dataset, about a third of incidents ended in death or injury, roughly three-quarters of attackers were strangers to their target, and residential and workplace targeting have both risen since 2020.

Allied Universal's World Security Report, based on a survey of 2,352 chief security officers in 31 countries, found 42 per cent reporting a significant rise in threats of violence against executives, and three-quarters saying their company had been targeted by misinformation or disinformation.

THREE THREAT STREAMS, ONE TARGET

1.Grievance-driven lone actors. The Thompson model: an individual with a grievance against an industry, a policy or a product, who researches routines and attacks at a predictable point. Healthcare, pharmaceuticals, technology, energy and finance are the most exposed sectors.

2.State-directed proxies. In March 2026, German authorities thwarted a Russian-ordered plot to kill the head of a German defence company, echoing the 2024 plot against Rheinmetall's chief executive. State actors now hire criminals to do this work (see article 3).

3.Politically motivated violence. The assassination of Turning Point USA's Charlie Kirk in September 2025 showed how quickly public commentary on contested issues can turn into physical risk. Executives who speak publicly on the Middle East, AI, energy or social policy carry more exposure than those who do not.

THE PROFESSIONAL VIEW

Executive protection is no longer about close protection officers alone. It is primarily an intelligence problem: knowing what is being said about your principals online, how much of their life is discoverable (home address, children's schools, travel patterns, car registrations), and whether any individual is moving from grievance towards action. Behavioural threat assessment, the same discipline that applies to workplace violence, is the core skill.

The weakest points are almost always the predictable ones: the walk from car to door, the regular gym, the published speaking engagement, the home.

After Leipzig: The Drone Threat

For a decade, the drone threat to crowded places was argued about in conference rooms. That debate ended at Leipzig/Halle airport. According to German reporting summarised by the European Council on Foreign Relations, CCTV shows a quadcopter, roughly the size of a microwave oven and carrying explosives, flying towards a parked Antonov cargo aircraft, striking a wing and falling to the tarmac, where a bus driver found it. The explosives did not detonate. It is the closest call yet to a drone-borne mass-casualty event in Europe.

THE WIDER PATTERN

Leipzig sits on top of a rising baseline. The German air navigation service recorded 227 drone sightings by pilots in 2025, and 2026 is on track to exceed that. Copenhagen closed for four hours in September 2025; Brussels, Oslo and Munich have all suffered closures. A single evening's disruption at Brussels has been estimated to cost around EUR 2 million. A June 2026 IISS research paper assessed it "highly likely" that Russia ran a drone campaign over Europe, largely in late 2025, with some flights possibly launched from shadow fleet vessels.

But security managers should resist reading this purely as a state problem. ECFR's Ulrike Franke notes that, despite plots, no major terrorist drone attack has yet occurred in Europe, which she calls surprising given how available the technology is. The tactics, techniques and procedures developed in Ukraine (fibre-optic guided drones immune to jamming, cheap first-person-view platforms, interceptor drones) are diffusing to every kind of actor.

THE THREE GAPS THAT MATTER TO PRIVATE OPERATORS

1.Detection. Radio-frequency detection, the cheapest option, fails against drones that are pre-programmed, autonomous or fibre-guided. Radar struggles with small, slow targets and birds. Optical systems need line of sight. Every serious assessment ends in the same place: layered sensors, and humans to interpret them.

2.Authority. In most jurisdictions, only police or the military may interfere with a drone in flight. Germany has amended its law to let the armed forces intercept in extreme cases, and France has created a route for private companies to provide drone protection for civilian infrastructure. The UK and US remain more restrictive for private operators. Jamming near an airport or a city centre can create more danger than it removes.

3.Procedure. Many venues have a drone policy that ends with "call the police". It does not say who decides to stop an event, move a crowd under cover, or protect a VIP arrival while the police are on their way.

THE PROFESSIONAL VIEW

Drone defence for most TiNYg members is not about buying an effector. It is about knowing your airspace (what normal looks like over your site), agreeing in advance with police who holds intervention authority, and building drone sightings into the same decision-making as a suspicious item or a hostile reconnaissance report. Hostile reconnaissance by drone, rather than attack by drone, is the more likely near-term use against private sites.

The New Epicenter of Global Terror

By Eghosa E. Osaghae

Source: https://www.foreignaffairs.com/nigeria/new-epicenter-global-terror#

Nov 09 – Twenty-five years after 9/11, much of the world has moved on from the war on terrorism. Following the defeat of the Islamic State in Iraq and Syria and the U.S. withdrawal from Afghanistan in 2021, Washington has turned to other major concerns; along with many of its European allies, the United States has been more preoccupied with the growing confrontation with China, and with the wars in Ukraine and the Middle East, than with the threat of transnational extremism. Buttressing this shift has been a general decline in terrorist attacks in many parts of the world since ISIS's peak, in the mid-2010s.

Yet there is one region of the world where terrorism not only persists but also appears to be growing. According to reports by the United Nations and the Global Terrorism Index, Africa is the overwhelming center of terrorist activity today. The African continent accounts for more than 50 percent of all global terrorism-related deaths over the past five years. It also hosts three of the four deadliest jihadi groups in the world: ISIS, which is now primarily based in Africa, Jamaat Nusrat al-Islam wal-Muslimin (JNIM), and al-Shabab. (The fourth is Tehrik-e-Taliban Pakistan, also known as the Pakistani Taliban.) Six of the ten countries that are most affected by terrorism are also in Africa: Burkina Faso, the Democratic Republic of the Congo, Mali, Niger, Nigeria, and Somalia. And whereas the Middle East has had a 93 percent

decline in terrorist attacks between 2017 and 2025, the Sahel has experienced a 17 percent growth over the same period, with a record 4,043 terrorism deaths in 2023 alone.

To the extent that African terrorism has attracted global concern, much of the attention has focused on the Sahel region. The broad swath of land separating the Sahara and the Maghreb in the north from sub-Saharan Africa is a hotbed of extremism, hosting JNIM and ISIS affiliates such as Boko Haram in Nigeria, Cameroon, and Chad, as well as bandit groups such as Lakurawa in Niger and Nigeria and al-Shabab in Somalia. But terrorist activity in Africa now extends to a host of other countries in western, central, and southern Africa as well, including Benin, the Central African Republic, Mozambique, and Togo. Many of these countries have little previous history of jihadi ideology or extremist violence. World leaders overlook this continent-wide terrorist threat at their own peril. Not only have terrorist groups become a major challenge to African stability and development; they also pose a growing danger to global security. For now, these groups may appear to have little capacity to project their power beyond Africa's borders. Yet amid the new scramble for Africa's mineral resources—and for influence on the continent—this may change. Global powers, especially China and Russia, have been increasing their efforts to gain economic, political, and military leverage in Africa, which has in turn undermined collective international initiatives to fight terrorism. And many African jihadi groups themselves have strong anti-Western sentiments and have been using the resource wars to help build transnational networks.

Thus far, the global response to the African threat has largely focused on military operations, especially in the Sahel. But to truly address the phenomenon, outside powers and world leaders will need to understand the underlying forces that have led to this proliferation of extremist groups. Above all, they will need to find new ways to help African countries address the erosion of state institutions and governance that has made terrorism endemic across the continent.

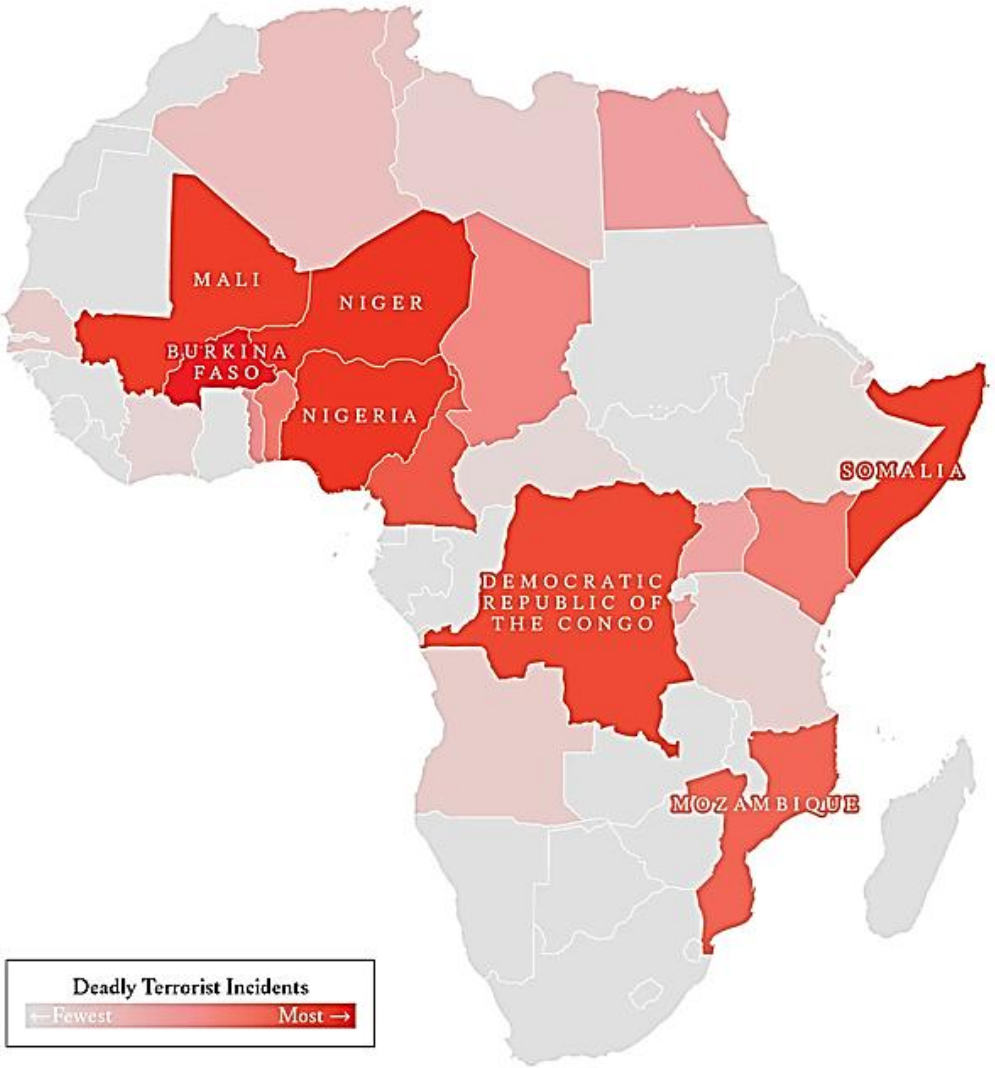
Neglected youth

Africa's entanglement with terrorist and jihadi groups is hardly new. Al-Qaeda's 1998 attacks on U.S. embassies in Dar-es-Salaam and Nairobi were planned from Sudan, where Osama bin Laden had been based between 1991 and 1996. After 9/11, security experts viewed those attacks as a crucial precursor that should have set off alarm bells. Then, in the early years of the twenty-first century, local African groups coalesced into al-Shabab, based in Somalia, which also began to pursue transnational terrorism as an affiliate of al-Qaeda. Later, al-Qaeda in the Islamic Maghreb formed a major foothold in Mali. These developments prompted a number of Western-led antiterrorism campaigns, often supported by African forces. Most notable were the military interventions in the Sahel led by the French and other Western special forces and the initial U.S.-supported intervention force in Somalia, the so-called Somali Warlord Alliance.

But these counterterrorism operations did little to stop extremist activity in Africa. In the 2010s, countries in and close to the Sahel began to transition from being breeding grounds of terrorism to becoming the focus of terrorist attacks. Over the past few years, these countries have not only continued to be the places where terrorist groups can organize, radicalize their adherents, and spread violent extremist ideology; they also now bear the brunt of terrorist attacks and killings and the instability and breakdown in security that go with them. Worse, this activity has spread to new areas of the continent, such as Benin, the Democratic Republic of the Congo, and Mozambique, where there had not been jihadis previously. In these countries, terrorist groups have capitalized on long-standing popular grievances spurred by government neglect, exclusion, and poverty. The jihadi expansion has

been led by new local groups with connections to al-Qaeda and its branch JNIM in the Sahel region of West Africa and to ISIS affiliates in central Africa, whose major motivations include generating wealth from illegal mining, smuggling, and transnational organized crime.

Where terrorism caused the most deaths in Africa, 2025



Source: 2026 Global Terrorism Index. Institute for Economics and Peace.

What the outside world has often failed to recognize—both in the earlier and more recent phases of extremism—are the underlying factors that have made so many African countries prone to this activity. In nearly every case, fragile or collapsing state institutions have been crucial enablers: states' inability to ensure the welfare and security of their citizens, to exercise sovereign authority over the length and breadth of their territory, and to alleviate the widespread poverty, unemployment, and disease that have created openings for extremism. In many countries, these factors have been exacerbated by large numbers of internally displaced persons and refugees, a lack of social infrastructure, and perennial violent conflict. The unique characteristics of African demography have added to the challenge. In contrast to the aging populations of most other regions of the world, people under the age of 30 make up nearly 70 percent of Africa's population and are also most affected by state failure. Large numbers of young people are not in school—more than 270 million African children in 2026, accounting for more than 40 percent of the global total. Nigeria alone has nearly 20 million youth out of school, the highest of any country in the world. At the same time, youth unemployment has remained persistently high: the continental average is 18 percent, but in some countries, such as Djibouti, where mass employment opportunities are limited and young people generally lack the requisite education for

skilled employment in the logistics and transport sector that dominates the economy, youth unemployment may reach more than 75 percent. Disaffected young Africans constitute a huge reservoir of potential recruits for extremist groups, which have grown commensurately: according to recent estimates, al-Shabab has more than 15,000 fighters and JNIM has around 6,000.

But state complicity also plays a role. It is now well documented that political leaders have been building ties to bandit and terrorism groups to secure and consolidate their power. For example, the emergence of Boko Haram and various other militant outfits in Nigeria has been abetted by state governors and influential politicians employing them to intimidate opponents during elections. It is worth noting, as well, that elites in Muslim-dominated northern Nigeria initially opposed the U.S. designation of Boko Haram as a terrorist group—based on the assumption that the group was defending the interests of mainstream Muslims and northerners. This kind of support helped legitimize the group and enabled it to extend its control beyond the northeast of the country. The adoption of sharia law in the early years of the twenty-first century by 12 predominantly Muslim states in northern Nigeria also helped incubate Boko Haram. In this sense, Nigeria followed the path of Sudan, whose long history of Islamic fundamentalism and practice of sharia law made it a safe haven for bin Laden as he began to build his ideology of global terrorism.

Yet another contributing factor has been climate change and natural resource wars. Many of these countries have difficult desert geographies and have been beset with growing food insecurity and conflicts over diminishing resources. The result has been the emergence of so-called ungoverned territories within a number of African countries—areas characterized by power vacuums, porous borders, and illicit mining of critical minerals and other natural resources by terrorist groups, bandits, and criminal gangs. Often in these places, parallel state structures have been established by nonstate actors—not only to provide public goods, including safety, protection, and social services but also to challenge state legitimacy through sectarian uprisings and war. As these extremist nonstate groups seek to root their ideologies in ethnic, religious, and communal identities, territorial control has become central to their goals. This is especially true of jihadi groups such as al-Shabab, Boko Haram, JNIM, and ISIS affiliates, which aim to create caliphates, although none has thus far demonstrated the capacity to take over an entire state.

Out of Africa

Although the domestic sources of African terrorism are important, external factors and global interconnections have been even more crucial to its spread. Take the continent's jihadi and radical Islamist movements, which have for decades been inspired and supported from outside. For example, the 1979 Iranian Revolution spurred the rise of Shiite movements among Muslim youths across Africa. The Iranian government actively supported the movements by sponsoring the establishment of schools and mosques, offering scholarships for students to study in Iran, and creating training and indoctrination programs. Today, Ibrahim al-Zakzaky's radical Islamic Movement of Nigeria, whose goal is to overthrow the secular government and establish Islamic law, remains one of the more resilient Iranian affiliates in Africa and has training camps in northwestern Nigeria that are linked to Iran and Lebanon's Hezbollah.

In the 1990s, the exploits of the Taliban in Afghanistan inspired young Muslim radicals in northern Nigeria, where the forerunners of Boko Haram initially called themselves the Taliban. In turn, terrorism researchers have identified Qatar, Saudi Arabia, Turkey, and other Middle Eastern powers as funders of Salafi extremism, which espouses the violent imposition of Islamic law on everyone, including fellow Muslims.

Such is the success of these efforts that many

African terrorist groups today consider themselves part of the global network of Salafist jihadism.

Among the most important external forces driving African terrorism are porous borders and the free flows of weapons, drugs, money, and human trafficking into and out of the continent. These flows have facilitated the integration of African groups into transnational terror networks. Al-Shabab was one of the earliest examples of this phenomenon: the group was founded by Somali supporters of the Afghan mujahideen in the late 1980s. Later, it became an affiliate of al-Qaeda, pledging allegiance to the group in 2012.

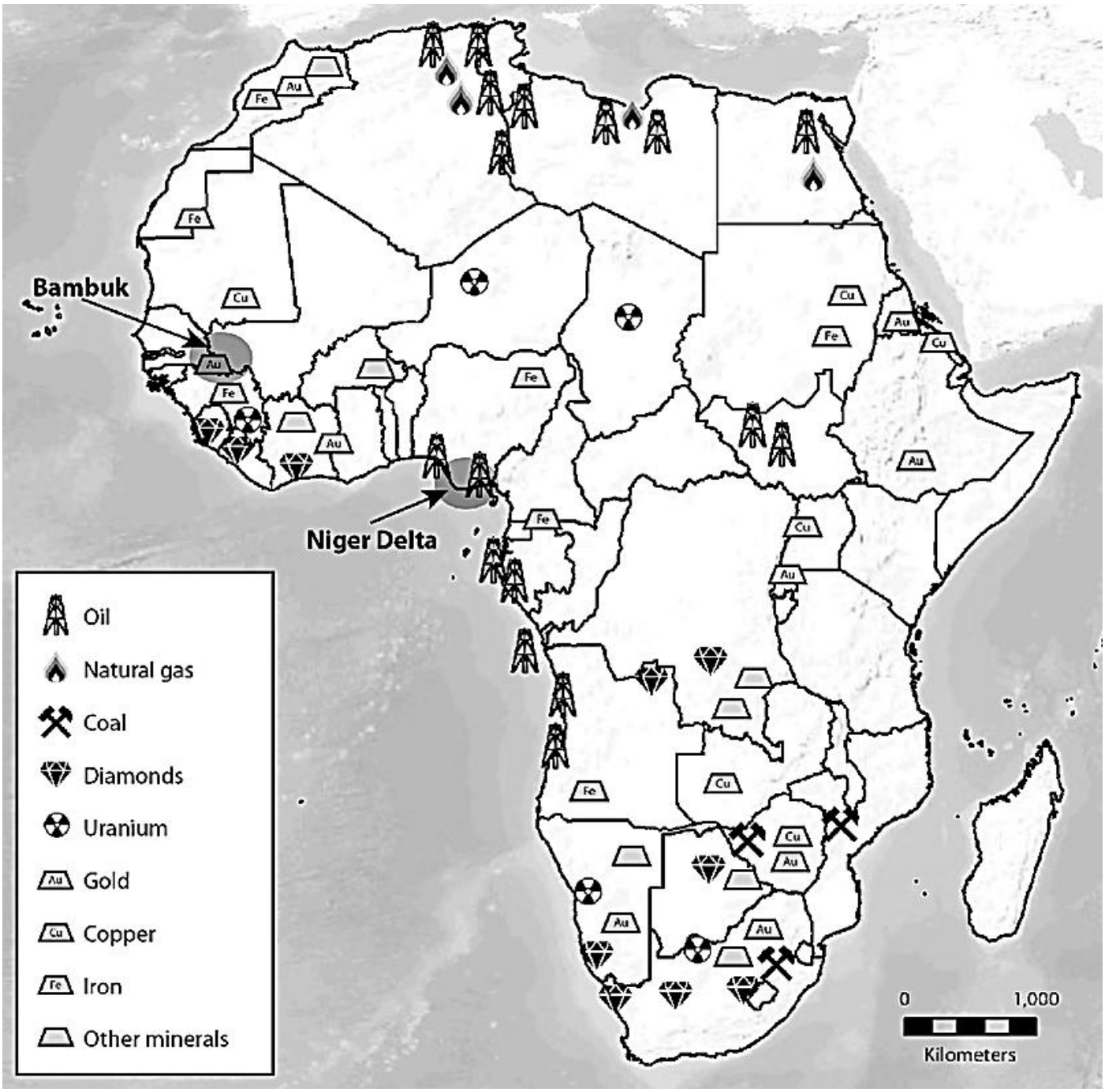
Other African groups followed a similar trajectory. Al-Qaeda's African affiliates have grown to include Ansaru, a splinter faction of Boko Haram operating in northern Nigeria, as well as al-Qaeda in the Islamic Maghreb, which is based in Algeria. ISIS has added a panoply of African groups to its own network, such as Islamic State Sahel Province in Burkina Faso, Mali, and Niger, and Islamic State West Africa Province, which is active in the Lake Chad Basin. And it has developed ties with Islamic State Central Africa Province, which also operates in parts of Mozambique and the Democratic Republic of the Congo and Uganda; and Islamic State in Somalia, which is a rival of al-Shabab. Meanwhile, al-Shabab has cultivated links to the Houthis in Yemen, a development that has heightened the potential for transnational terrorism to become enmeshed in the struggle for control of the Red Sea and the Gulf of Aden between Egypt, Ethiopia, Saudi Arabia, and Turkey following conflicts and closures in the Strait of Hormuz.

These transnational affiliations have offered African groups many advantages, bringing new sources of funding, new weapons (including drones), and training in suicide bombing and IEDs, as well as indoctrination, foreign fighters, intelligence, and logistics. In return, African terrorist groups have helped their international affiliates by engaging in sea piracy and smuggling, human trafficking and migrant smuggling, money laundering, kidnapping for ransom, robbery, livestock rustling, drug trafficking, and illegal mining. African groups use many of these activities, as well as illegally taxing the areas under their control, to raise illicit funds for their international affiliates.

In addition, African jihadis provide personnel for international operations—al-Shabab members have been involved in terrorist training operations in the Philippines—and safe havens for fugitive terrorists. During the decades of the post-9/11 war on terrorism, there was a steady influx to Africa of foreign terrorists, fighters, and instructors who were fleeing Iran, Iraq, Syria and other parts of the Middle East. Others came from North Africa, especially following the civil war in Libya and unrest in Algeria. These foreign extremists brought with them massive amounts of weapons and helped turn Africa into a center of terrorist activity. As the epicenter of global terrorism today, Africa now houses numerous al-Qaeda and ISIS operatives, a fact that increases the risk that Africa-based groups may be planning operations beyond the continent.

More minerals, more militants

In theory, international engagement in African security should help contain the rising terrorism threat. But the record thus far is not promising. During the war on terrorism, the United States, the EU, the United Nations, and international security organizations provided support for numerous counterterrorism campaigns on the continent. These efforts included backing the G5 Sahel—a counterterrorism initiative by Burkina Faso, Chad, Mali, Mauritania, and Niger—as well as support for regional counterterrorism initiatives, including in Mozambique and Somalia, as well as the Multinational Joint Task Force, which aimed to combat terrorism in the Lake Chad region. Most of these efforts failed or were not sustained long enough to change the trajectory, and the worsening security situations that they left in



their wake fueled anti-Western sentiment. And now, with Russia and China pursuing interests of their own in many parts of Africa, involvement by outside powers is often driven by a desire for strategic minerals and a quest for geopolitical influence, interventions that have only further encouraged terrorist activity. In the Sahel, the withdrawal of U.S. and French forces between 2022 and early 2025 created power and security vacuums. Russia has quickly exploited the situation, using bilateral defense pacts and mercenary and Africa Corps forces to gain access to minerals and natural resources that France had previously controlled. Indeed, in many parts of Africa, global competition for critical minerals has become a new driver in the spread of terrorism. In the Manono district of Congo, for instance, American,

Australian, and Chinese firms are enmeshed in long-running disputes over lithium deposits, which has made counterterrorism operations in the same area more difficult: the various international players no longer want to coordinate on counterterrorism and terrorist groups are using external rivalries to strengthen their own operations. A similar scenario is playing out in other resource-rich areas. It is now urgent that leading world powers adopt a different approach. A first step is to recognize the problem for what it is. Jihadi terrorism today is not a local or regional problem afflicting a handful of African countries; it is a worldwide threat. It can be effectively tackled only through concerted and sustained international action. Although internationally backed counterterrorism efforts by the African Union and other regional forces are more needed than ever, the new scramble for resources has become an obstacle to international collaboration in Africa. In this regard, it will be crucial to embrace the common protocols and regulatory frameworks for critical minerals and other resources being developed by the AU and other regional African organizations—which seek to reduce the scope for illicit activities and ensure that that the countries benefit more from the resources through more inclusive and accountable governance structures. Most important, outside powers need to engage with the root causes that have made the continent so prone to terrorist activity, even when it has been effectively countered elsewhere in the world. As the former UN Secretary-General Ban Ki-moon said in 2015, "Good governance is what will kill terrorism." Northern Ireland after the Good Friday Agreement—whose institutional reforms such as power sharing, human rights protections, and community policing proved to be more effective than military operations—is a case in point; so is the 2016 peace agreement between the Colombian government and the FARC, which included governance reforms in previously neglected parts of the country as part of its stabilization measures.

The United States as well as governments in Europe and international bodies need to shift their focus from military operations to addressing the actual social and economic sources of state fragility that have made so many African countries fertile ground for conflict and extremist violence. This would of course involve strengthening state capacities, and it would require regional efforts as well as more targeted development assistance. None of it will be easy, but doing nothing would be far worse. Unless African countries and their international partners can begin to address the underlying dynamics that are driving Africa's transnational terrorism problem, it is unlikely to stay in Africa for much longer.

Eghosa E. Osaghae is Director-General of the Nigerian Institute of International Affairs.

Six Christians Beheaded by Islamists in Northern Mozambique

Source: https://www.barnabasaid.org/us/news/six-christians-beheaded-by-islamists-in-northern-mozambique/

Nov 10 – Six Christians have been beheaded in separate attacks carried out by Islamists in Cabo Delgado Province, northern Mozambique.

Three were captured and killed by militants from Islamic State Mozambique (IS-M) in Matambalale, Muidumbe District, on Sunday November 1.

Three others suffered the same in separate attacks in Mueda District.

In the past few months, IS-M attacks against Christians in Cabo Delgado have become more frequent, with at least eight fatalities reported in September and into October.



Counter-terrorism experts have assessed that IS-M has grown to an estimated 400-500 fighters following a recruitment drive in early 2026.

An attack on a Christian village in Cabo Delgado in 2024

According to a senior analyst from the Armed Conflict Location and Event Data project, "IS-M is engaged in a political project … that rejects the secular state and advocates for rule based on their interpretation of Islamic law."
Around 2,750 civilians have been killed by IS-M since 2017, while many thousands have been displaced by the ongoing violence.

Czech FM: PC Europe never talked about the danger of Islamic terrorism from migration

By Etgar Lefkovits
Source: https://www.jns.org/news/israel-news/czech-fm-pc-europe-never-talked-about-the-danger-of-islamic-terrorism-from-migration

Nov 19 – European nations are beginning to recognize the terrorism threats posed by mass migration, having ignored the issue for years due to political correctness, the Czech foreign minister said on Wednesday. "I think people in Europe and in many European countries are starting to realize the problem with aggressive Islamism and the level of terrorism that might be hidden inside the problem we call the mass migration," Petr Macinka told JNS during a visit to Jerusalem. The top Czech diplomat said his country has always refused mass migration, including during a surge in 2015, and remains one of Europe's safest countries, contrasting the Czech Republic's situation with that of Germany, Sweden, France, Belgium and other Western European countries.
"There is a group of people who are carrying their culture with them, their rules, their way of life and religion, and they think they can come to Europe and live with their own rules, with Sharia," Macinka said, referring to Islamic religious law. "When we see what happened in Germany since 2015, there was not a week without a bombing, stabbing, or mass raping, etc.," he said.

"The Politically Correct Europe was never able to describe it with the right words," Macinka continued. "We knew that mass migration can bring the risk of Islamist terrorism to Europe, but we were not allowed to say that. They thought that this was politically incorrect because they thought that even terrorists have their human rights. Well, we don't think that way."

Ties that bind
Macinka was in Israel this week as part of a top

government delegation led by Czech Prime Minister Andrej Babiš along with senior ministers covering defense, public health and sports. One of Israel's staunchest allies in Europe, the Czech Republic has been an outspoken voice for Israel on the continent and in international forums ever since diplomatic relations were restored in 1990 after the end of Communist rule.

"Our own historical experience and dark history makes us much closer than some other nations and countries in Europe," he said. Czechoslovakia was abandoned by its Western allies in 1938 and 1939, leading to its dismemberment and German occupation before World War II even began in Europe. Macinka noted that the Czech Minister of Sport found a listing of family members killed during the Holocaust during the delegation's visit to the Yad Vashem Museum in Jerusalem.

The historic friendship between Israel and the Czech Republic dates back to early 20th-century Zionist ties and pivotal military and diplomatic support during Israel's founding in 1948.

Czechoslovakia's first president, Tomáš Garrigue Masaryk, supported Zionism and opposed antisemitism, and visited Mandatory Palestine in 1927 out of lifelong sympathy for the Jewish people and personal religious and scholarly interest in the Holy Land.

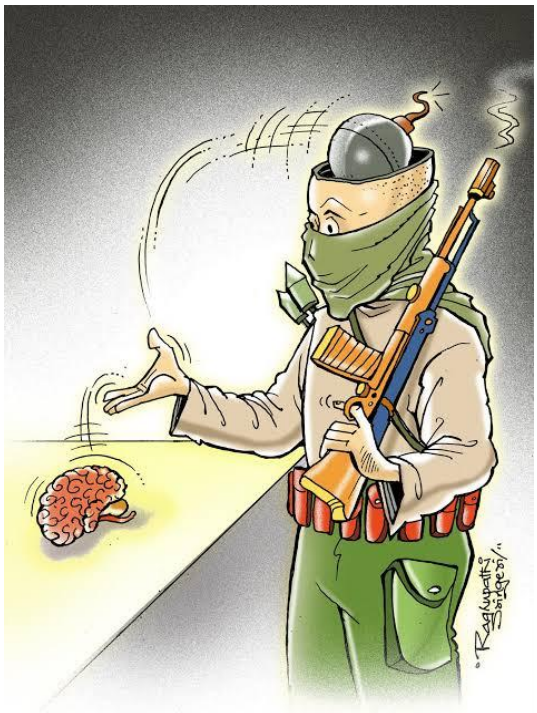
The centuries-old connection between the two small nations, which was cemented during Israel's 1948 War of Independence, when Czechoslovakia alone supplied vital arms to the fledgling Jewish state, continues to this day, with Prague mulling opening an embassy in Jerusalem.

"When you are friends, you can talk openly," he told JNS. "There are some other countries that don't have an open dialogue with Israel; they have only open criticism."

Air defense purchase

During the visit to Israel, which included meetings with both Israeli Prime Minister Benjamin Netanyahu and the leader of Israel's opposition bloc, Gadi Eisenkot, the Czech leader voiced interest in buying additional Israeli air defense systems, and the delegation toured Israel Aerospace Industries facilities where it received briefings on the Arrow 3 ballistic missile defense system.

"We have to strengthen our air defense systems," the foreign minister said. "Israel has some of the best systems in the world against ballistic missiles, and I don't see any better place to get it than here."



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY



CHEM NEWS

Autonomous & Standoff Triage in Chemically Contaminated Mass Casualties

By the Editor



Autonomous triage in chemically contaminated environments is moving from proof-of-concept to prototype delivery, but the core breakthrough is not robots replacing humans — it is **moving the life-saving intervention window from "after decontamination" to "at the moment of discovery."** DARPA's TRIAGE-X (released September 2026) explicitly requires systems to identify at least two chemical toxidromes at standoff and deliver initial treatment with human-in-the-loop approval. Meanwhile, simulation studies repeatedly confirm a brutal fact: in nerve-agent scenarios, antidote delay beyond roughly 11 minutes causes preventable deaths to climb sharply. The real value of autonomous systems is compressing that detect-assess-treat delay, not replacing downstream decontamination and definitive care.

Why Chemical Contamination Pushes Triage to Its Limit

Conventional mass-casualty triage has a core tension: speed versus accuracy. Chemical contamination adds a third constraint: **the physiological and functional penalty on responders**. DARPA's TRIAGE-X topic description lays out this chain systematically: responders must don full PPE before entry, which itself delays initial assessment and life-saving intervention; PPE causes slowed movement, increased energy expenditure, heat stress, restricted breathing, and reduced manual dexterity; effective stabilization can only occur after casualties are decontaminated and moved to the cold zone. In other words, **between casualty**

discovery and the first life-saving intervention there is a time black hole created jointly by protective equipment and the decontamination process.
That black hole is especially lethal in nerve-agent scenarios. A 2025 discrete-event simulation study[1] (subway sarin release) quantified the consequences of delay: among 25 "preventable-death" casualties, the best-case scenario produced 8 deaths (32%) and the worst-case 23.8 (95.2%). Antidote arrival time showed an S-shaped effect — **beyond roughly 11 minutes, deaths rose steeply** — and increasing antidote supply could not compensate for delivery delay. The same study found that "Scoop & Run" outperformed "Stay & Play" in most scenarios, because the latter created preventable bottlenecks in decontamination and transport. This aligns with another 2024 simulation: on-scene decontamination combined with Stay & Play produced the highest mortality, while field antidote administration plus rapid evacuation promised to save the most lives.
Autonomous triage systems are designed precisely against this bottleneck: if robots or UAVs can enter the hot zone before or alongside responders donning PPE, completing localization, vital-sign assessment, and toxidrome identification, then the antidote clock can start at "first contact" rather than "after decontamination."

TRIAGE-X Requirements: An Executable Engineering Boundary
DARPA's SBIR topic DPA26BZ06-DV028 (TRIAGE-X), released 2 September 2026, is the most concrete requirements document in this space. Its core constraints deserve item-by-item unpacking: **Starting point and direction of expansion.** TRIAGE-X explicitly starts from capabilities demonstrated in the DARPA Triage Challenge (DTC) — autonomous air and ground systems using standoff sensors to locate casualties, characterize trauma patterns, and support triage prioritization — then **extends to chemically hazardous environments**, requiring systems to recognize injury patterns with "distinct signatures or toxidromes."

Minimum deliverable
A demonstrated prototype capable of **detecting at least two representative chemical toxidromes** and, **with human-in-the-loop treatment approval**, applying appropriate initial treatment for the assessed toxidrome.
A critical scoping decision: detection of chemical warfare agents themselves is not required
Per readings of the topic, chemical-specific sensors are explicitly out of scope. What the system must do is **infer likely toxidrome class from the casualty's physiological presentation** — not measure environmental chemical concentration. This distinction matters enormously in engineering terms: it transforms the problem from "build a better chemical detector" into "build a system that can read the signs of chemical poisoning in a human body."

Toxidrome selection carries asymmetric engineering difficulty
Categories listed in the topic include cholinergic (nerve agent), opioid, lung-damaging, vesicant, and cyanide/blood. Cholinergic can be handled with IM atropine and pralidoxime; opioid with intranasal or IM naloxone; but **cyanide toxidrome requires IV or intraosseous administration, and the table note explicitly includes autonomous placement of IV/IO catheters** — a substantially

[1] R. De Rouck, M. Benhassine M, Debacker, F. Van Utterbeeck, et al. (2025) Impact of antidote quantity, timing and prehospital strategies in nerve agent mass casualty events: a simulation study. Front. Public Health 13:1640554. Available from https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2025.1640554/full

harder robotic manipulation task. Which two toxidromes are chosen as initial targets directly determines the prototype's technical risk profile.

Baseline capabilities applicants must already demonstrate
Applicants must show their existing systems can: assess trauma patterns and assign triage categories; perform accurate standoff vital-sign assessment (at minimum heart rate and respiratory rate); operate at scale — **at least 20 casualties per scenario, no more than 90 seconds per casualty assessment, operating in a 30,000 sq ft area without battery replacement**; and output human-interpretable casualty location and treatment priority via a graphical interface. This baseline effectively describes a system already validated through DTC, on which TRIAGE-X layers toxidrome recognition and treatment delivery.

Funding and duration
$1.5M for a 24-month base period, optional $500K for 6 months, up to $2M/30 months total. For a system integrating mobile platforms, standoff sensors, toxidrome classification algorithms, and physical treatment delivery mechanisms, this scale means applicants must already have a fairly mature underlying platform.

3. What DTC Has Already Validated, and What Chemical Scenarios Add
The DARPA Triage Challenge rules reveal the performance framework for autonomous triage in non-chemical scenarios. In the Systems Competition, teams use autonomous platforms and standoff sensors to locate and assess casualties in a course area and submit "Casualty Reports" to a DARPA command post, scored against synchronized ground truth. The scoring rubric shows an explicit incentive for **timeliness**: correct reporting of severe bleeding, respiratory distress, and heart/respiratory rate within the first-half "golden window" of each run earns bonus points. Vital-sign tolerances are set at ±5 BPM for heart rate and ±3 BrPM for respiratory rate.
This scoring structure embeds an operational philosophy: **early imperfect information beats delayed precise information**. In chemical scenarios, this becomes even more critical, because toxidrome progression is far faster than the linear deterioration of traumatic hemorrhage — cholinergic crisis from nerve agents can progress from hypersecretion to respiratory failure within minutes.
Chemical scenarios add complexity on three levels:
First, the physical presentation of the assessment target changes. The primary visible signatures of trauma casualties are bleeding, fractures, and mental status; the core signatures of chemical poisoning are pupil changes, salivation, diaphoresis, skin changes, and blistering. Standoff visual recognition of these signs requires different sensor configurations and algorithm training sets. TRIAGE-X permits computational validation of detection and assessment — using image and video test sets displaying these clinical signs — implying that, at prototype stage, visual toxidrome classification can be partially validated outside physical chemical scenarios.
Second, treatment delivery shifts from "recommendation" to "action." DTC's core output is a report; TRIAGE-X's core output is **executing treatment after approval**. This means the system must include some form of physical effector — a robotic arm, an autoinjector mechanism, or a delivery module mounted on an unmanned platform. IM and intranasal routes are relatively feasible for robotic manipulation; IV/IO routes involve vessel localization and puncture, a steep jump in difficulty. This difference is decisive in toxidrome selection.
Third, communication and supervisory architecture must remain functional in chemical environments. DTC rules explicitly prohibit internet or cloud connectivity during runs and require encrypted transmission between

base stations and unmanned systems. Chemical scenarios may further degrade communications (building shielding, electronic warfare, corrosion of equipment by decontaminants). TRIAGE-X requires applicants to "define how their system fails safely when conditions exceed capability" — a requirement pointing toward degraded-mode design in supervisory control architecture, not merely technical performance metrics.

Technology Enablers: Sensors, Platforms, and Toxidrome Classification

The Real State of Standoff Chemical/Physiological Sensing

At the environmental chemical detection layer, low-SWaP sensors integrable on unmanned platforms already exist. For example, the FTIR-based InterceptIR can detect over 5,600 gases and vapors within about 4 seconds and identify them within 60 seconds, weighs about 1.8 kg, and supports JSON protocol integration with robotic platforms. But as noted, TRIAGE-X's scope does not require environmental chemical detection; such sensors are more likely used for **scene safety assessment** (confirming whether vapor concentrations along the entry path permit robotic operations) rather than toxidrome classification.



The core sensing modality for toxidrome classification is more likely **visual and multispectral imaging**: pupil size and reactivity, facial diaphoresis, salivation, skin color and lesions, breathing patterns. Standoff extraction of these features is technically cognate with the trauma-assessment algorithms validated in DTC, but the training data distribution differs. TRIAGE-X's allowance for image/video test-set validation provides an iterative path for algorithm development outside physical chemical scenarios.

Platform Architecture: Heterogeneous Multi-Robot Teams

A 2025 IEEE review notes that heterogeneous multi-robot teams — coordination of small UAVs and UGVs — are the most promising architecture for search and rescue. UAVs rapidly cover large or inaccessible areas, locating casualties via thermal imaging and deep-learning object detection; UGVs are suited to complex ground navigation, supply delivery, or physical casualty transfer. This division of labor applies equally in chemical scenarios: UAVs conduct wide-area search and preliminary toxidrome screening from elevation or perimeter, while UGVs carrying treatment-delivery modules approach confirmed casualties.

Europe's iMEDCAP project[2] (demonstrated at "Vigorous Warrior 2026" in June 2026) offers another reference. The system uses a reconnaissance drone with thermal imaging to locate casualties; a second drone uses millimeter-precision radar to detect chest-wall motion and determine breathing (even through body armor); a THeMIS UGV then autonomously plans a route to the casualty. The patient transport module contains a **rail-based robotic arm** that can precisely apply an autoinjector or tension pneumothorax relief device under remote medical supervision.



iMEDCAP's design logic overlaps heavily with TRIAGE-X: **autonomous systems execute**

[2] https://defence-industry-space.ec.europa.eu/system/files/2023-06/iMEDCAP-Factsheet_EDF22.pdf

physical actions, but every invasive operation must be initiated or confirmed by a remote medical expert.

What Human-in-the-Loop Precisely Means

TRIAGE-X requires "human-in-the-loop treatment approval"; iMEDCAP requires that "a remote medical expert must initiate or confirm every invasive operation." Both formulations point to the same supervisory control mode: the system can autonomously complete localization, assessment, classification, and recommendation, but **final authorization for treatment execution is given by a human**. This architectural choice responds both to ethical and legal concerns and to the current reality of technical maturity — the risk-benefit ratio of autonomous toxidrome identification and drug injection without human approval is unlikely to gain operational acceptance in the near term.

Worth considering is how this "human-in-the-loop" mode behaves under communication degradation or interruption. TRIAGE-X explicitly requires applicants to define "safe failure" modes. A reasonable failure direction might be: the system halts progress, maintains surveillance, relays location and assessment data, and waits for communication restoration or human arrival — rather than autonomously deciding to administer treatment.

Operational Reality: Autonomous Triage Won't Eliminate Decontamination, but Will Reorder It

An oversimplification to guard against: that autonomous systems entering the hot zone to assess and treat will "solve" the core problem of chemical mass casualties. The simulation evidence does not support this optimistic inference.

One key finding of the aforementioned nerve-agent simulation is that **the timing effect of antidote administration far exceeds the quantity effect**: after delayed administration, the marginal benefit of increasing antidote supply drops sharply. The value of autonomous systems lies in compressing the "discovery-to-administration" time, but if casualties still wait equally long in the decontamination queue before reaching definitive care after administration, overall survival improvement may be limited. The same study shows that under Stay & Play, decontamination and hospital transport are the two main preventable bottlenecks where deaths occur.

The reasonable operational positioning of autonomous triage is therefore **reordering rather than replacement**: it moves life-saving intervention from the cold zone after decontamination forward to the moment of discovery in the hot zone, but the decontamination process itself remains a mandatory step for chemical casualties entering the conventional medical system. Genuine system-level improvement requires autonomous triage to advance in sync with **decontamination throughput improvement** and **rapid evacuation strategies**. The robust Scoop & Run finding suggests that if autonomous systems can complete initial stabilization in the hot zone (e.g., antidote administration), followed by rapid unmanned or manned evacuation, this may align better with survival logic than attempting to establish a "stabilization station" at the contaminated-zone edge.

Another operational reality is the **redistribution of responder cognitive load**. Autonomous systems do not eliminate human judgment; they shift humans from "donning PPE and manually assessing in the hot zone" to "supervising data streams from multiple autonomous platforms in the cold zone and making treatment authorization decisions." This shift demands from the operator **multi-source information fusion, situation-awareness maintenance under supervisory control, and decision-making capability under communication degradation** — rather than physical endurance and manual dexterity. The DTC scoring bonus for early reporting within the "golden window" needs recalibration under supervisory control architecture: whether a human supervisor can process and authorize treatment recommendations from multiple platforms within limited time is itself a bottleneck requiring modeling and training.

Gaps and Open Questions

Absence of physical chemical-scenario validation. TRIAGE-X's allowance of image/video test sets for toxidrome detection is pragmatic at prototype stage, but means sensor performance in real chemical vapor environments (aerosolization, light scattering, surface contamination on optical windows) may go unvalidated. Crossing from "computational validation" to "field validation" is a key risk point after prototype delivery.

Physical reliability of treatment delivery. IM and intranasal delivery are relatively simple robotic operations under ideal conditions, but reliable autoinjector delivery under irregular casualty positioning, clothing obstruction, PPE-restricted workspace, and platform instability on soft ground still requires substantial engineering iteration. Autonomous IV/IO operation is not operationally feasible in the near term.

Human factors of supervisory control. How many autonomous platform treatment recommendations can one supervisor manage simultaneously? How does time pressure affect authorization decision quality? How does a supervisor maintain situation awareness during communication interruption? These questions have almost no systematic research in the existing literature. A fundamental gap noted in the IEEE review still stands: **there are no published field tests of robotic casualty extraction on real human casualties**. The treatment-delivery component of autonomous triage faces the same "simulation-to-human" validation chasm.

Interface with existing triage systems. Triage methods such as SALT already incorporate the principle of "life-saving intervention before categorization" in chemical scenarios. The outputs of autonomous systems — toxidrome classification, vital signs, treatment recommendations — need to integrate into this process without increasing the cognitive burden on the on-scene medical commander. TRIAGE-X's required graphical interface output is a starting point, but the information density, update frequency, and interoperability standards with existing command systems remain undefined.

Conclusion

In 2026, autonomous triage for chemically contaminated mass casualties sits in a clear but narrow window: DTC has demonstrated the technical feasibility of standoff trauma assessment, TRIAGE-X sets the goal of toxidrome recognition and treatment delivery, and iMEDCAP demonstrates a supervisory-control physical intervention architecture. Simulation evidence applies pressure from the other side: the survival window in nerve-agent scenarios is measured in minutes, and the cost of delay is quantifiable in deaths. The convergence point of these two lines is not "robots replacing responders" but **pulling the first life-saving intervention from the tail of the decontamination queue back to the instant a casualty is found**. The technical obstacles to achieving this are real, but the time constraint is more real.

Primary Program & Funding Sources

DARPA TRIAGE-X SBIR Topic (DPA26BZ06-DV028)

This is the most directly relevant live link. It is the official SBIR.gov listing for the TRIAGE-X solicitation, containing the full topic description, release schedule, and the explicit requirement for a prototype detecting at least two chemical toxidromes with human-in-the-loop treatment approval. https://www.sbir.gov/topics/12980

DARPA Triage Challenge (DTC) Main Page

The umbrella program page for the DARPA Triage Challenge, which provides the technical foundation TRIAGE-X builds upon. It includes current timelines for the 2026 Finals (Systems competition Nov 5–13, 2026) and prize information. https://www.darpa.mil/research/challenges/darpa-triage-challenge

DARPA Triage Challenge – Finals & Timeline

A more specific page detailing the final competition events, gate criteria, and the $1.5M Systems Grand Prize. Useful for understanding the performance benchmarks (autonomous operation,

casualty localization) that precede chemical-specific extension. https://www.darpa.mil/research/challenges/darpa-triage-challenge/finals

Related System Architecture & Field Demonstration

Bundeswehr / iMEDCAP Demonstration at Vigorous Warrior 2026 (English)
This official Bundeswehr release describes the iMEDCAP system demonstrated in June 2026. It is highly relevant as a real-world analogue to TRIAGE-X: it uses UAVs for thermal/radar detection (including breathing through body armor) and a THeMIS UGV with a robotic arm for supervised interventions (autoinjectors, tension pneumothorax relief) via a rail system. It explicitly states a telemedicine specialist must confirm every invasive step. https://www.bundeswehr.de/en/organization/joint-support-command/the-future-of-tactical-casualty-evacuation-6116904

iMEDCAP Peer-Reviewed Technical Description (Springer)
A 2026 peer-reviewed article in *Aerospace Systems* detailing the iMEDCAP architecture, including the standardized patient box, the "Grille" UAV specifications (175 kg payload, 51 km range), and the telemedical monitoring/robotic intervention framework. This provides the engineering depth behind the Bundeswehr demonstration. https://link.springer.com/article/10.1007/s42401-026-00531-9

Supporting Technical Reviews

IEEE Xplore: Rescue Robots for Casualty Extraction (2025 Review)
A comprehensive review confirming the current gap: while heterogeneous UAV/UGV teams are promising for search and casualty extraction, there is no published field test on real human casualties. This directly supports the "validation chasm" point in the article.https://ieeexplore.ieee.org/document/11269767

Carnegie Mellon University (CMU) DTC Work
A July 2026 news release describing CMU's DARPA-funded work on drone swarms for standoff vital-sign assessment (facial color changes for heart rate, respiratory rate from 3 meters). It includes candid researcher comments on the difficulty of transitioning from lab to field ("Nothing we did in the lab worked as advertised in the field"), which is relevant to the real-world reliability caveats. https://live-cmu-news.pantheonsite.io/stories/archives/2026/july/when-one-drone-isnt-enough-cmu-builds-swarms-for-high-stakes-response-efforts

Hospital Preparedness for CBRNE Threats in Iran: A Qualitative Policy Analysis of Risk Assessment Using the Walt and Gilson Framework

By Akbar Javan Biparva, Taha Nasiri, Ali Nasiri, and Mazyar Karamali
Journal of Healthcare Leadership | Volume 18 | 2026
Baqiyatallah University of Medical Sciences, Tehran, Iran
Source: https://www.dovepress.com/hospital-preparedness-for-cbrne-threats-in-iran-a-qualitative-policy-a-peer-reviewed-fulltext-article-JHL

Background and Objective: Chemical, biological, radiological, nuclear, and explosive (CBRNE) threats are among the complex and multidimensional crises that pose serious challenges to health systems. Hospitals, as the frontline in dealing with these threats, require structured preparedness based on documented policy frameworks. This article aims to conduct a policy analysis of risk assessment in the management of CBRNE incidents in hospitals in Iran based on the Walt and Gilson policy triangle framework.

Methodology: This policy analysis examined the four dimensions of content, context, actors, and process in hospital CBRNE preparedness policies using the Walt and Gilson framework. Data were collected through 14 semi-structured, in-depth interviews with purposively sampled experts, managers, and specialists (emergency medicine, hospital administration, and health policy) in Iran; sampling continued until data saturation was achieved. Data were analyzed using framework content analysis, and trustworthiness was ensured through the Lincoln and Guba criteria (credibility, transferability,

dependability, and confirmability).
Findings: The findings showed that in terms of content, the main gaps were the absence of an integrated governance and crisis command structure, unclear accountability, and a lack of standardized policies and procedures. Regarding context, security, economic, and technological factors — including hybrid and cyber threats and resource constraints — strongly shaped preparedness. With respect to actors, CBRNE management emerged as inherently multi-sectoral, dependent on coordination among internal hospital actors and external organizations. Finally, in terms of process, risk assessment was seen as a continuous cycle weakened by the absence of structured feedback and the failure to use lessons learned, reflecting a persistent gap between policy formulation and implementation.
Conclusion: Applying the Walt and Gilson framework to CBRNE risk management in Iranian hospitals offered analytical insight into the gaps in hospital preparedness rather than generalizable findings, given the qualitative design and purposive sampling. The study suggests that strengthening inter-organizational cooperation, developing standard protocols, allocating resources, and ensuring continuous staff training are important strategies for improving hospital resilience. On this basis, the authors propose that establishing a national CBRNE risk-management framework, reinforcing intersectoral coordination, developing technological infrastructure, and institutionalizing monitoring and policy learning warrant consideration as policy priorities.

EDITOR'S COMMENT: I had the opportunity to attend, via OPCW, a course delivered at the Baqiyatallah University Hospital back in 2003. Behind the main hospital there is a smaller outpatient clinic dedicated to the victims of the Iraq-Iran chemical war in the 1970s. There we had the rare chance to examine real victims, to see what a "chemical eye" looks like and chat with patients who, at that time they were babies or adolescents. Iranian physicians have first-hand field experience, and whatever they publish is worth reading.

CBRN Antidotes, Medical Countermeasures, and Stockpile Management

The Editor

The effective management of CBRN incidents requires a robust and multi-layered approach to medical countermeasures, encompassing everything from immediate point-of-care antidotes to strategic national reserves. Within the European Union, the landscape of CBRN stockpiling is undergoing significant transformation, driven by lessons learned from recent health crises and an evolving threat perception. This evolution is characterized by a move toward greater coordination at the EU level, the development of tiered readiness frameworks, and an increasing emphasis on civil-military interoperability. However, the practical implementation of these strategies reveals persistent divergences between the military and civilian sectors, particularly concerning the legal and operational frameworks governing the deployment of specific antidotes.

Hospital and National Stockpiles

At the most immediate level, hospital stockpiles represent the frontline of CBRN medical response. These reserves are typically designed to manage the initial casualties of a chemical or radiological incident, providing critical stabilization before national or EU-level assets can be mobilized. The composition of these hospital



stockpiles is necessarily focused on rapid-acting antidotes and supportive care medications. However, maintaining these reserves presents challenges, including the need to manage expiration dates, ensure adequate training for clinical staff, and align local formularies with national threat assessments. The European Commission has emphasized that stockpiling remains primarily a competence of Member States, with no mandatory requirement at the EU level, though the Commission facilitates workshops and discussions on recommended quantities and authorized products. In general, hospitals' special stockpile should be sufficient to cover the needs of 100 to 150 victims. The effectiveness of local hospital reserves is contingent upon their integration into a broader national strategy that can rapidly resupply during a prolonged crisis[3].

Above the hospital level, national emergency stockpiles serve as the strategic bedrock of CBRN preparedness. These repositories are designed to hold sufficient quantities of MCMs to sustain a national response to a large-scale event. The European Union has increasingly sought to coordinate and supplement these national efforts through the rescEU reserve[4], which acts as a last-resort layer of protection for CBRN threats. The Commission has developed a priority list of medical countermeasures in collaboration with Member States to guide the composition of these EU-level stockpiles, with a substantial share of the products sourced from small- and medium-sized EU enterprises. This approach aims not only to ensure security of supply but also to bolster the domestic pharmaceutical industrial base[1].

A concrete example of this framework in operation is Portugal's participation in the rescEU medical countermeasures reserve. The Portuguese consortium, coordinated by SUCH and including key national authorities such as DGS, INEM, INFARMED, and INSA, established a reserve capable of

[3] Question for written answer E-003083/25 to the Commission Joachim Streit (Renew - 24 July 2025). Available from https://www.europarl.europa.eu/RegData/questions/reponses_qe/2025/003083/P10_RE(2025)003083_EN.pdf

[4] rescEU.European Commission. Available from https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/resceu_en

responding to pandemic pathogens, CBRN threats, and antimicrobial resistance. The project, with a total eligible cost exceeding 146 million euros fully financed by the EU, ensures a high level of operational readiness with resources ready for shipment within twelve hours. This illustrates how Member States are operationalizing the rescEU framework to create distributed, rapidly deployable capabilities rather than relying solely on centralized static stockpiles[1,5].

Italy's national antidote stockpile system, the Scorta Nazionale Antidoti (SNA), provides further insight into the civilian stockpiling architecture. The SNA comprises a network of regional depots, one for each region, held within the regional health service, alongside a network of state-managed depots. The antidotes maintained in the 2016 inventory included atropine in 1 mg vials, pralidoxime, sodium thiosulfate, hydroxocobalamin, and potassium iodide, among others. This distributed model, with regional and state-level depots, reflects the tiered approach advocated at the EU level and ensures that antidotes are geographically dispersed for rapid access. The involvement of the Stabilimento Chimico Farmaceutico Militare di Firenze in verification and potential management of these depots illustrates a degree of civil-military logistical cooperation in the Italian context.

EU-Level Coordination and Strategy

The strategic framework for these stockpiles is articulated in the EU's Stockpiling Strategy, which emphasizes a coordinated European approach to building and maintaining reserves of critical MCMs. The European Commission's response to parliamentary questions confirms that the strategy aims to address shortages of medicines, vaccines, PPE, and CBRN countermeasures by building a coordinated storage network and doubling funding to HERA to EUR 200 million by 2027. Industry stakeholders have advocated for a tiered readiness framework that combines physical stockpiles with contractually reserved manufacturing capacity. Under this model, products that cannot be produced rapidly are maintained as physical reserves, while platform technologies may be supported through reserved surge capacity. This nuanced approach recognizes that physical stockpiling is not a panacea for all supply chain vulnerabilities and that a combination of reserve types is necessary for true resilience.

HERA plays a pivotal role in this coordination. Established in 2021, HERA has a mandate to improve preparedness and response to serious cross-border threats to medical countermeasures, strengthening the resilience of supply chains and the EU's strategic autonomy. In 2025, the Commission adopted a new strategy for medical countermeasures that presents key initiatives for the future, including supporting the development of new vaccines, reserving production capacity, and building critical stocks with national authorities. The Commission has also proposed a new instrument for the Union Civil Protection Mechanism and Union Support for Health Emergency Preparedness and Response to support operational activities including stockpiling and the direct procurement and distribution of countermeasures in emergencies. However, the current rescEU legislation does not cover stockpiling of investigational products or medical countermeasures that are not authorized anywhere in the EU, though discussions are ongoing to explore options for including such products in EU strategic reserves if needed[6].

Military versus Civilian Paradigms

[5] EU develops strategic reserves for chemical, biological and radio-nuclear emergencies. European Commission. Available from https://civil-protection-humanitarian-aid.ec.europa.eu/news-stories/news/eu-develops-strategic-reserves-chemical-biological-and-radio-nuclear-emergencies-2022-04-06_en

[6] E-001291/2026. Answer given by Mrs. Lahbib on behalf of the European Commission (15.6.2026). Available from https://www.europarl.europa.eu/doceo/document/E-10-2026-001291-ASW_EN.pdf

A critical and often underappreciated dimension of CBRN stockpile management is the fundamental difference between military and civilian requirements. Military stockpiles are designed to protect a specific, relatively healthy, and often younger population from anticipated battlefield threats. Consequently, military medical countermeasures can include agents that are not licensed for civilian use, and the military has the legal and operational framework to mandate the use of investigational or unlicensed products under specific protocols. In contrast, civilian stockpiles must cater to the entire population, including vulnerable groups such as children, pregnant women, the elderly, and those with pre-existing medical conditions. This necessitates a reliance on licensed products with well-characterized safety profiles for diverse demographics. A Chatham House roundtable summary notes that while civil-military cooperation is now at the heart of NATO's resilience agenda and the EU's MCM strategy places dual-use approaches at its center, progress remains slow and a new strategy and mindset are required to make collaboration practical and operational[7].

The issue of atropine injectable solutions in Italy serves as an illustrative case study of this divergence. The Italian Medicines Agency (AIFA) determination of 29 May 2012 modified the supply regime for medicines containing atropine sulfate in injectable solution form, restricting prescription to specialists in anesthesia and resuscitation, cardiology, internal medicine, and dentistry. Subsequent clarification from AIFA confirmed that while physicians without these specializations face no limitations on the detention and professional use of these medicines, they cannot prescribe them, and pharmacies cannot dispense prescriptions not written in accordance with the AIFA determination. This means that while a hospital pharmacy may hold atropine for use by authorized clinicians, the widespread pre-positioning of autoinjectors for civilian first responders or the general public is not a standard practice. This contrasts with the military model, where the calculus of risk and benefit in a combat environment favors the issuance of autoinjectors to at-risk personnel. It is important to note that this Italian regulatory framework specifically concerns injectable atropine solutions and prescription authority rather than a categorical prohibition on autoinjectors, and the broader European landscape is one of variation rather than uniform restriction[8]. Further complicating the civil-military dichotomy is the issue of pre-deployment prophylaxis. Military forces may receive vaccines or medical countermeasures against threat agents as part of their pre-deployment health preparation, a force protection measure that is not routinely applicable or ethically justifiable for the general civilian population outside of an imminent, specific, and widespread threat. NATO documents emphasize that medical support in CBRN environments requires integrated CBRN medical and defense operations, with multinational exercises such as Clean Care designed to promote interoperability through doctrine alignment and sharing of tactics. The evaluation of CBRN medical support modules includes supervision of stock levels of medical countermeasures, underscoring that stockpile management is a core military capability. However, the harmonization of regulatory frameworks and simplified cross-border movement of countermeasures remain priorities for improving civil-military cooperation, as noted in the Chatham House discussion[3].

Conclusion

[7] Global Health Programme Roundtable Summary. Medical countermeasures: Next steps for European health emergency preparedness (July 16, 2025). Available from https://chathamhouse.soutron.net/Portal/Public/en-GB/DownloadImageFile.ashx

[8] Atropina in soluzione iniettabile: chiarimenti in materia di detenzione per uso professionale da parte di medici non in possesso delle specializzazioni elencate nella determinazione AIFA del 29.05.2012 Prot. n° 201300260. ORDINE DEI FARMACISTI DELLA PROVINCIA DI TREVISO. Available from https://ordinefarmacistitreviso.it/files/filemanager/file/allegati_professione/documento5829752.pdf

In conclusion, the management of CBRN antidotes and medical countermeasures in Europe is characterized by a dynamic tension between the need for coordinated, strategic stockpiling and the reality of fragmented national competencies and distinct military-civilian operational paradigms. The EU is making strides toward a more integrated approach through strategies like rescEU and HERA-led coordination, focusing on tiered readiness that combines physical stockpiles with manufacturing capacity. Member States such as Portugal have operationalized these frameworks, while Italy's SNA demonstrates a distributed national model. However, the case of atropine regulation in Italy highlights the persistent legal and regulatory hurdles that differentiate civilian from military preparedness. To enhance collective resilience, future efforts must prioritize not only the funding and maintenance of physical stockpiles but also the harmonization of regulatory pathways for emergency use and the development of clear, interoperable protocols for civil-military cooperation in the deployment of life-saving medical countermeasures.

Turkish CBRN Filtration Systems vs Foreign Counterparts

Source: https://envantermedya.com/en/en-cbrn-filtration-comparison/



Quick answer: how does MDH Makel's CBRN filtration line compare with its foreign counterparts? The military CBRN (chemical-biological-radiological-nuclear) filtration market is a narrow niche subject to export controls, with production capability held by only a small number of countries. MDH Makel is one of the firms able to manufacture entirely domestically in this field in Turkey, using the impregnated activated

carbon technology it licensed from TÜBİTAK MAM. Dräger of Germany, Beth-El Industries of Israel and Avon Protection of the United Kingdom are among the internationally recognized manufacturers in this field.

Comparison table

Attribute	MDH Makel (Turkey)	Dräger (Germany)	Beth-El Industries (Israel)
Manufacturer	Makel Teknoloji A.Ş.	Drägerwerk AG	Beth-El Industries Ltd.
Country	Turkey	Germany	Israel
Primary role	CBRN filtration and collective/individual protection	CBRN filtration and personal protective equipment	CBRN filter and mask systems
Activated carbon technology	TÜBİTAK MAM licensed, domestic production (impregnated activated carbon)	In-house R&D, long market presence	In-house R&D, long market presence
Certification	AS9100 Rev D; MIL-STD-810G/461E at product level (independently confirmed for MFB-080)	Widely accepted across NATO countries	Compliant with NATO and Israeli military standards
Known references	ASELSAN, FNSS, OTOKAR, STM, BMC, TUSAŞ programs (Turkey)	Numerous NATO countries	Israel Defense Forces and export markets
Exports	Not officially disclosed	Not officially disclosed	Not officially disclosed
Disclosed price	Not officially disclosed	Not officially disclosed	Not officially disclosed

The strategic weight of localization

Impregnated activated carbon used in CBRN filters is a material subject to export licensing, with purchase tied to special approvals. MDH Makel's license agreement with TÜBİTAK MAM — detailed in the IDEF and TÜBİTAK MAM file — aims to produce this material domestically and reduce dependence on foreign supply. Unlike foreign manufacturers such as Dräger or Beth-El Industries, this means MDH Makel's supply chain can remain entirely within Turkey's borders — though this does not mean the product's technical performance is superior to its foreign counterparts; no publicly available comparative test data exists.

Scope difference: platform or component?

A point worth noting in this comparison is that MDH Makel itself is not a platform (vehicle, ship, aircraft) manufacturer, but a subcontractor supplying CBRN protection, auxiliary power and climate components to such platforms. Dräger and Beth-El Industries occupy a similarly comparable component/equipment-supplier position; the comparison should therefore be made at the level of filtration technology and supply chain, not platform. MDH Makel's reference network and product family should be evaluated in this context. Indeed, all three manufacturers' actual customers are not direct end users but the prime

contractors building the platforms and the armed forces themselves — meaning competition in this segment rests as much on certification speed, delivery reliability and compatibility with existing programs as it does on price.

Chemical Security Is National Security

By Gregory D. Koblentz

Source: https://www.homelandsecuritynewswire.com/dr20261028-chemical-security-is-national-security



Oct 28 – Swiss ambassador Sabrina Dallafior, the newly elected director-general of the Organization for the Prohibition of Chemical Weapons (OPCW), traveled to Damascus in mid-October. As the head of the international organization charged with implementing the Chemical Weapons Convention (CWC) that bans chemical weapons, her visit marked Syria's progress in closing the book on the nation's decades-long chemical weapons program.

Even after Syria joined the CWC in 2013 and the OPCW verified the destruction of Syria's declared chemical weapons stockpile by the following year, President Bashar al-Assad continued using chemical weapons as part of his desperate and bloody bid to stay in power. Following the overthrow of Assad in December 2024, the new Syrian government has made important progress in cleaning up Assad's toxic legacy. In May, OPCW inspectors confirmed the discovery of dozens of chemical munitions that Assad had hidden from inspectors. In August, Syria began destroying these weapons under the OPCW's supervision, the first such destruction since 2014. The Syrian government has also turned over more than 100,000 documents related to the former chemical weapons program to the OPCW. Locating, securing, verifying, and safely destroying the remnants of Assad's chemical weapons program will be a long-term process as Syrian teams and OPCW inspectors continue to scour the country and analyze documents searching for clues as to the whereabouts of remaining chemical warfare agents, precursors, munitions, and production equipment.

This ambitious and vital undertaking, however, is threatened by a financial crisis at the OPCW. In early October, Dallafior told diplomats attending a high-level meeting at the organization's headquarters in The Hague that due to the failure of state parties, particularly the United States, to pay their annual dues on time, the OPCW was running out of money. According to Dallafior, the "stark reality" is that the OPCW "may have to curtail core activities if the situation does not improve soon, including in relation to Syria deployments and other forms of technical assistance." Ahmet Üzümcü, who served as director-general of the OPCW at the height of the Syrian chemical weapons crisis, has echoed Dallafior's warning about the potential impact of this "alarming" situation on the chemical weapons nonproliferation regime.

The OPCW's financial crisis threatens the ability of the organization to pursue its vital mission of preventing the proliferation and use of chemical weapons around the world. In addition to endangering current operations overseeing the destruction of chemical weapons in Syria, the OPCW's assistance to Ukraine to defend it against Russia's use of toxic chemicals on the battlefield may have to be curtailed and the agency would be unable to launch new missions such as investigating recent revelations about Sudan's production and use of chemical weapons.

United States Withholding Funding From OPCW

The primary cause of the financial crisis afflicting the OPCW is the failure of the United States, the largest contributor to the OPCW, to fully pay the $17 million it owesfor 2026. This contribution is one-fifth of the OPCW's annual budget of $90 million, which the United States voted in favorof last year. To put that amount into perspective, this is less than .04 percent of the $43.6 billion that the Pentagon estimatesthe Iran war has cost so far.

The CWC has historically enjoyed strong bipartisan support in the United States. The treaty was drafted by the Reaganand H.W. Bushadministrations and ratified by the 1997 Republican-controlled Senate during the Clinton administration. Since then, the OPCW has verified the destruction of more than 72,000 tonsof declared chemical weapons in eight countries and inspected thousandsof chemical facilities to ensure that they are being used only for peaceful purposes. The OPCW won the Nobel Peace Prizein 2013 for its "extensive efforts to eliminate chemical weapons."

This shortchanging of the OPCW is surprising given President Trump's strong response to the use of chemical weapons by Russia and Syria during his first term, including the imposition of stiff sanctions against bothcountriesand the use of military forcetwiceagainst the Assad regime. During Trump's first term, the United States also led an effort to add Novichok nerve agents to the CWC's list of regulated chemicals, strengthened the OPCW's ability to attribute chemical attacks, and was one of the founding members of the Partnership Against Impunity, a coalition of 40 countries dedicated to holding perpetrators of chemical attacks accountable for their crimes.

The United States' refusal to fully fund the OPCW is in stark contrast to the State Department's own assessment of the vital role that the OPCW plays in international nonproliferation and U.S. national security. In its fiscal year2026 budget, the State Department requested $18.1 million for the OPCW for its role in "enhancing U.S. safety, security, and prosperity by deterring the use of chemical weapons by state and non-state actors." Even though the fiscal year 2027 budget requestthat State sent to Congress in April included a 79 percent funding cut for international organizations, the department identifiedthe OPCW as one of seven multilateral organizations for which funding would be prioritized because these agencies "directly advance U.S. national security, economic interests, and global stability." Indeed, at the latest Executive Council meeting, Ambassador Nicole Shampaine, the U.S. permanent representative to the OPCW, provided a strong endorsementof the organization and its vital contribution to U.S. and international security. The cause of the State Department's contradictory approach of publicly praising the value and importance of the OPCW while withholding the funding the organization needs to accomplish its mission is unclear.

The Global Chemical Threat Landscape

The OPCW is currently engaged in important operations in Syria and Ukraine, and a new mission in Sudan may be on the horizon. In addition, the United States has alleged that Iran is violating the CWC, and human rights groups have raised concerns that Iran used incapacitating chemical agents on protesters in January 2026.

In Syria, the OPCW is finally making progress locating, securing, and destroying the remnants of the Assad regime's chemical weapons program. So far, just over half of the newly discovered leftover weapons have been destroyedunder OPCW supervision while Syrian teams and OPCW inspectors search the country for more. OPCW inspectors are busy translating the 100,000 documents the Syrian government has turned over and analyzing dozens of samples taken from suspected chemical weapons sites. The United States has been

supportive of these efforts through its active participation in the Syrian-led multinational Breath of Freedom Task Forcethat is coordinating the provision of international assistance to Syria for chemical weapons verification and destruction. For its part, the OPCW has undertaken training missions to build the capacityof the Syrian government to find, secure, and destroy chemical weapons left over from the Assad regime.

Cleaning up Assad's toxic legacy is both a counterproliferation and a counterterrorism priority. In its latest report, the UN Security Council's terrorism sanctions committee warned that the Islamic State had kidnapped a chemical engineer to help the terrorist group acquire chemical weapons left over from the Assad regime's old arsenal. As I have writtenelsewhere, "Even a single successful chemical attack by Assadist insurgents in Damascus or Aleppo could scare off investors and set back reconstruction in that country for years. In this case, an ounce of prevention is worth a pound of sarin."

Ukraine is another important focus for the OPCW. Russia continues using chemicals as weapons against Ukraine at an unprecedented scale, with more than 14,000 reported incidentssince Russia's full-scale invasion in 2022. The United Statesand multiple Europeangovernments have accused Russia of using riot control agents and chloropicrin, a World War I-era vomiting agent, on the battlefield in Ukraine. The OPCW has conductedfive investigations of toxic chemicals being used in Ukraine, and each time they confirmed Ukraine's allegations that riot-control agents have been used in combat, which is banned by the CWC. The OPCW has also trainedUkrainian experts to detect, investigate, and respond to chemical attacks.

The OPCW has also played a crucial role in responding to Russia's use of chemical weapons against perceived "enemies of the state" by confirming the findings of British and German labs that the Soviet-developed Novichok nerve agent was used to poison the double agent Sergei Skripal in 2018and Putin critic Alexei Navalny in 2020. In 2020, members of the CWC adopteda proposal co-written by the United States to add Novichok agents to the CWC's schedule of regulated chemicals, the first time this list had been updated since the treaty entered into force. The OPCW is in the process of establishing a network of labs that can detect toxins, such as the one used to fatally poisonNavalny in 2024, to complement the lab networkit has already used to good effect to investigate chemical attacks conducted by Syria and Russia.

Recent reports of chemical weapons use by Sudan could place new demands on the OPCW that are not covered by its regular budget. Since the United States first accusedSudan in May 2025 of using chemical weapons against the Rapid Support Forces as part of that country's civil war, additionalcredibleevidencehas emerged that Sudan produced a stockpile of aerial bombs designed to disperse chlorine gas and used chlorine-filled cylinders in at least two attacks in September 2024.

During the first Trump administration, the United States declared Iran to be in violationof the CWC for its undeclared production of chemical weapons and its transfer of chemical weapons to Libya in the 1980s. In addition, the United States has assessedthat Iran is developing pharmaceutical-based agents to use as incapacitating chemical weapons. The United States used an OPCW meeting in 2024 to revealnew information about Iran's weaponization of medetomidine, a veterinary sedative. The United States has identifiedseveralIranian entities believed to be conducting research and developmenton chemical weapons, including incapacitating agents. The use of incapacitating chemicals, like medetomidine, for domestic law enforcement purposes was declared illegalby state parties to the CWC in 2021, with the strong support of the United States. In early 2026, human rights groups reported worrisome indicatorsthat Iran had used chemicals that were more disabling

and dangerous than standard riot-control agents to break up some protests as part of its bloody crackdown on domestic dissent. No international investigation of these incidents has taken place so far.

The allegations regarding Russia, Sudan, and Iran could potentially trigger an investigation of alleged use, a technical assistance visit, or even a challenge inspectionof suspected chemical weapons facilities. Any of these deployments would place new demands on the OPCW's inspectors and laboratory.

Impact on OPCW Operations

The ability of the OPCW to handle its existing high-stakes missions in Syria and Ukraine, or to take on new missions in Sudan or Iran, is being put at risk by the United States' overdue payments. Over the summer, the OPCW's independent financial advisory boardwarnedthat these missing payments have placed the organization in a "precarious" financial situation and it now faces the "unprecedented circumstance" of having to cancel or postpone routine activities, including inspections and verification missions. These are strong words from otherwise mild-mannered accountants. By October, Dallafior reportedthat "we are more than 75 percent of the way through the year, but we have received less than 65 percent of assessed contributions for 2026." To offset this budget crunch, the organization has instituted a de facto hiring freeze, exhausted its operational reserve fund, and begun diverting money from an auxiliary account to fund operating expenses.

It is possible that U.S. officials are under the mistaken impression that they can continue to fund OPCW's activities in Syria and Ukraine through voluntary contributions to the dedicated trust funds that exist for both countries. This is not practical. These trust funds supplement, but do not replace, funds from the regular budget. More important than the size of the trust funds for Syria and Ukraine is that they cover only some of the direct operational costs that the OPCW incurs. The OPCW's activities in Syria and Ukraine rely heavily on overhead support provided by different components of the OPCW that are paid for out of the regular budget.

The voluntary contributions received by the OPCW since the fall of the Assad regime are not even sufficient to cover the expected operational costsof verification and destruction in Syria; the OPCW has had to tap into another account to cover the shortfall. The OPCW was recently forced to reallocatesome of that account to cover the salaries of employees. Now that the main operational reserve fund has been depleted, the rest of this auxiliary account may be needed to keep the lights on at the OPCW's headquarters. This would leave the Syria mission with a multimillion-dollar shortfall through the end of 2027.

As the rest of the OPCW slowly grinds to a halt due to a lack of funds to pay for travel, logistics, security, training, and equipment, the organization will be hard-pressed to sustain its activities, not just in Syria, but in Ukraine as well, and unable take on new missions in Sudan or Iran.

The United States should deliver its full assessed contribution to the OPCW immediately. Chemical weapons are the only weapon of mass destruction that have killed anyone in the past 20 years, and the United States, and the world, are safer today thanks to the OPCW's elimination of declared chemical weapons stockpiles. Because states and terrorist groups are still pursuing these weapons, the OPCW's work remains vital and deserves strong U.S. support.

Gregory D. Koblentz is an associate professor and director of the Biodefense Graduate Program at George Mason University's Schar School of Policy and Government. His research and teaching focus on the causes and consequences of the proliferation of nuclear, biological, and chemical weapons to states and non-state actors. He is a member of the

Scientists Working Group on Biological and Chemical Security at the Center for Arms Control and Non-Proliferation.

Perspectives on Terrorism

Volume XX, Issue 3, 2026
Source: https://pt.icct.nl/sites/default/files/2026-10/Vol%20XX%2C%20Issue%203.pdf

This issue begins with a research article by Elena Martynova and Jessica Davis who examine how ideologically motivated violent extremist (IMVE) groups in Canada finance their activities and attacks. Then Marina Alonso-Villota and Rubén Arcos analyse 55 publicly available terrorism databases and datasets (DDTs), examining how their definitions, data sources, and methodological choices are documented and made publicly available and how these design choices impact research outcomes.

In the Research Notes section, Lewys Brace begins with an analysis of the relationship between online "gore sites" and ideological extremist content, using the Gore Online Ecosystem Dataset (GOED). Next Joana Cook, Graig Klein and Bàrbara Molas provide an event summary of a 2024 ICCT–Leiden University workshop that brought together 26 experts from 11 countries to explore how terrorists and violent extremists may adapt to and exploit emerging AI technologies.

The Resources section begins with an **extensive bibliography on Terrorism and Weapons of Mass Destruction (CBRN)** by Associate Editor, Judith Tinnes. Finally, the Book Reviews section begins with an essay by Kaitlyn DaVisio, who reviews Julia Ebner's, The Language of Terrorists. Peter S. Henne then reviews Tricia L. Bacon's, The Counterinsurgency Dilemma: Foreign Fighter Influence on Insurgencies in Afghanistan and Somalia

Bibliography: Terrorism and Weapons of Mass Destruction (CBRN)

PT PERSPECTIVES ON TERRORISM

Judith Tinnes*

Volume XX, Issue 3
September 2026



This bibliography contains journal articles, book chapters, books, edited volumes, theses, grey literature, bibliographies and other resources on the use (or intended use) of weapons of mass destruction (i.e., chemical, biological, radiological, or nuclear weapons) by terrorist actors. It focuses on recent publications (up to July 2026) and should not be considered exhaustive. The literature has been retrieved by manually browsing more than 200 core and periphery sources in the field of Terrorism Studies. Additionally, full-text as well as reference retrieval systems have been employed to broaden the search.



By Brig Gen John Galatas, MD, MSc, HAMC and Prof Chara Spiliopoulou, MD







New Army smokescreen blocks radar tracking, infrared and more

Source: https://newatlas.com/military/new-army-smokescreen-disables-radar-tracking-infrared-and-more/

Oct 29 – Hiding on the battlefield is becoming easier as the US Army Combat Capabilities Development Command Chemical Biological Center (DEVCOM CBC) tests a new smokescreen designed to shield soldiers from visual inspection, night vision, infrared sensors, and radar beams alike.

Historically, the "fog of war" has been incidental rather than deliberate. When visibility on the field of conflict degraded, it was usually due to weather or heavy smoke from cannon fire, which generals often regarded as a nuisance, preferring a clear view of the battle in order to better deploy and move their resources.

That attitude was swept away by the time the First World War broke out.

By that time, weapons had become so precise and deadly in their effect that it

was far better not to be seen, so an arms race developed between the observer and the attack. The Cold War saw the development of vehicle-integrated smoke generators like the



observed. During the conflict, methods were developed to create thick clouds of impenetrable chemical smoke by burning heavy oil, titanium tetrachloride, and chlorosulfuric acid to hide trenches, infantry, and ships from enemy eyes.

By World War II, obscuration techniques became standard operating procedures.



Vaporized petroleum oils – known as "fog oil" – and engine exhaust systems protected entire fleets, seaports, and cities against enemy US M56 Coyote and M58 Wolf, as well as grenade launchers firing red phosphorus or hexachloroethane smoke mixtures.

The Millimeter Wave SOM deploys thousands of carbon fibers into the air to suppress radar capabilities | Imani Games

That was all well and good. However, though these chemical smoke screens could blind the eye and other devices using the visual or infrared spectra (and believe me, when a military smoke grenade goes off in your vicinity, you are really blind), radar beams could still see right through it. This is because radar operates on the millimeter scale of the spectrum and the smoke particles are simply too small to interfere with the beams.

Dr. Jill Harland (Left) and Michael Smith (Right) brief leaders during a recent live field demonstration on the development and functionality of the Millimeter Wave Screening Obscuration Module (SOM) and potential for integration with other technologies | Patrick Rodeheaver

The US Army's Millimeter Wave Screening Obscuration Module (SOM) changes all that by mixing in thousands of specially coated carbon filaments or fibers. When these disperse into the air, they act as passive electrical dipoles on the same frequency as military radar systems. As the beam passes through the smoke cloud, the fibers absorb,



scatter, and deflect it, causing the return signal to blur and drop below detection levels. Field demonstrations of the SOM in August at the Aberdeen Proving Ground in



US M56 Coyote smoke generator

Maryland were conducted in the open air using designated target signalers beaming fixed radar signatures to simulate battlefield radar reflections. The portable module dispersed about 30 lb (13.6 kg) of fibers to evaluate how rapidly the cloud could suppress active radar tracking. "Several targets or signatures were set up, and we had to obscure those targets," said Michael Smith, a mechanical engineer at DEVCOM CBC. "We used radar to observe the cloud formation and show the degradation of the radar signatures of each of those targets. As the cloud formed, the signature dropped, and we got our obscuration that way."

Smith added: "Watching the radar screens during the live dissemination was a defining moment for the entire development team. Our objective is to buy Soldiers critical time on the battlefield; improving survivability directly accomplishes our core mission."



M58 Wolf smoke generator

Following successful technical validation, DEVCOM CBC officially transitioned the system to the Portfolio Management Executive for Chemical, Biological, Radiological and Nuclear Defense (PME CBRND), marking a key milestone toward delivering the capability to warfighters.

The exact nature of the fibers is still classified, as is their toxicity, due to security protocols. That being said, protocols require such obscurants to undergo a full toxicological evaluation by the US Army Center for Health Promotion and Preventive Medicine (CHPPM) or the National Research Council (NRC) to set safety guidelines for military personnel during training and operations.

Session SFMC
NRBC : du terrain à l'hôpital

Posters présentés le 12 novembre 2025

Médecine de Catastrophe - Urgences Collectives 2026;10:48–49



P1

Examen post-mortem des corps contaminés : enjeu médical et criminalistique face aux menaces NRBC

Post-mortem examination of contaminated bodies: Medical and forensic challenge in the face of CBRN threats

Olivier Maresca [1], Hadrien Diakonoff [2], Arnaud Gouet [3], Anne-Sophie Lorin [2], Marie Boillet [2], Sébastien Follot [1], Guillaume Visseaux [2]

[1] *Groupe d'investigation en milieu dégradé, Institut de recherche criminelle de la Gendarmerie nationale (IRCGN), 5, boulevard de l'Hautil, 95000 Pontoise, France*

[2] *Département médecine légale odontologie, Institut de recherche criminelle de la Gendarmerie nationale (IRCGN), 5, boulevard de l'Hautil, 95000 Pontoise, France*

[3] *Force nationale NRBC de la Gendarmerie nationale (F2NRBC), France*

**Auteur correspondant.*

Adresse e-mail : guillaume.visseaux@gendarmerie.interieur.gouv.fr (G. Visseaux)

L'examen post-mortem des corps contaminés constitue un enjeu majeur à l'intersection de la médecine légale, de la criminalistique, de la santé publique et de l'éthique biomédicale (*Fig. 1*). Face à la diversité des agents de la menace de nature nucléaire, radiologique, biologique et chimique (NRBC), le médecin légiste doit concilier des impératifs contradictoires : assurer la sécurité des opérateurs, préserver la valeur probante des éléments recueillis et garantir la dignité du défunt. L'exploration de la mort en contexte NRBC, qu'elle découle d'un accident industriel, d'une exposition criminelle ou d'un acte terroriste, nécessite des protocoles spécifiques combinant biosécurité, rigueur scientifique et respect éthique. Cet article propose une analyse des enjeux éthiques et criminalistiques associés à ces pratiques, en s'appuyant sur les recommandations institutionnelles internationales. Il met en lumière la tension constante entre recherche de vérité, protection des personnels et respect dû aux victimes, tout en soulignant la nécessité d'une coordination interdisciplinaire accrue dans la gestion médicolégale des situations NRBC.

Déclaration de liens d'intérêts Les auteurs déclarent ne pas avoir de liens d'intérêts.

http://dx.doi.org/10.1016/j.pxur.2025.12.007



Wearable touchscreen weaves its way into your garment fabric

By Etiido Uko

Source: https://newatlas.com/wearables/wearable-touchscreen-fabric-garment/



The 96 by 54-pixel display can run a calculator, show a photo gallery, play a video, work as a compass, respond to voice commands, receive images over Bluetooth, as well as read and display body temperature | National University of Singapore

Oct 31 – Screens have become indispensable in most of our daily lives. We have them on phones, billboards, tiny wearables, coffee makers, toilets, and everywhere else. Scientists have now figured out a way to integrate them into the very fabric of clothes.

Researchers at the National University of Singapore (NUS) have found a way to turn ordinary-looking fabric into an interactive display screen.

We're not talking about a screen embedded in a shirt; the fabric *itself* is the screen. It can play videos, display notifications, measure your body temperature, and respond when you touch it! The enabling technology is a special, pressure-sensitive electronic fiber containing miniature LED chips, electrical connections, and a touch-sensitive layer. Each fiber is about 1 mm thick and 10 meters (32.8 ft) long.

For the demonstration, the researchers incorporated 54 of these fibers into the forearm of a sleeve. Each fiber contains 96 LEDs, resulting in a 96 × 54-pixel display with a 168 × 105-mm screen size; a 30 frames-per-second refresh rate; and 8-bit color depth. Granted, that's a fairly low-resolution screen by modern standards, but it can display recognizable images, animations, and simple graphical interfaces. Plus, it's a shirt sleeve!

Beyond the display fibers, the scientists also incorporated a microphone, a speaker, and several sensors into flexible garment fibers. The project is detailed in the journal, *Nature*.

So, how does it actually work? The first part of the trick is the electronic fibers themselves, which the researchers call digital pixel fibers. Each fiber is a long, flexible plastic thread, containing a row of miniature LED chips, tiny electrical wires, and a touch-sensitive layer. Each LED acts as an individual pixel that can light up in different colors,

while the electrical wires supply power and carry instructions that tell the LEDs what to display.

Getting all these electronics into something as thin and flexible as a thread was no small feat. The researchers started by arranging thousands of miniature RGB LED chips in a straight line, then running several incredibly thin, insulated copper wires along them. Using a programmable laser, they carefully removed the insulation at specific points where the wires needed to connect to the LEDs. They then applied solder and heated the assembly, allowing the molten metal to bond only to the exposed copper sections. This method enabled them to connect more than 5,000 electronic chips through over 20,000 electrical connections.

With the LEDs and their electrical connections in place, the researchers used a process called thermal drawing to turn the assembly into a fiber. This involved heating a larger polymer structure until it softened, then stretching it into a much thinner, elongated form while continuously feeding the interconnected LED strip into it. The process encased the electronics in a transparent, flexible polymer and incorporated conductive layers beneath the LEDs for touch sensing.

Each finished fiber essentially works like a long, narrow digital display. The LEDs contain red, green, and blue light-emitting elements whose brightness can be adjusted to produce different colors. A controller sends digital instructions along the copper wires, telling each LED what color to produce and how brightly to shine. Each LED receives its instructions and passes the remaining data to the next one, allowing the entire row to display different colors and patterns simultaneously.



Asst. Prof. Tural Khudiyev (second from right) from the College of Design and Engineering, NUS, with team members Heng Fu, PhD student (first from right), Ziang Li, PhD candidate (second from left), and Swetika Chaturvedi, Research Associate (first from left) | National University of Singapore

With the individual fibers working, the next step was to assemble them into an actual touchscreen. For their prototype, the researchers incorporated 54 electronic fibers – each containing 96 individually

controllable LEDs – into the forearm section of a garment sleeve, turning it into a functional two-dimensional screen.



Beyond the touchscreen itself, the researchers also incorporated several specialized electronic fibers into the garment, manufactured using the same technique as the display fibers.

These include a microphone and speaker for voice commands and audio playback; motion sensors to detect movement and orientation; a magnetometer for compass functionality; a temperature sensor to monitor body temperature; and an ambient light sensor to automatically adjust the screen's brightness. Together, these components allow the sleeve to perform several functions associated with early smartphones, including playing videos with sound, responding to voice commands, automatically rotating its display, and showing the wearer's body temperature.

Now, flexible displays, electronic textiles, and smart garments already exist. However, most approaches either attach electronic components to fabric or integrate relatively simple sensing and lighting functions. However, a programmable, touch-sensitive graphical user interface built from electronic fibers that form part of the garment itself is a first.

What's more, despite all the electronics involved, the researchers demonstrated that the electronic fabric could withstand 50 machine washes and 1,000 bending cycles without substantial deterioration in its display or touch performance. The manufacturing architecture, which integrates more than 5,000 chips with over 20,000 electrical connections while retaining the fabric's flexibility and breathability, is also a major achievement.

Potential applications include smart clothing that displays notifications, navigation instructions, and other information without requiring users to reach for their phones. In healthcare, garments could continuously monitor vital signs such as body temperature and heart rate, allowing wearers to view and interact with their health data directly on their clothing.

Athletes could use similar garments to track performance, while workers in industrial environments could receive safety alerts and operating instructions on their sleeves. The researchers also envision integrating artificial intelligence into future versions, potentially enabling clothing that responds intelligently to the wearer and their surroundings.

On the flip side, a 1-mm-thick thread is relatively thick. The display resolution is also quite low by modern standards.

The researchers are now working to improve the display's resolution by developing smaller electronic components and thinner fibers, while integrating more advanced sensors and on-device AI capabilities. The ultimate goal is to combine display, touch sensing, and intelligent processing into a single textile platform, paving the way for clothing that can monitor its wearer, understand its surroundings, and provide information or assistance when needed.

Israel warns US that Iran may use chemical weapons, but Washington questions intelligence - report

Source: https://www.jpost.com/middle-east/iran-news/article-913753

Nov 03 – Israel has provided the United States with intelligence indicating that Iran is considering using chemical weapons against its adversaries, but officials in Washington are divided over the information's credibility and significance, *The* New York Times reported on Tuesday, citing American and regional officials.

Some senior US officials received the intelligence with concern, while others expressed deep skepticism, viewing it as part of a pressure campaign by Prime Minister Benjamin Netanyahu's government aimed at convincing the Trump administration to resume large-scale fighting against Iran.

According to the report, during discussions with US intelligence agencies and other officials over the past two weeks, senior Israeli officials presented the chemical weapons threat as more urgent than Iran's ambitions to develop nuclear weapons.

Advertisement

Israeli intelligence officials told their American counterparts that they believe Iran is rapidly advancing technology that would allow it to mount chemical weapons on missiles or smuggle them into Israel or another country to carry out an attack.

Other senior American officials believe the threat should be taken seriously, particularly in light of a series of recent warnings about Iranian preparations to attack US interests.

According to the newspaper, there is little disagreement within the American intelligence community that Iran is developing chemical weapons. The central dispute concerns whether Iranian leaders would actually use them, particularly if Iran is not attacked again.

Gulf officials question Israeli chemical weapons intelligence: 'No evidence'

Israel also shared some of the intelligence with officials in Gulf states. Several questioned whether Iran was developing plans to use chemical weapons and believe Israel is attempting to push the United States and its partners toward a more intensive phase of the war.

A regional official told the newspaper that Israel had presented Gulf countries with assessments suggesting Iran was working to make its chemical weapons operational, but had not shared supporting evidence.

According to the official, Gulf governments regarded the claims as lacking seriousness.

For some American officials, the warnings have revived memories of the faulty intelligence surrounding Iraq's weapons of mass destruction in 2002.

At the time, US intelligence agencies presented the White House with a firm assessment that Iraq possessed such weapons, although the country had largely abandoned or suspended its nuclear, chemical and biological weapons programs.

Even among those briefed on the new intelligence, assessments differ regarding how quickly and effectively Iran could deploy chemical weapons.

According to experts and American officials who spoke with the newspaper, mounting a chemical weapon on a ballistic missile is not particularly difficult, but ensuring the effective dispersal of the chemical agent is more complicated.

Smuggling a bomb across a border also presents difficulties. Another possibility mentioned was the use of a drone.

Despite the Israeli warnings, the newspaper reported that preparations for responding to chemical weapons attacks are not a central component of the Home Front Command exercises taking place across Israel this week.

Two Home Front Command officials said

there had also been no widespread reminders distributed to officers or the public regarding protective instructions against such a threat.
The IDF declined to comment.

US prepares potential Iran strike as Washington, Tehran pursue diplomatic solution

The intelligence was shared as the United States and Iran explore the possibility of a diplomatic breakthrough while simultaneously preparing for a resumption of hostilities.
According to senior American officials, US Central Command (CENTCOM) has a plan for an attack on Iran that could be carried out as early as Wednesday, November 4, one day after the US midterm elections. The report stated that three American aircraft carriers are currently in the region, while the preferred operational window for an attack is expected to be brief. One of the aircraft carriers will need to return to its home port after the beginning of November, and particularly dark nights are expected in the coming days, providing favorable conditions for military operations.
However, President Donald Trump has not yet approved a large-scale attack, and diplomatic contacts between Washington and Tehran are continuing.
In recent weeks, the United States has concentrated warships, fighter jets and bombers in the region in preparation for a possible relatively short military campaign involving intensive strikes.
At the same time, diplomats are attempting to formulate an agreement that would reopen the Strait of Hormuz, address Iran's nuclear program and postpone further military action.
According to the report, the military buildup could also serve as leverage to support the diplomatic effort.
Meanwhile, US intelligence agencies assess that the threat to Americans in the Middle East and several other countries is at its highest level since the war began in February.
Intelligence collection was intensified after an Iranian plot to attack a base in Britain used by American fighter jets was uncovered.
On October 23, a warning memorandum regarding potential Iranian attacks was sent to senior administration officials. Diplomats and other personnel were subsequently placed on heightened alert.
The newspaper also linked Netanyahu's efforts to his political situation following the Israeli elections, in which he failed to secure a clear path toward forming a government.
Several commentators who spoke with the newspaper suggested that Netanyahu might attempt to use a national security emergency to pressure opposition leaders into joining a coalition under his leadership.

Iran denies chemical weapons program as US officials warn of possible escalation

American allegations regarding an Iranian chemical weapons program date back decades.
In 2003, Iran acknowledged that it had developed chemical capabilities during the Iran-Iraq War but claimed that it subsequently dismantled them.
Tehran denies possessing chemical weapons and has previously described such accusations as psychological warfare conducted by Israel and Netanyahu.
Dana Stroul, a former senior Pentagon official responsible for Middle East policy during the Biden administration, said it has been known for more than two decades that Iran has been stockpiling components for chemical weapons, but has never used them.
However, she warned that Tehran could feel "existential pressure" and potentially cross the threshold into directly using such weapons offensively.
A spokesperson for Netanyahu's office told the *NYT*: "Israel closely monitors every threat posed by the Iranian terrorist regime and is prepared to confront it."
The White House did not respond to the newspaper's request for comment, but an American official said Trump would defend the United States and its allies against any potential threat.

EDITOR'S COMMENT: Iran might not possess a nuclear bomb, but it has the know-how for chemical weapons and the industry to support the production of new ones. The same might apply for biological weapons. We used to say that if Israel is seriously cornered, it will use its nukes; the same applies for Iran and possible CWAs. The big problem is that GCC allies are not adequately prepared to deal with an asymmetric attack and mass contaminated casualties even if only military targets are hit. Only hope that the famous perception of "it will not happen to us" belongs to the past.

Chemical Weapons Under International Law: The CWC, OPCW and Accountability

By Edmarverson A. Santos
Source: https://www.diplomacyandlaw.com/post/chemical-weapons

Chemical weapons are prohibited under international law through a combination of treaty obligations and customary rules governing armed conflict. The principal legal instrument is the Chemical Weapons Convention (CWC), which prohibits States Parties from developing, producing, acquiring, stockpiling, transferring or using chemical weapons. The Organisation for the Prohibition of Chemical Weapons (OPCW) oversees the Convention's implementation, verifies declarations and destruction activities, and investigates alleged chemical weapons use within its mandate.

The prohibition extends beyond conventional battlefields. Toxic agents such as VX and sarin, as well as industrial chemicals such as chlorine when used for prohibited purposes, fall within the Convention's legal framework. Its obligations apply in peacetime and during armed conflict, while national implementing legislation addresses prohibited activities by individuals and organizations.

The CWC has achieved substantial results. In July 2023, the OPCW confirmed the irreversible destruction of all chemical weapons stockpiles declared by States Parties up to that point, representing approximately 72,304 metric tons of chemical agents. Yet subsequent discoveries of undeclared weapons in Syria demonstrate that the destruction of known stockpiles does not establish the absence of prohibited weapons elsewhere.

Three questions determine the legal treatment of chemical weapons: what conduct international law prohibits, how compliance is established, and which institutions can hold violators accountable. Although the CWC establishes extensive obligations and an international verification system, responsibility for chemical attacks must still be determined through the applicable rules of state responsibility, domestic criminal law, and international criminal jurisdiction.

1. Chemical Weapons: Definition and Legal Scope

Article II of the CWC defines chemical weapons by reference to toxic chemicals, their precursors, specially designed munitions, and equipment associated with their use. The definition extends beyond bombs, artillery shells, and poisonous gases deployed during military operations.

Under Article II(2), a toxic chemical is any chemical capable, through its action on life processes, of causing death, temporary incapacitation, or permanent harm to humans or animals. The definition applies regardless of the chemical's origin, method of production, or physical form.

A substance does not become a chemical weapon solely because it is toxic. Its intended purpose, the quantities involved, and the equipment associated with its use may determine whether it falls within the Convention's prohibitions.

1.1 The General-Purpose Criterion

The CWC adopts a general-purpose criterion under Article II(1). Toxic chemicals and their precursors fall within the definition of chemical weapons unless intended for purposes not prohibited under the Convention, provided their types and quantities remain consistent with those purposes.
Article II(9) identifies permitted categories, including industrial, agricultural, research, medical, and pharmaceutical activities. It also recognizes protective purposes, certain military purposes unrelated to chemical warfare, and law enforcement. These categories do not provide unrestricted exceptions. The nature and scale of the activity must remain consistent with its stated purpose.
This approach addresses the problem of dual-use chemicals. Chlorine, for example, has legitimate applications in water treatment and industrial production. Its ordinary manufacture and use do not constitute chemical weapons activities. Deliberately releasing chlorine to exploit its toxic effects against people, however, may bring the substance within the Convention's definition of a chemical weapon.
The general-purpose criterion prevents circumvention through technical classification. A substance does not escape the prohibition merely because it was never designed as a military agent or does not appear in the Convention's schedules. Its intended use remains legally decisive.

1.2 VX, Sarin and Chlorine: Agents and Schedules

Chemical warfare agents differ in their physiological effects, persistence, and potential to cause harm. Nerve agents interfere with the normal functioning of the nervous system, while blister agents damage exposed tissue. Choking agents primarily injure the respiratory system.
VX is an exceptionally toxic organophosphorus nerve agent. It inhibits acetylcholinesterase, an enzyme required for normal nerve signaling. Severe exposure can cause respiratory failure and death. Sarin operates through a similar toxic mechanism, although its physical characteristics and persistence differ from those of VX.
Sulfur mustard is a blister agent associated with severe skin, eye, and respiratory injuries. Chlorine, by contrast, is a common industrial chemical that can cause serious lung damage when inhaled at harmful concentrations. Its civilian applications do not prevent it from being used as a chemical weapon.
The CWC's Annex on Chemicals establishes three schedules for applying verification and control measures. Schedule 1 includes substances such as VX, sarin, and sulfur mustard, which present particularly serious risks under the treaty's scheduling criteria and have limited legitimate applications.
Schedule 2 covers other toxic chemicals and precursors presenting significant risks, while Schedule 3 includes substances with relevant weapons-related risks that may also be produced in substantial quantities for peaceful purposes.
The schedules serve regulatory purposes rather than defining the outer limits of the prohibition. Chlorine is not listed in them, but its use as a chemical weapon remains prohibited. The legal classification depends on the Convention's general-purpose criterion, not simply the presence of a substance on a schedule.

1.3 Riot Control and Law Enforcement

The CWC distinguishes the use of chemicals for legitimate law enforcement from their employment as methods of warfare. Article II(7) defines riot control agents by their capacity to produce rapid sensory irritation or disabling physical effects that disappear within a short period after exposure ends.

Article I(5) expressly prohibits States Parties from using riot control agents as a method of warfare. The prohibition applies even where the same agent may be lawfully employed for certain domestic policing activities.
The distinction becomes more difficult when substances produce incapacitation through the central nervous system rather than temporary sensory irritation. On December 1, 2021, the OPCW Conference of the States Parties adopted Decision C-26/DEC.10, addressing the aerosolized use of central nervous system-acting chemicals for law-enforcement purposes.
The Conference determined that such aerosolized use is inconsistent with law enforcement as a permitted purpose under the Convention. The decision drew on scientific findings concerning the substantial risks associated with these substances, including the possibility of permanent injury or death.
It did not prohibit their legitimate medical or other permitted applications. The decision specifically addressed aerosolized use in the context of law enforcement.
A government's designation of a substance as an incapacitating agent does not independently establish that its deployment is permissible. The applicable legal assessment must consider the chemical's effects, its intended purpose, and the Convention's requirements.

2. From the Geneva Protocol to a Comprehensive Prohibition

International restrictions on chemical warfare developed before the establishment of the CWC. Early efforts addressed particular methods of combat, including the use of poison and poisonous gases. Industrialized chemical warfare during the First World War demonstrated the destructive consequences of large-scale toxic-agent deployment.
The use of chlorine, phosgene, and mustard agents during that conflict caused extensive casualties and long-term injuries. The experience contributed to international efforts to prohibit chemical warfare, although early legal instruments did not eliminate the production or possession of the substances involved.

2.1 The Limited Reach of the 1925 Geneva Protocol

The 1925 Geneva Protocol prohibited the use in war of asphyxiating, poisonous, or other gases and analogous liquids, materials, and devices. It reinforced earlier restrictions on poisonous weapons and became a central instrument regulating chemical warfare.
Its principal limitation concerned the activities that it regulated. The Protocol prohibited use but did not establish a comprehensive ban on developing, manufacturing, or stockpiling chemical weapons. States could maintain substantial arsenals without necessarily breaching its terms.
Reservations concerning retaliation further complicated the historical regime. Some States accepted the prohibition while reserving the possibility of responding in kind if an opposing party used chemical weapons first. Such reservations reflected an approach in which deterrence and the possibility of retaliation remained prominent considerations.
Chemical warfare nevertheless continued after 1925. Iraqi forces employed chemical weapons during the Iran–Iraq War, including against Iranian forces and Kurdish civilians. The March 1988 attack on Halabja became one of the most prominent examples of chemical weapons use against a civilian population.
These incidents exposed the limitations of restrictions on battlefield use without corresponding international mechanisms to eliminate chemical arsenals and verify compliance. Subsequent negotiations sought a comprehensive system that would regulate the entire life cycle of chemical weapons.
The Chemical Weapons Convention opened for signature in Paris on January 13, 1993, and entered into force on April 29, 1997. Unlike the Geneva Protocol,

it prohibited an entire category of weapons and established international verification of destruction and relevant chemical activities.

2.2 Customary Prohibition in Armed Conflict

The prohibition on using chemical weapons also exists independently of the CWC as a rule of customary international humanitarian law. Rule 74 of the International Committee of the Red Cross's study of customary international humanitarian law identifies the prohibition as applicable in both international and non-international armed conflicts.

Customary international law develops through sufficiently general state practice accepted as law. In the chemical weapons context, treaty practice, national legislation, military manuals, and repeated international condemnation support the existence of a prohibition extending beyond CWC membership.

The International Criminal Tribunal for the former Yugoslavia examined this development in Prosecutor v. Tadić, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Case No. IT-94-1-AR72, October 2, 1995.

In paragraph 124, the Appeals Chamber concluded that international consensus had emerged on the prohibition of chemical weapons in internal armed conflicts. Its reasoning drew partly on international reactions to Iraq's use of chemical weapons against Kurdish civilians.

The decision supported the development of customary rules regulating methods of warfare in non-international conflicts. It did not establish that every treaty rule applicable to international armed conflicts had automatically become applicable to internal conflicts.

This distinction is central to international humanitarian law. Customary rules prohibit chemical weapons use by parties to armed conflicts, including organized non-state armed groups. The CWC imposes additional treaty obligations on States Parties concerning production, possession, transfer, verification, and destruction.

The two legal regimes are complementary, but their sources and obligations are not identical.

3. The Convention's Prohibitions and State Duties

The CWC establishes a comprehensive legal system for chemical disarmament and non-proliferation. Its general prohibitions are accompanied by obligations concerning declarations, destruction, verification, and national implementation.

The Convention also preserves legitimate chemical activities. Article VI recognizes that States Parties may develop, produce, acquire, retain, transfer, and use toxic chemicals and precursors for purposes not prohibited under the treaty, subject to its regulatory conditions.

The Convention's operation reflects the principle of pacta sunt servanda, expressed in Article 26 of the Vienna Convention on the Law of Treaties. Treaties in force bind their parties and must be performed in good faith. The specific requirements of chemical disarmament arise from the CWC itself.

3.1 Article I: Prohibited Conduct Without Exception

Article I establishes the CWC's principal prohibitions. Each State Party undertakes never under any circumstances to develop, produce, otherwise acquire, stockpile, or retain chemical weapons, or transfer them directly or indirectly to anyone.

The provision separately prohibits chemical weapons use, military preparations for use, and assistance, encouragement, or inducement of prohibited activities.

The Convention does not provide an exception permitting chemical warfare in self-defense, military necessity, or retaliation against another party's chemical

attack. Its general prohibitions apply regardless of the circumstances in which a State might seek to employ these weapons.
Article XXII also prohibits reservations to the Convention's articles. Reservations to its annexes are permitted only if compatible with the Convention's object and purpose. States Parties cannot selectively exclude the central prohibition on chemical weapons use through a treaty reservation.
The obligations extend beyond the conduct of government armed forces. Prohibited transfers or assistance may constitute treaty breaches, and States Parties must adopt domestic measures addressing activities undertaken by natural and legal persons within the Convention's jurisdictional requirements.

3.2 Declarations, Destruction and National Legislation

Article III requires States Parties to submit declarations concerning chemical weapons, relevant production facilities, historical transfers, and other specified activities. These declarations provide the basis for international verification.
Articles IV and V establish obligations concerning the destruction of chemical weapons and chemical weapons production facilities. Destruction must follow prescribed procedures and verification requirements. The Convention also contains separate arrangements for old and abandoned chemical weapons, reflecting their different historical and technical circumstances.
Article VII requires States Parties to adopt the necessary national implementation measures. Under Article VII(1)(a), these measures must prohibit natural and legal persons from undertaking activities forbidden by the Convention within the specified territorial and jurisdictional scope, including through penal legislation.
Article VII(1)(c) extends the relevant penal legislation to prohibited activities undertaken abroad by natural persons possessing the State Party's nationality, in conformity with international law. Article VII(2) requires cooperation and appropriate legal assistance between States Parties to facilitate implementation.
These obligations give the Convention a domestic enforcement dimension. National authorities must possess the legal means to address prohibited activities, while international verification examines compliance with the treaty's requirements.
The Convention also addresses assistance and protection against chemical attacks through Article X. Article XI promotes international cooperation in peaceful chemical activities, reflecting the objective of eliminating chemical weapons without unnecessarily obstructing legitimate scientific and industrial development.

4. The OPCW: Verification, Inspections and Compliance

The OPCW was established under Article VIII of the CWC to implement its provisions and oversee the international verification system. Its headquarters are located in The Hague, Netherlands.
The organization monitors declarations, conducts inspections, verifies destruction, and assists States Parties with implementation. It also addresses compliance concerns through the institutional procedures established by the Convention.
The OPCW's authority is defined by its constituent treaty and subsequent decisions adopted within that legal framework. It can establish technical findings and support compliance decisions, but it does not possess general criminal jurisdiction or the authority to convict individuals.

4.1 The Conference, Executive Council and Secretariat

The Conference of the States Parties is the OPCW's principal policy-making body. It considers matters relating to treaty implementation, reviews compliance, and exercises the powers assigned to it under the Convention.

The Executive Council supervises aspects of the organization's activities and addresses implementation and compliance concerns within its mandate. It may recommend measures to the Conference and exercise powers delegated to it in accordance with the Convention.
The Technical Secretariat conducts much of the organization's scientific and operational work. Its responsibilities include inspecting relevant facilities, examining declarations, analyzing technical information, and preparing reports for the policy-making organs.
Designated laboratories provide specialized analytical capabilities. National authorities coordinate the domestic implementation of treaty obligations and serve as points of contact with the OPCW.
These institutional arrangements allow technical findings to inform compliance decisions while preserving the different functions assigned to the organization's constituent bodies.

4.2 Routine Verification and Challenge Inspections

The CWC's Verification Annex establishes inspection procedures according to the activities and facilities concerned. Routine verification covers declared chemical weapons, destruction operations, scheduled chemicals, and other relevant industrial production.
For legitimate chemical facilities, inspections assess whether declarations correspond with observable activities and whether operations are consistent with treaty obligations. The applicable requirements depend on the substances, quantities, and verification categories involved.
Article IX provides a mechanism for resolving concerns about possible non-compliance. A State Party may request a challenge inspection of another State Party's facility or location within the Convention's jurisdictional framework.
The inspected State Party is obliged to accept the inspection in accordance with treaty procedures. The Convention also provides safeguards for confidential information and mechanisms intended to prevent abusive requests.
Challenge inspections differ from routine verification and investigations of alleged attacks. They are designed to clarify compliance concerns arising under the treaty rather than automatically determine criminal responsibility.

4.3 Destruction of Declared Stockpiles in 2023

On July 7, 2023, the OPCW confirmed that the last chemical weapon from the stockpiles declared by States Parties had been irreversibly destroyed. The final destruction occurred at the Blue Grass Chemical Agent-Destruction Pilot Plant in Kentucky, United States.
The verified destruction covered approximately 72,304 metric tons of declared chemical agents accumulated under the Convention's declaration and verification system. It marked the completion of a central objective of the CWC.
The achievement concerned declared stockpiles. It did not establish that all national declarations were complete, that undisclosed weapons could not exist, or that every remaining treaty obligation had been fulfilled.
Old and abandoned chemical weapons continue to require identification and destruction under the Convention's applicable procedures. Industrial verification must also continue to prevent renewed prohibited production.
Subsequent discoveries in Syria demonstrated the practical significance of these remaining obligations. Earlier verified destruction activities had not revealed the full extent of the former Syrian chemical weapons programme.

5. Investigation and Attribution of Alleged Attacks

Investigations of alleged chemical weapons attacks involve several factual questions. Investigators must determine whether a toxic chemical was present,

whether it was employed as a weapon, how the incident occurred, and whether the available evidence identifies those responsible.
Scientific confirmation of chemical exposure does not establish the identity of the perpetrator. Evidence linking an attack to a military unit or organization may support an attribution finding, but individual criminal liability requires additional legal determinations.
International investigative mechanisms operate under defined mandates and evidentiary standards. Their findings may assist subsequent legal proceedings without replacing the functions of national or international courts.

5.1 OPCW Missions and Their Different Mandates

The OPCW established its Fact-Finding Mission (FFM) in Syria in 2014 to determine whether toxic chemicals had been used as weapons. Its mandate did not include identifying the perpetrators of alleged attacks.
The OPCW–United Nations Joint Investigative Mechanism (JIM), established through Security Council Resolution 2235 (2015), subsequently investigated responsibility for specified incidents. Its mandate expired in November 2017.
On June 27, 2018, the OPCW Conference of the States Parties adopted Decision C-SS-4/DEC.3, authorizing arrangements to identify perpetrators of chemical weapons use in Syria. The Investigation and Identification Team (IIT) was established pursuant to that decision.
The IIT examines qualifying incidents for which the FFM determined that chemical weapons use or likely use occurred and for which the former JIM had not issued a final attribution finding.
The Declaration Assessment Team (DAT) performed a different function. Established in 2014, it examined gaps, inconsistencies, and discrepancies in Syria's declared chemical weapons programme.
Following the change of government in Syria, these activities were coordinated through the OPCW Office of Special Missions, established on June 1, 2025.
The IIT's legal authority remains limited. Its fifth report, issued as OPCW Technical Secretariat document S/2478/2026 on January 21, 2026, expressly states that the team is not a judicial body authorized to assign individual criminal responsibility. Nor does it possess authority to make final findings of non-compliance with the CWC.
The team's mandate is to establish facts and identify perpetrators within the framework of the relevant OPCW decisions. Formal treaty compliance measures and criminal adjudication belong to different institutional processes.
Outside these Syria-specific arrangements, the United Nations Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons provides a separate investigative framework. Its mandate and procedures should not be equated with those of the IIT.

5.2 Evidence, Attribution and Evidentiary Thresholds

Chemical weapons investigations may involve environmental samples, biomedical specimens, laboratory findings, witness interviews, medical records, satellite imagery, and authenticated photographs or videos.
Investigators may examine munition remnants, delivery systems, and the circumstances of military operations. Technical findings are assessed alongside witness testimony and other available information to determine whether the evidence supports a coherent account of an incident.
Chain-of-custody procedures help establish the origin, handling, and integrity of physical evidence. They are particularly important when investigators gain access to a site long after an alleged attack or when materials have passed through several custodians.

The IIT applies a reasonable-grounds evidentiary standard. Its conclusions depend on the collective assessment and corroboration of available information, including the consideration of alternative explanations.
The fifth IIT report concerning Kafr Zeita describes the examination of witness statements, samples, munition remnants, computer modeling, satellite imagery, and other documentary evidence. The investigators assessed the consistency and probative value of that material before reaching their attribution findings.
The reasonable-grounds standard differs from the criminal standard of proof beyond reasonable doubt. An IIT finding may identify a perpetrator for institutional purposes without establishing every element required for conviction.
Criminal courts must independently assess jurisdiction, the elements of the alleged offense, individual responsibility, and the procedural rights of the accused.

6. Syria: Attribution, Disarmament and Treaty Compliance

Syria illustrates the difficulty of enforcing a comprehensive chemical weapons prohibition during armed conflict and political instability. Its experience includes verified chemical weapons use, incomplete declarations, disarmament operations, and successive investigative mechanisms.
The Syrian case demonstrates that compliance cannot be assessed solely by measuring the quantity of weapons destroyed. Complete declarations, access to relevant facilities, cooperation with investigators, and the elimination of undeclared capabilities remain independent legal requirements.
The obligations of the Syrian state did not disappear following the fall of Bashar al-Assad's government in December 2024. A change of government does not ordinarily terminate the international legal personality of the State or extinguish its existing treaty commitments.

6.1 Accession and Security Council Resolution 2118

The large-scale chemical attack in the Ghouta area near Damascus on August 21, 2013, intensified international efforts to address Syria's chemical weapons programme.
The United Nations Mission to Investigate Allegations of the Use of Chemical Weapons in the Syrian Arab Republic established that chemical weapons had been used in Ghouta, including the nerve agent sarin. Its September 2013 findings were supported by biomedical and environmental evidence, laboratory analysis, and the examination of affected sites and munitions.
The mission's mandate concerned determining whether chemical weapons had been used. It did not include formally attributing the attack to a particular perpetrator.
Syria deposited its instrument of accession to the CWC on September 14, 2013, and the Convention entered into force for Syria on October 14, 2013. These developments accompanied international arrangements for eliminating its declared chemical weapons.
On September 27, 2013, the United Nations Security Council adopted Resolution 2118, endorsing arrangements for the destruction of Syria's chemical weapons programme and reinforcing the relevant international obligations.
The OPCW subsequently supervised the removal and destruction of declared chemical agents and other relevant materials. These operations were significant, but concerns about the accuracy and completeness of Syria's declarations remained.
Subsequent OPCW investigations established additional instances of chemical weapons use. The former Syrian authorities' incomplete declarations and failure to disclose the full scope of their programme prevented earlier destruction activities from resolving Syria's compliance obligations.

6.2 Attribution Findings for State and Non-State Actors

The OPCW's investigations identified perpetrators of several chemical attacks in Syria. The findings differ according to the incident, the available evidence, and the actors involved.

In its third IIT report, S/2125/2023, issued on January 27, 2023, the OPCW concluded that there were reasonable grounds to believe that Syrian Arab Air Forces were responsible for the April 7, 2018 chemical attack in Douma.

The report found that at least one helicopter operating under the control of the Syrian Tiger Forces dropped two cylinders containing toxic chlorine gas onto residential buildings. The attack killed 43 named individuals and affected dozens more.

The fourth IIT report, S/2255/2024, issued on February 22, 2024, concerned the September 1, 2015 attack in Marea. It concluded that there were reasonable grounds to believe units of the Islamic State in Iraq and the Levant (ISIL) had deployed sulfur mustard during military operations against the town.

The Marea investigation identified modified artillery projectiles used to disperse the chemical agent. It also examined evidence concerning the organizational structures and command arrangements involved in the operation.

The findings demonstrate that chemical weapons use in Syria involved both state forces and organized armed groups. The applicable obligations of non-state actors in international law depend on the relevant legal regime. Parties to an armed conflict are bound by applicable international humanitarian law, while the CWC imposes treaty obligations on its States Parties.

In January 2026, the IIT issued its fifth report, S/2478/2026, addressing an incident in Kafr Zeita on October 1, 2016.

The investigation concluded that there were reasonable grounds to believe a Syrian Arab Air Force helicopter dropped at least one pressurized chlorine cylinder near a cave system in the Wadi al-Aanz valley. The cylinder struck an area near the ventilation openings of a hospital operating within the cave complex.

The cylinder ruptured and released chlorine gas, injuring 35 named individuals and affecting dozens more. The IIT considered physical evidence, witness statements, imagery, computer modeling, and other information before identifying the Syrian Arab Air Forces as the perpetrators within its mandate.

These reports provide documented attribution findings, not criminal convictions. They do not establish that every individual associated with the military units or organizations involved bears criminal responsibility.

6.3 Undeclared Weapons and the 2026 Disarmament Effort

The fall of the Assad government in December 2024 created new opportunities for OPCW access to facilities, documentation, and other locations associated with Syria's chemical weapons programme.

On February 8, 2025, the OPCW Director-General visited Damascus and met representatives of the new Syrian authorities. Subsequent cooperation allowed investigators to examine suspected locations, collect documentation, and continue verification activities.

In May 2026, an OPCW expert team discovered a significant quantity of previously undeclared chemical weapons-related materials. The findings included chemical munitions, separately stored substances, equipment, and thousands of pages of documentation concerning the former Syrian programme.

Among the discoveries were aerial bombs resembling types previously associated with chemical attacks in Syria, along with rockets of a type connected to the 2013 Ghouta attack.

The discoveries confirmed the OPCW's longstanding assessment that the former Syrian authorities had withheld information about the extent of their chemical weapons activities.
On July 9, 2026, the OPCW Executive Council adopted Decision EC-112/DEC.7, reinstating Syria's rights and privileges under the Convention. Those rights had been suspended in 2021 following findings concerning the former Syrian government's non-compliance.
The reinstatement followed progress in cooperation, including amendments to Syria's initial declaration, preparations for systematic verification, and initial steps toward the destruction of identified remnants.
The Executive Council also approved a detailed plan for verifying the destruction of Category 3 chemical weapons at Al Qutayfah and facility agreements relating to the Al Qutayfah and Homs chemical weapons storage facilities.
The decision did not certify complete compliance. Syria remained responsible for fulfilling its outstanding obligations, and the OPCW retained its verification responsibilities.
Further progress was confirmed later in 2026. In an address delivered on October 26, OPCW Deputy Director-General Mekondjo Kaapanda-Girnus reported that 42 previously undeclared chemical aerial bombs associated with the former Syrian programme had been discovered, declared, and irreversibly destroyed during the year under OPCW verification.
The destruction marked the first OPCW-verified elimination of chemical munitions in Syria since 2014. The available official confirmation does not establish that all 42 bombs had been destroyed before the July reinstatement decision.
Syria's experience demonstrates the difference between verified destruction of identified weapons and complete fulfillment of treaty obligations. International verification must continue until remaining declarations, materials, and facilities have been addressed in accordance with the Convention.

7. From Treaty Violations to Legal Accountability

International law distinguishes the responsibility of States from the criminal responsibility of individuals. A chemical weapons attack may engage both forms of responsibility, but the applicable rules, evidentiary requirements, and institutions differ.
A State may incur international responsibility when conduct attributable to it breaches an obligation binding upon that State. Criminal proceedings require a separate legal basis and proof that an individual committed an offense within the jurisdiction of the court concerned.
The OPCW contributes to accountability by investigating incidents, preserving relevant information, and reporting findings. It does not prosecute or convict alleged perpetrators.

7.1 State Responsibility and Article XII Measures

The international responsibility of a State arises when conduct attributable to it breaches an international obligation. The general framework is reflected in the International Law Commission's 2001 Articles on Responsibility of States for Internationally Wrongful Acts.
The Articles are not a treaty, although significant provisions reflect customary international law. Article 2 identifies attribution and breach as the elements of an internationally wrongful act.
Where a State's armed forces violate the CWC, attribution may follow from their status as state organs under the general law of responsibility. Different questions arise where private persons or organized armed groups are involved, particularly when instructions, direction, or control by the State are alleged.
The consequences of state responsibility in international law may include cessation of the wrongful conduct, assurances of non-repetition where appropriate, and reparation for legally established injury.

Article XII of the CWC establishes additional procedures for addressing treaty compliance concerns. Under Article XII(2), the Conference of the States Parties may restrict or suspend a State Party's rights and privileges when the applicable conditions are satisfied, including failure to comply with a request by the Executive Council to remedy a compliance problem.
Article XII(3) authorizes the Conference to recommend collective measures to States Parties, in conformity with international law, where activities prohibited by the Convention may cause serious damage to its object and purpose.
Article XII(4) imposes a different obligation. In cases of particular gravity, the Conference shall bring the issue, including relevant information and conclusions, to the attention of the United Nations General Assembly and Security Council.
This mandatory referral provision does not itself authorize military force or impose Security Council sanctions. Any subsequent UN action must rest on the legal powers and procedures applicable to the relevant UN organ.
The suspension of certain Syrian rights and privileges in 2021, followed by their reinstatement in July 2026, illustrates the operation of the Convention's compliance procedures. Reinstatement reflected progress under the treaty without extinguishing questions concerning earlier violations or outstanding obligations.

7.2 War Crimes and the Limits of ICC Jurisdiction

Chemical weapons use during armed conflict may constitute a war crime under international criminal law. Article 8 of the Rome Statute identifies prohibited methods of warfare, including the employment of poison, poisoned weapons, and asphyxiating or poisonous gases.
Articles 8(2)(b)(xvii) and 8(2)(b)(xviii) address these offenses in international armed conflicts.
At the Kampala Review Conference on June 10, 2010, States Parties adopted Resolution RC/Res.5, introducing corresponding provisions for non-international armed conflicts through Articles 8(2)(e)(xiii) and 8(2)(e)(xiv).
The amendments did not become applicable to every State Party automatically. Under Article 121(5) of the Rome Statute, amendments to Article 8 enter into force for accepting States Parties one year after the deposit of their instruments of ratification or acceptance.
Article 121(5) also provides that, regarding a crime covered by an amendment, the Court shall not exercise jurisdiction when the crime is committed by the nationals of a State Party that has not accepted the amendment or on that State Party's territory.
These amendment-specific conditions must be considered alongside the ordinary jurisdictional provisions of Articles 11, 12, and 13 and any relevant question concerning Security Council referral.
The Kampala amendments to Article 8 first entered into force on September 26, 2012, for San Marino, following its ratification on September 26, 2011. Their subsequent application depends on the relevant State's treaty position and the applicable jurisdictional rules.
A violation of the CWC does not automatically constitute a war crime within the jurisdiction of the ICC. The conduct must satisfy the elements of an offense defined in the Rome Statute.
For the provisions concerning poison and prohibited gases, those elements include the employment of substances or weapons meeting the specified harmful characteristics, a connection with the relevant category of armed conflict, and awareness of the factual circumstances establishing that conflict.
The ICC's Elements of Crimes specify additional requirements concerning the substances and the circumstances of their use. Treaty prohibitions concerning possession, production, or transfer cannot simply be converted into the Rome Statute's offenses concerning employment of prohibited weapons.

The Rome Statute of the International Criminal Court also establishes jurisdictional limitations. Syria is not a State Party, and the Court does not possess general jurisdiction over crimes committed on Syrian territory merely because the alleged conduct violates international criminal law.
A Security Council referral under Article 13(b), an applicable territorial or nationality connection, or another legally valid basis would be necessary. The relevant temporal and substantive jurisdictional requirements would still need to be examined.
Chemical weapons use may also form part of crimes against humanity where the separate elements of Article 7 are established. These include a widespread or systematic attack directed against a civilian population, undertaken pursuant to or in furtherance of a State or organizational policy, and the accused's knowledge of the attack.
The use of a chemical agent alone does not establish those additional requirements.

7.3 Domestic Prosecutions and the VX Incident

Domestic criminal jurisdiction provides an important means of enforcing chemical weapons prohibitions. Article VII of the CWC requires States Parties to adopt implementing legislation, including penal measures addressing prohibited activities by natural and legal persons.
The Convention also requires nationality-based extensions of the relevant penal legislation and cooperation between States Parties. These provisions recognize that prohibited chemical weapons activities may involve cross-border transfers, foreign nationals, and conduct occurring outside the territory of the prosecuting State.
United Nations Security Council Resolution 1540 (2004), adopted under Chapter VII of the UN Charter, reinforces national obligations concerning weapons of mass destruction. It requires States to adopt and enforce appropriate laws preventing non-state actors from manufacturing, acquiring, possessing, developing, transporting, transferring, or using nuclear, chemical, or biological weapons and their means of delivery, as well as establishing relevant domestic controls.
The fatal VX incident at Kuala Lumpur International Airport 2 on February 13, 2017, illustrates chemical weapons use outside conventional warfare.
Malaysian authorities reported that VX had been identified in connection with the death of a North Korean national. The deceased was widely identified as Kim Jong-nam. The OPCW's official decision addressed the incident on the basis of information supplied by Malaysia rather than an independent OPCW criminal determination.
On March 9, 2017, the OPCW Executive Council adopted Decision EC-84/DEC.8, expressing grave concern over Malaysia's report that VX had been used in the fatal incident. The Council supported Malaysia's investigation and requested technical assistance from the Director-General upon Malaysia's request.
The criminal investigation remained a matter for Malaysian authorities. Any separate allegation of responsibility by another State would require evidence and application of the relevant international attribution rules.
The incident demonstrates that intentional poisoning involving a chemical weapon does not automatically constitute a war crime. Without the necessary connection to an armed conflict, liability must be assessed under other applicable legal provisions, including domestic criminal law.
National proceedings may also involve international crimes arising during armed conflicts. The July 25, 2025 decisions of the French Court of Cassation concerning Syria provide an important illustration of the procedural questions that can arise.
In case No. 24-84.393, the Court examined an arrest warrant issued against Bashar al-Assad in November 2023 in connection with allegations of complicity in crimes against humanity and war crimes arising from chemical attacks in Syria in August 2013.

The Court held that incumbent foreign heads of state benefit from personal immunity before French criminal courts under the applicable international law. It determined that the legality of an arrest warrant must be assessed according to the circumstances existing when the warrant was issued.
Because Assad was a serving head of state in November 2023, the Court annulled the warrant. It expressly indicated that this annulment did not determine the validity of a warrant issued after the individual had ceased to hold office.
The judgment did not decide Assad's criminal guilt or innocence. It addressed the procedural consequences of immunity at the time the warrant was issued.
In a separate decision delivered the same day, case No. 24-84.071, the Court addressed functional immunity for foreign state officials. It held that, subject to applicable treaty provisions, functional immunity could not be invoked to prevent proceedings concerning genocide, crimes against humanity, or war crimes.
These rulings illustrate the importance of distinguishing substantive criminal responsibility from jurisdiction and immunity. They do not establish a universal rule eliminating the personal immunity of serving heads of state before foreign national courts.
Evidence preservation is another essential part of accountability. The United Nations General Assembly established the International, Impartial and Independent Mechanism for Syria (IIIM) through Resolution 71/248 in December 2016.
The IIIM collects, consolidates, preserves, and analyzes evidence relating to serious international crimes committed in Syria since March 2011, with the objective of assisting competent criminal jurisdictions.
Its cooperation with the OPCW is particularly relevant to chemical weapons investigations. The institutions have established arrangements allowing the IIIM to access relevant OPCW material, including information collected through IIT investigations.
The IIIM is not a court and does not possess authority to conduct criminal trials. Its contribution lies in preserving evidence and supporting jurisdictions legally empowered to investigate and prosecute international crimes.

8. The Remaining Limits of Chemical Disarmament

The CWC has achieved exceptionally broad participation for an international disarmament treaty. As of November 2026, it has 193 States Parties, representing approximately 98 percent of the world's population.
Egypt, Israel, North Korea, and South Sudan remain outside full participation in the Convention. Israel has signed but not ratified the treaty, while the other three States have not joined. The continued absence of these States limits the Convention's universality. Their treaty positions differ from those of States Parties, although the customary prohibition on chemical weapons use during armed conflict remains applicable independently of CWC membership.
Undeclared chemical weapons programmes present another difficulty. Verification operates through national declarations, inspections, technical information, and other activities authorized by the Convention. Where States conceal facilities or materials, investigators may face substantial obstacles to establishing the full scale of prohibited activity.
Old and abandoned chemical weapons require continuing attention. They may present serious risks long after the conflicts or programmes responsible for their existence have ended. The Convention's provisions recognize that historical weapons can create ongoing obligations concerning identification, destruction, and international cooperation.
Non-state actors create additional security concerns. Chemical substances and relevant technical knowledge may be available through legitimate industries or

research institutions. Preventing diversion requires effective national legislation, export and transfer controls, law enforcement, and international cooperation.
Scientific and technological developments also affect verification. New chemical compounds, changes in production methods, and increasingly sophisticated industrial processes may complicate the identification of prohibited weapons development.
The CWC's general-purpose criterion permits its prohibitions to apply beyond an exhaustive list of named substances. Practical monitoring, however, still depends on scientific expertise, accurate national declarations, and adequate institutional resources.
The OPCW's continuing responsibilities consequently extend beyond stockpile destruction. They include industrial inspections, verification of outstanding declarations, assistance and protection, support for national implementation, and measures designed to prevent renewed chemical weapons production.
These responsibilities concern the practical capacity of States and international institutions to establish compliance and respond to evidence of prohibited activities. The underlying legal prohibition remains firmly established.

Conclusion

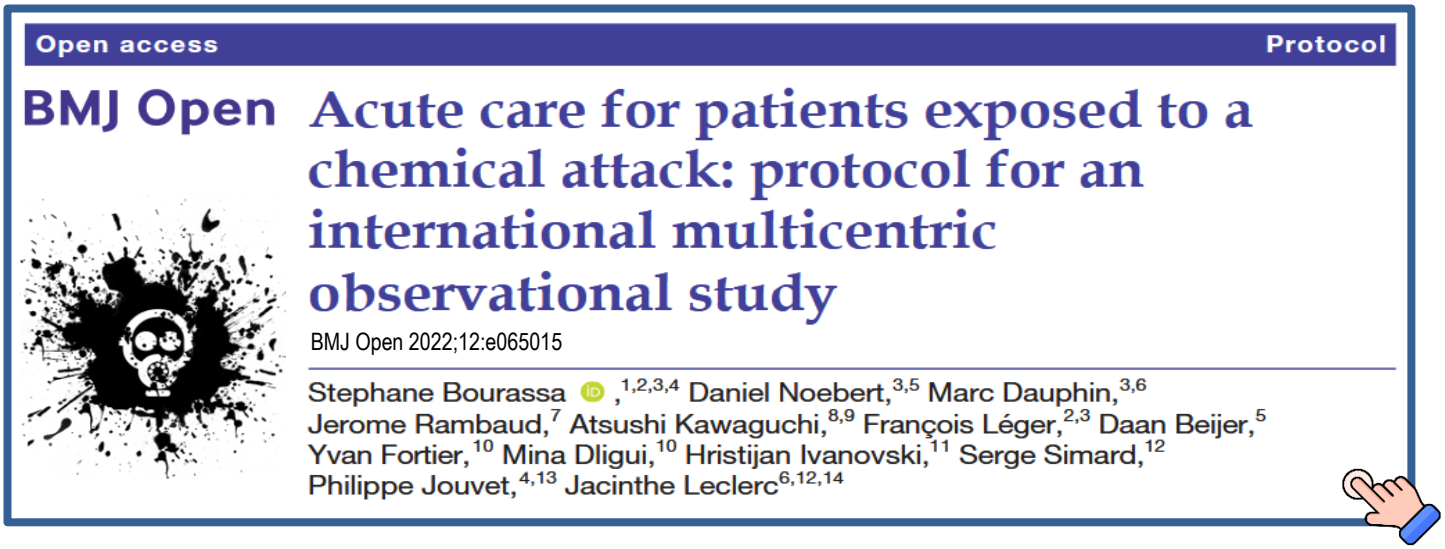
The prohibition of chemical weapons is firmly established in international law. The Chemical Weapons Convention provides a comprehensive treaty system governing their development, production, acquisition, transfer, possession, and use. Customary international humanitarian law independently prohibits chemical warfare in both international and non-international armed conflicts.
The OPCW gives practical effect to the Convention through declarations, inspections, technical verification, and investigations. Its confirmation in 2023 that all stockpiles declared up to that point had been destroyed represents a major achievement in international disarmament. Subsequent discoveries in Syria demonstrate why the elimination of declared weapons cannot be equated with complete assurance that no prohibited materials remain.
Accountability depends on further legal mechanisms. Treaty compliance procedures address States Parties' obligations, the law of state responsibility governs internationally wrongful conduct attributable to States, and criminal jurisdiction determines whether individuals may be prosecuted for particular offenses.
The Syrian investigations and subsequent judicial proceedings illustrate the limits of institutional attribution. Even where credible evidence identifies those responsible for chemical attacks, prosecution may depend on jurisdiction, immunity, the availability of admissible evidence, and the applicable criminal law.
The effectiveness of the international chemical weapons regime rests on maintaining the connection between a comprehensive legal prohibition, independent verification, and enforceable accountability. Each performs a distinct function. The existence of one does not guarantee the operation of the others, and the continuing elimination of chemical weapons depends on all three.

References

Amendment to Article 8 of the Rome Statute of the International Criminal Court (2010) Adopted at Kampala on 10 June 2010, entered into force on 26 September 2012. United Nations Treaty Series, vol. 2868, p. 195. Resolution RC/Res.5. Available at: https://treaties-prod.un.org/pages/ViewDetails.aspx?chapter=18&clang=_en&mtdsg_no=XVIII-10-a&src=TREATY (Accessed: 25 October 2026).
Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction (1992) Adopted on 3 September 1992, opened for signature on 13 January 1993, entered into force on 29 April 1997. United Nations Treaty Series, vol. 1975, p. 45. Available at: https://treaties.un.org/pages/ViewDetails.aspx?chapter=26&clang=_en&mtdsg_no=XXVI-3&src=TREATY (Accessed: 25 October 2026).

Cour de cassation (2025a) Pourvoi n° 24-84.071, Assemblée plénière, judgment of 25 July 2025, ECLI:FR:CCASS:2025:CR90684. Available at: https://www.courdecassation.fr/publications/bulletin-des-arrets-de-la-chambre-criminelle/numero-7-juillet-2025/immunite (Accessed: 25 October 2026).
Cour de cassation (2025b) Pourvoi n° 24-84.393, Assemblée plénière, judgment of 25 July 2025, ECLI:FR:CCASS:2025:CR90685. Available at: https://www.courdecassation.fr/publications/bulletin-des-arrets-de-la-chambre-criminelle/numero-7-juillet-2025/instruction (Accessed: 25 October 2026).
International Committee of the Red Cross (2005) 'Rule 74. Chemical Weapons', Customary International Humanitarian Law Database [online]. Available at: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule74 (Accessed: 25 October 2026).
International Criminal Court (2013) Elements of Crimes. The Hague: International Criminal Court. Available at: https://www.icc-cpi.int/sites/default/files/Publications/Elements-of-Crimes.pdf (Accessed: 25 October 2026).
International Criminal Tribunal for the Former Yugoslavia (1995) Prosecutor v. Duško Tadić, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Case No. IT-94-1-AR72, Appeals Chamber, 2 October 1995. Available at: https://cld.irmct.org/assets/Uploads/full-text-dec/1995/95-10-02%20Tadic%20Interlocutory%20Decision%20on%20Jurisdiction.pdf (Accessed: 1 November 2026).
International Law Commission (2001) Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries. Report of the International Law Commission on the Work of Its Fifty-Third Session, UN Doc. A/56/10, Chapter IV. Available at: https://legal.un.org/ilc/reports/2001/english/content.pdf (Accessed: 1 November 2026).
International, Impartial and Independent Mechanism (n.d.) Frequently Asked Questions [online]. United Nations. Available at: https://iiim.un.org/who-we-are/faqs/ (Accessed: 1 November 2026).
Organisation for the Prohibition of Chemical Weapons (2017) Chemical Weapons Incident in Kuala Lumpur, Malaysia. Executive Council Decision EC-84/DEC.8, 9 March 2017. Available at: https://www.opcw.org/sites/default/files/documents/EC/84/en/ec84dec08_e_.pdf (Accessed: 1 November 2026).
Organisation for the Prohibition of Chemical Weapons (2018) Addressing the Threat from Chemical Weapons Use. Conference of the States Parties Decision C-SS-4/DEC.3, 27 June 2018. Available at: https://www.opcw.org/documents/2018/06/c-ss-4dec3/decision-addressing-threat-chemical-weapons-use (Accessed: 1 November 2026).
Organisation for the Prohibition of Chemical Weapons (2021) Understanding Regarding the Aerosolised Use of Central Nervous System-Acting Chemicals for Law Enforcement Purposes. Conference of the States Parties Decision C-26/DEC.10, 1 December 2021. Available at: https://www.opcw.org/documents/2021/12/c-26dec10/decision-understanding-regarding-aerosolised-use-central-nervous-system (Accessed: 1 November 2026).
Organisation for the Prohibition of Chemical Weapons (2023a) OPCW Confirms: All Declared Chemical Weapons Stockpiles Verified as Irreversibly Destroyed [online]. 7 July 2023. Available at: https://www.opcw.org/media-centre/news/2023/07/opcw-confirms-all-declared-chemical-weapons-stockpiles-verified (Accessed: 1 November 2026).
Organisation for the Prohibition of Chemical Weapons (2023b) Third Report by the OPCW Investigation and Identification Team: Douma (Syrian Arab Republic), 7 April 2018. Note by the Technical Secretariat, S/2125/2023, 27 January 2023. Available at: https://www.opcw.org/sites/default/files/documents/2023/01/s-2125-2023%28e%29.pdf (Accessed: 1 November 2026).
Organisation for the Prohibition of Chemical Weapons (2024) Fourth Report by the OPCW Investigation and Identification Team: Marea (Syrian Arab Republic), 1 September 2015. Note by the Technical Secretariat, S/2255/2024, 22 February 2024. Available at: https://www.opcw.org/documents/2024/02/s22552024/note-technical-secretariat-fourth-report-opcw-investigation-and (Accessed: 1 November 2026).
Organisation for the Prohibition of Chemical Weapons (2025) OPCW Director-General Visits Syria; Meets with Syrian Caretaker Authorities to Discuss Next Steps in Eliminating Syria's Chemical Weapons Programme [online]. 8 February 2025. Available at: https://www.opcw.org/media-centre/news/2025/02/opcw-director-general-visits-syria-meets-syrian-caretaker-authorities (Accessed: 1 November 2026).
Organisation for the Prohibition of Chemical Weapons (2026a) Deployment of OPCW Expert Team to Syrian Arab Republic Finds Chemical Weapons Previously Undeclared to the Organisation [online]. 27 May 2026. Available at: https://www.opcw.org/media-centre/news/2026/05/deployment-opcw-expert-team-syrian-arab-republic-finds-chemical-weapons (Accessed: 1 November 2026).
Organisation for the Prohibition of Chemical Weapons (2026b) Fifth Report by the OPCW Investigation and Identification Team: Kafr Zeita (Syrian Arab Republic), 1 October 2016. Note by the Technical Secretariat, S/2478/2026, 21 January 2026. Available at: https://www.opcw.org/sites/default/files/documents/2026/01/s-2478-2026%28e%29.pdf (Accessed: 1 November 2026).
Organisation for the Prohibition of Chemical Weapons (2026c) Keynote Address by OPCW Deputy Director-General H.E. Mrs Mekondjo Kaapanda-Girnus at Annual OPCW-Asser Training Programme on Disarmament and Non-Proliferation of Weapons of Mass Destruction [online].

26 October 2026. Available at: https://www.opcw.org/media-centre/speeches-statements/2026/10/keynote-address-opcw-deputy-director-general-he-mrs (Accessed: 1 November 2026).
Organisation for the Prohibition of Chemical Weapons (2026d) OPCW by the Numbers [online]. Statistics updated to 30 September 2026. Available at: https://www.opcw.org/media-centre/opcw-numbers (Accessed: 1 November 2026).
Organisation for the Prohibition of Chemical Weapons (2026e) Reinstatement of the Rights and Privileges of the Syrian Arab Republic Under the Chemical Weapons Convention. Executive Council Decision EC-112/DEC.7, 9 July 2026. Available at: https://www.opcw.org/sites/default/files/documents/2026/07/ec112dec07%28e%29.pdf (Accessed: 1 November 2026).
Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare (1925) Signed at Geneva on 17 June 1925, entered into force on 9 May 1926. League of Nations Treaty Series, vol. 94, p. 65. Available at: https://treaties.un.org/pages/showdetails.aspx?objid=0800000280167ca8 (Accessed: 1 November 2026).
Rome Statute of the International Criminal Court (1998) Adopted at Rome on 17 July 1998, entered into force on 1 July 2002. United Nations Treaty Series, vol. 2187, p. 3. Available at: https://legal.un.org/ilc/texts/instruments/english/conventions/7_4_1998.pdf (Accessed: 1 November 2026).
United Nations General Assembly (2016) International, Impartial and Independent Mechanism to Assist in the Investigation and Prosecution of Persons Responsible for the Most Serious Crimes under International Law Committed in the Syrian Arab Republic since March 2011. Resolution 71/248, UN Doc. A/RES/71/248, adopted 21 December 2016. Available at: https://digitallibrary.un.org/record/856708/files/A_RES_71_248-EN.pdf (Accessed: 1 November 2026).
United Nations Secretary-General (2013) Report of the United Nations Mission to Investigate Allegations of the Use of Chemical Weapons in the Syrian Arab Republic on the Alleged Use of Chemical Weapons in the Ghouta Area of Damascus on 21 August 2013. UN Docs. A/67/997–S/2013/553, 16 September 2013. Available at: https://digitallibrary.un.org/record/756814/files/A_67_997%26S_2013_553-EN.pdf (Accessed: 1 November 2026).
United Nations Security Council (2004) Resolution 1540 (2004). UN Doc. S/RES/1540(2004), 28 April 2004. Available at: https://digitallibrary.un.org/record/520326 (Accessed: 2 November 2026).
United Nations Security Council (2013) Resolution 2118 (2013). UN Doc. S/RES/2118(2013), 27 September 2013. Available at: https://digitallibrary.un.org/record/757830 (Accessed: 2 November 2026).
United Nations Security Council (2015) Resolution 2235 (2015). UN Doc. S/RES/2235(2015), 7 August 2015. Available at: https://digitallibrary.un.org/record/798722 (Accessed: 2 November 2026).
Vienna Convention on the Law of Treaties (1969) Adopted on 22 May 1969, opened for signature at Vienna on 23 May 1969, entered into force on 27 January 1980. United Nations Treaty Series, vol. 1155, p. 331. Available at: https://treaties.un.org/pages/ViewDetailsIII.aspx?chapter=23&mtdsg_no=XXIII-1&src=IND (Accessed: 2 November 2026).


Open access Protocol

BMJ Open

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

BMJ Open 2022;12:e065015

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

STRENGTHS AND LIMITATIONS OF THIS STUDY

⇒ The pioneering methods used in the measurement of medical responses in the contaminated area after a chemical attack—a topic that, to date to our knowledge, has not been studied thoroughly. The zone of interest consists of the interventions taking place in prehospital settings, beginning at the incident site and ending at the patient's transfer to a clean zone.

⇒ The interventions assessed in this study are based on three key integrated competences, namely, (1) protection (for the staff and the patients), (2) decontamination (immediate and specialised (medical decontamination)) and (3) medical interventions.

⇒ The inclusion of both civilian and military healthcare resources in the study.

⇒ Issues raised by authorities around the world restricting access to data may adversely affect this study.

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.

Ethics and dissemination The Sainte-Justine Research Centre Ethics Committee approved this multicentric study and is acting as the main evaluating centre. Study results will be disseminated through various means, including conferences, indexed publications in medical databases and social media.

Disaster Medicine and Public Health Preparedness

www.cambridge.org/dmp

Radiation and Chemical Program Research for Multi-Utility and Repurposed Countermeasures: A US Department of Health and Human Services Agencies Perspective

Commentary

Cite this article: Rios CI, Garcia EE, Hogdahl TS II, *et al*. Radiation and chemical program research for multi-utility and repurposed countermeasures: A US Department of Health and Human Services agencies perspective. *Disaster Med Public Health Prep*. **18**(e35), 1–11. doi: https://doi.org/10.1017/dmp.2023.226.

Keywords:
Chemical and Radiological Threats; Sulfur Mustard; Skin and lung injury; Medical countermeasures

Corresponding author:
Carmen I. Rios; Email: carmen.rios@nih.gov

Carmen I. Rios PhD[1], Efrain E. Garcia PhD[2], Thomas S. Hogdahl II BS[3], Mary J. Homer PhD[4], Narayan V. Iyer PhD[3], Judith W. Laney PhD[2], Shannon G. Loelius PhD[4], Merriline M. Satyamitra PhD[1] and Andrea L. DiCarlo PhD[1]

[1]Radiation and Nuclear Countermeasures Program (RNCP), National Institute of Allergy and Infectious Diseases (NIAID), National Institutes of Health (NIH), US Department of Health and Human Services (HHS), Washington, DC, USA; [2]Chemical Medical Countermeasures (MCM) Program, Biomedical Advanced Research and Development Authority (BARDA), Administration for Strategic Preparedness and Response (ASPR), Washington, DC, USA; [3]Burn/Blast MCM Program, Biomedical Advanced Research and Development Authority (BARDA), Administration for Strategic Preparedness and Response (ASPR), Washington, DC, USA and [4]Radiological/Nuclear MCM Program, Division of Chemical, Biological, Radiological, and Nuclear Medical Countermeasures, Biomedical Advanced Research and Development Authority (BARDA), Administration for Strategic Preparedness and Response (ASPR), HHS, Washington, DC, USA

Abstract
Although chemical and radiological agents cause toxicity through different mechanisms, the multiorgan injuries caused by these threats share similarities that convene on the level of basic biological responses. This publication will discuss these areas of convergence and explore "multi-utility" approaches that could be leveraged to address common injury mechanisms underlying actions of chemical and radiological agents in a threat-agnostic manner. In addition, we will provide an overview of the current state of radiological and chemical threat research, discuss the US Government's efforts toward medical preparedness, and identify potential areas for collaboration geared toward enhancing preparedness and response against radiological and chemical threats. We also will discuss previous regulatory experience to provide insight on how to navigate regulatory paths for US Food and Drug Administration (FDA) approval/licensure/ clearance for products addressing chemical or radiological/nuclear threats. This publication follows a 2022 trans-agency meeting titled, "Overlapping Science in Radiation and Sulfur Mustard Exposures of Skin and Lung: Consideration of Models, Mechanisms, Organ Systems, and Medical Countermeasures," sponsored by the National Institute of Allergy and Infectious Diseases (NIAID), a part of the National Institutes of Health (NIH). Discussions from this meeting explored the overlapping nature of radiation and chemical injury and spurred increased interest in how preparedness for one threat leads to preparedness for the other. Herein, subject matter experts from the NIAID and the Biomedical Advanced Research and Development Authority (BARDA), a part of the Administration for Strategic Preparedness and Response (ASPR), summarize the knowledge gained from recently funded biomedical research, as well as insights from the 2022 meeting. These topics include identification of common areas for collaboration, potential use of biomarkers of injury to identify injuries caused by both hazards, and common and widely available treatments that could treat damage caused by radiological or chemical threats.

Delivering Chemical Warfare Agent Antidotes with Unmanned Aerial Vehicles (UAVs) at the Incident Site

The Editor

The rapid delivery of medical countermeasures (MCMs) to casualties during a chemical warfare agent (CWA) incident represents one of the most challenging aspects of prehospital CBRN medical response. In particular, incidents involving nerve agents, such as sarin (GB), soman (GD), tabun (GA), VX and other organophosphorus compounds, require immediate recognition and timely administration of appropriate antidotes. Delays in treatment can substantially increase morbidity and mortality, particularly when large numbers of casualties are involved.

Conventional emergency medical services may encounter considerable difficulties reaching the point of exposure. These include inaccessible terrain, road congestion, damaged infrastructure, security restrictions, the presence of an active chemical hazard, and the requirement to establish Hot, Warm and Cold Zones. Furthermore, medical personnel may be unable to approach casualties before appropriate respiratory and dermal protection is available. These circumstances create a potential operational role for unmanned aerial vehicles (UAVs), which could transport antidotes and other essential medical supplies directly to designated locations within or adjacent to the incident area.

The application of UAVs in emergency medical logistics is no longer purely theoretical. Their use for transporting blood products, medications, automated external defibrillators (AEDs) and emergency equipment has been investigated in several countries. However, the specific application of delivering CWA

antidotes to contaminated incident sites remains insufficiently developed and validated. The central question is not simply whether a drone can carry an antidote, but whether it can deliver the correct medical countermeasure, intact and accessible, to the correct location, within a clinically meaningful timeframe, without creating additional risks for casualties or responders.

Medical countermeasures and delivery requirements

The selection of the medical payload must be based on the suspected chemical agent, the clinical presentation and the applicable national medical protocols. There is no universal antidote applicable to all CWAs.

For nerve agent poisoning, the principal medical countermeasures include atropine, oximes such as pralidoxime or obidoxime, and benzodiazepines such as diazepam or midazolam for seizure management. Depending on national authorization and operational doctrine, these substances may be available in individual or combined autoinjectors.

The European Medicines Agency (EMA), in its 2024 guidance document[9], Guidance on the use of medicinal products for treatment in case of exposure to chemical agents used as weapons of terrorism, crime, or warfare, provides particularly relevant information concerning available antidotes, autoinjectors, indications and limitations. It identifies several products authorized in European countries, including Ineurope, Trobigard, Rafaject and IZAS-05, as well as the US-approved DuoDote product.

The delivery system should therefore accommodate different types of medical packages rather than being designed around a single antidote. Particular attention should be paid to the dimensions, weight, packaging, storage conditions, temperature sensitivity and mechanical protection of autoinjectors.

An important distinction is necessary: UAV delivery should not be confused with automated antidote administration. The immediate operational objective should be to deliver a clearly identifiable medical package to a casualty or, preferably, to a trained responder who can assess the patient and administer the appropriate treatment. Direct injection by an autonomous flying platform would introduce substantial clinical, ethical and technical problems and should not be considered an established capability.

The EMA guidance also highlights the limitations of adult autoinjectors in paediatric casualties, particularly the difficulties associated with fixed-dose preparations. Consequently, a UAV-based medical delivery system should not assume that every casualty can receive an identical antidote package.

Available UAV delivery technologies and commercial solutions

Several technological approaches are currently available for transporting and releasing small medical packages. They include dedicated cargo UAVs, externally mounted payload-release mechanisms, parachute-assisted delivery, winch systems and enclosed delivery containers.

Although these technologies have been developed primarily for rescue, logistics, industrial and humanitarian applications, many could potentially be adapted for CBRN medical response.

[9] EMA guidance document on the use of medicinal productsfor treatment in case of exposure to chemical agents used as weapons of terrorism, crime, or warfare. EMA (July 12, 2024). Available from https://www.ema.europa.eu/system/files/documents/regulatory-procedural-guideline/ema-guidance-document-use-medicinal-products-treatment-case-exposure-chem_en.pdf

Multi-rotor UAVs with payload-release mechanisms

One of the most accessible solutions is the use of commercially available multi-rotor UAVs equipped with dedicated payload-release devices.

An example is the Chinese manufacturer CZI and its TH4 V2 payload-release system[10]. The manufacturer specifies compatibility with DJI M400, M350 and M300 platforms through the DJI SkyPort V2.0 interface. The device weighs approximately 310 g and provides four individual release positions. Its stated single-head payload limit is up to 620 g on the M300 RTK and 650 g on the M350 RTK under the specified mounting configuration.



The system is particularly interesting for CBRN applications because it permits multiple small packages to be carried and released during a single flight.

A larger alternative is the CZI TD40/TD40P material dispenser, designed for DJI T40/T20 platforms. According to the manufacturer, it supports four or eight release positions, depending on configuration, and a total stated payload capacity of 40 or 80 kg respectively. Each individual release position can carry up to 10 kg, subject to the aircraft's actual payload limitations.

These devices demonstrate that multi-package aerial delivery is commercially available. However, their advertised payload capacity should not be interpreted as evidence of suitability for medical antidote delivery in a contaminated environment. The latter requires additional validation concerning package integrity, release accuracy, contamination protection and clinical accessibility.

Cone-shaped and enclosed delivery containers









An alternative approach involves the use of enclosed delivery containers, including capsule-shaped or cone-shaped packages.

The attraction of such designs is their potential to protect the medical payload during flight and delivery, while providing a clearly identifiable package that can be retrieved by a casualty or responder. A cone-shaped container may offer aerodynamic advantages compared with an

[10] https://www.czi.com.cn/en/product-detail/common

irregularly shaped package, depending on its orientation and design. It may also be easier to identify and retrieve if equipped with a contrasting colour, reflective markings or an external handle.
Chinese UAV manufacturers and developers have introduced various rescue-material release and delivery mechanisms. For example, Chinese patents describe cylindrical and compartmentalized UAV-mounted containers designed for sequential release of rescue supplies[11].
It is important, however, to distinguish between an actual commercially marketed product and a patented or experimental concept. I could not verify a specific commercially established product marketed under the exact designation drone cone for CWA antidote delivery. Therefore, cone-shaped delivery should be considered a potentially useful design approach rather than an already validated CBRN medical delivery solution.
For CWA applications, the enclosed container should ideally provide impact protection, moisture resistance, secure closure, tamper evidence and protection against external contamination. It should also permit retrieval without requiring the recipient to handle potentially contaminated external surfaces unnecessarily.

Winch and tethered delivery systems
Winch-based delivery is arguably one of the most promising approaches for CBRN medical applications.



DJI Matrice 350 with MT20 winch and medical cargo box

Instead of releasing a package from altitude, the UAV remains airborne while lowering the payload using a cable or electrically operated winch. The package is subsequently released or retrieved by a person on the ground.
This approach offers several advantages. It avoids the impact associated with free-fall delivery, reduces the possibility of damaging fragile medical equipment and allows delivery to locations where landing is impossible or undesirable. It may also permit more precise placement between buildings, vehicles, vegetation or other obstacles.
Evidence from medical UAV research supports the feasibility of this approach. A 2024 review by Surman and Lockey, Unmanned aerial vehicles and pre-hospital emergency medicine, examines the potential of UAVs for transporting medications and medical equipment in prehospital environments[12].
The limitations include cable oscillation, entanglement with structures, additional energy consumption, payload instability and the possibility that the tether may become contaminated if it enters the hazardous area.

[11] https://patents.google.com/patent/CN117429607A/zh
[12] K. Surman, and D. Lockey. Unmanned aerial vehicles and pre-hospital emergency medicine. *Scand J Trauma Resusc Emerg Med* 32, 9 (2024). Available from https://link.springer.com/article/10.1186/s13049-024-01180-7

For CBRN operations, the winch mechanism should ideally be designed to release the package without requiring the aircraft itself to descend into the contaminated zone.

Parachute-assisted delivery

Parachute-assisted delivery is another available technological approach. A medical package is released from the UAV and descends using a small parachute or controlled descent system.



Its main advantage is that the aircraft can maintain a greater separation from the ground and avoid landing in an unsafe environment.

ParaZero Technologies has successfully completed a groundbreaking IDF field trial of its DropAir system for precision delivery of blood transfusions.

However, parachute deployment introduces important limitations. Wind, turbulence, thermal currents and the aerodynamic characteristics of the package can produce significant deviations from the intended landing point. A parachute can also become entangled in trees, power lines, buildings or other structures.

These limitations are particularly relevant in an urban CBRN incident, where casualties may be surrounded by buildings, vehicles, debris and emergency response equipment.

A further concern is the possibility of the package landing in the wrong contamination zone. Delivery accuracy is therefore as important as flight accuracy.

Dedicated medical-delivery UAVs

Dedicated cargo UAVs provide another option. Unlike small commercial quadcopters equipped with release mechanisms, these platforms are specifically designed to transport medical supplies or other relatively substantial payloads. Two Chinese examples illustrate the progress of this market.

In June 2025, Shanghai reported a medical-equipment delivery demonstration using an ARK 40 octocopter at the Fudan University Shanghai Cancer Center[13]. The aircraft incorporated visual navigation, millimetre-wave radar and real-time kinematic (RTK) positioning. The delivery took approximately ten minutes.



[13] https://english.shanghai.gov.cn/en-Latest-WhatsNew/20250702/2b32070fd8774b8495ee8b409c6b5ba0.html



Another example is the TR9S, used in a medical supply delivery demonstration in Chongqing [14] in May 2025. The reported aircraft payload capacity was 9 kg, with a maximum stated range of 30 km without cargo and 20 km when fully loaded. A 12 km medical supply route was completed in approximately 19 minutes.

These examples demonstrate that dedicated medical cargo UAVs are moving beyond laboratory experimentation towards practical logistics applications. Nevertheless, hospital-to-hospital delivery is operationally different from delivering antidotes to casualties in a contaminated environment.

Comparative assessment of delivery methods

The following comparison considers their potential suitability for CBRN medical operations rather than simply their commercial availability.

Delivery method	Principal advantage	Principal limitation
Multi-position release device	Multiple packages per flight	Limited individual payload
Enclosed capsule/cone	Package protection and identification	Impact and retrieval issues
Winch/tether	Controlled placement without landing	Cable entanglement and contamination
Parachute	Separation between UAV and ground	Wind-dependent accuracy
Dedicated cargo UAV	Greater payload capacity	Size, cost and operational restrictions
UAV landing	Direct package accessibility	Requires safe landing area

A particularly interesting possibility would be combining two technologies: a dedicated medical UAV equipped with an enclosed, impact-resistant capsule and a controlled winch-release mechanism. Such a configuration could provide better protection for the medical countermeasures while minimizing the need for the aircraft to approach the contaminated surface.

Advantages of UAV-delivered antidotes in CBRN incidents

The most important advantage is the potential reduction in the time required to make medical countermeasures available at the incident site. During a nerve agent attack, casualties may deteriorate rapidly. In situations where access is restricted, the ability to deliver autoinjectors to an isolated casualty or a forward medical team could provide an important additional capability.

[14] https://english.liangjiang.gov.cn/2025-05/15/c_1093547.htm

A second advantage is the reduction of unnecessary responder exposure. Medical personnel would not necessarily have to enter the hazardous area simply to transport a small medical package. This is particularly relevant in incidents involving large contaminated areas, inaccessible locations or potentially continuing chemical releases.
A third advantage is the possibility of supporting multiple delivery points during a single mission. Multi-position release systems could carry separate medical packages for different casualty collection points or designated response teams.
UAVs could also be integrated into a wider CBRN reconnaissance and situational-awareness system. An aircraft carrying thermal imaging, optical cameras and suitable chemical detection equipment could support incident assessment while another aircraft performs medical delivery. These functions should preferably be allocated to separate aircraft when the payload or mission requirements would compromise performance.
Finally, UAV delivery could be particularly useful in situations where conventional ground access is obstructed, including collapsed infrastructure, industrial accidents, transport incidents, maritime emergencies and large-scale terrorist attacks.
The 2025 systematic review by Zhang and colleagues[15] on UAVs in prehospital emergency care provides a broader overview of the growing medical applications and the associated technical and operational challenges.

Navigation, positioning and delivery accuracy

Navigation is arguably one of the most critical challenges when considering the use of UAVs for antidote delivery at CBRN incident sites.
The aircraft must reach a specific delivery point, potentially within a complex urban or industrial environment, while maintaining a safe distance from the contaminated area and avoiding obstacles. Conventional UAV navigation relies heavily on Global Navigation Satellite Systems (GNSS)[16], including GPS, Galileo and other satellite positioning services. Although these systems provide satisfactory accuracy under normal circumstances, their reliability cannot be assumed in every emergency environment.
Buildings, tunnels, industrial structures and underground infrastructure may interfere with satellite signals. In addition, deliberate GNSS jamming or spoofing could compromise navigation during a terrorist incident or military operation.
A robust CBRN delivery platform should therefore combine several navigation technologies. These may include GNSS and RTK positioning, inertial navigation systems (INS), visual positioning, optical flow, LiDAR and millimetre-wave radar.
RTK can provide centimetre-level positioning under appropriate operating conditions, but it depends on reliable satellite observations and correction data. It should not be treated as an independent solution for GNSS-denied operations.
Visual navigation and LiDAR may support obstacle avoidance and local positioning where satellite coverage is poor. However, smoke, dust, darkness, reflective surfaces and poor visibility can reduce their effectiveness.

[15] Y. Zhang, J. Cao and S. Ye (2026). Unmanned aerial vehicles in prehospital emergency care: current evidence, technological advances, and future perspectives. Front. Public Health 13:1739160. Available from https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2025.1739160/full
[16] https://www.gps.gov/other-global-navigation-satellite-systems-gnss

The use of autonomous navigation becomes particularly important when operating in an environment where the remote pilot has limited direct visibility of the aircraft or delivery point.
A relevant 2025 study by Hussain and colleagues, published in the Journal of Field Robotics, examines autonomous aerial transport in a marine GNSS-denied environment[17]. Although its operational setting is different, it illustrates the importance of alternative navigation techniques in environments where conventional satellite positioning is unreliable.
Delivery accuracy presents a separate challenge from navigation accuracy. An aircraft may reach its intended coordinates without successfully delivering the package to the casualty. Wind, rotor downwash, package oscillation, release timing and the movement of the aircraft can all influence the final delivery position.
This distinction is particularly important when delivering antidotes to individual casualties rather than to a general casualty collection point.
For this reason, the preferred operational approach would involve delivery to a designated, clearly identifiable landing or retrieval area, rather than attempting to drop packages directly onto individual patients.

Environmental and operational challenges

Chemical contamination and rotor downwash

One of the most important considerations is the effect of rotor downwash on contaminated surfaces. Multi-rotor UAVs generate considerable downward airflow. When operating close to a contaminated surface, this airflow may redistribute contaminated dust, droplets or other particulate material, depending on the characteristics of the agent and the environmental conditions.
This could potentially increase secondary contamination or interfere with the work of decontamination teams. Accordingly, UAVs should not automatically be considered safe simply because they are unmanned. Their flight profile, operating altitude and delivery mechanism must be evaluated in relation to the contamination characteristics. Where possible, delivery should take place from a position that minimizes disturbance of contaminated material.

Weather and visibility

Wind is a major limitation, particularly for parachute and free-release systems. Strong crosswinds can affect the aircraft's stability and produce substantial package displacement.
Rain, fog, dust and smoke may also interfere with sensors and navigation systems. Low temperatures can reduce battery performance, while high temperatures may affect both battery operation and pharmaceutical storage conditions.

Battery endurance and payload

The relationship between payload and flight endurance must also be considered. Increasing the weight of the medical package, release mechanism and protective container reduces the available flight time. The problem becomes more significant when the aircraft must maintain a safe reserve of energy for its return journey.
A further challenge is the need to carry sufficient antidote supplies for multiple casualties without exceeding the aircraft's maximum payload.

[17] J. Sun, Z. Niu, Y. Dong, et al. (2025). An Aerial Transport System in Marine GNSS-Denied Environment. *Journal of Field Robotics*, *42*(5), pp.2192-2217. Available from https://onlinelibrary.wiley.com/doi/10.1002/rob.22520

Contamination of the UAV
An aircraft operating inside or close to a contaminated area may itself become contaminated.
This creates problems concerning its subsequent recovery, maintenance, battery replacement, transportation and reuse. It may also create a secondary contamination risk for operators and other response personnel. For this reason, disposable or replaceable external delivery containers, dedicated CBRN UAVs and appropriate post-mission decontamination arrangements should be considered.

Communication and command integration
A further problem concerns the integration of UAV operations into the incident command structure.
The UAV operator must receive accurate information concerning the location of casualties, the boundaries of the Hot and Warm Zones, changing meteorological conditions and any restrictions imposed by other aircraft or emergency operations.
A medical delivery UAV should therefore operate under an established tasking and coordination mechanism rather than independently selecting delivery locations.

Regulatory, medical and safety considerations

The deployment of UAVs for CBRN medical delivery in Europe must take account of the European Union regulatory framework for unmanned aircraft.
Under Commission Implementing Regulation (EU) 2019/947, operations are classified according to their operational risk. The Open category does not permit dropping material, flying over assemblies of people or transporting dangerous goods. Consequently, an emergency antidote-delivery operation cannot simply be treated as an ordinary recreational or commercial drone flight.
The Specific category may be relevant, subject to the applicable operational authorization and risk assessment. Operations involving dangerous goods that could cause harm in the event of an accident may require the Certified category.
The applicable provisions and operational requirements are available through the European Union Aviation Safety Agency (EASA) – Easy Access Rules for Unmanned Aircraft Systems[18].
Medical considerations are equally important. Antidotes must be transported under conditions that preserve their pharmaceutical integrity. Temperature monitoring, protection from direct sunlight, mechanical protection and appropriate packaging must be incorporated into the delivery system.
There must also be a clear chain of custody and identification. The receiving responder should be able to establish the contents, expiry date, batch number and intended clinical application of each package.
Finally, the system must be compatible with existing CBRN medical procedures. UAV delivery cannot replace casualty triage, clinical assessment, appropriate PPE, decontamination or professional administration of antidotes.

A proposed operational concept for CBRN antidote delivery

A practical approach would involve establishing a dedicated UAV medical-delivery capability within the CBRN response organization.

[18] EASA eRules: aviation rules for the 21st century. Available from https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-unmanned-aircraft-systems



The system could consist of a forward medical supply station located in the Cold Zone, a UAV equipped with a protected medical container and a command-and-control arrangement linking the UAV operator with the CBRN medical team.
Upon identification of casualties requiring urgent medical countermeasures, the medical command element would request a delivery mission. The package would be selected according to the suspected agent and the approved medical protocol.
The UAV would then transport the package to a predetermined retrieval point, preferably outside the area of highest contamination. Where direct access is impossible, an appropriately validated winch or controlled-release system could be employed.
A responder or designated casualty would retrieve the package. The receiving team would verify its contents and administer the appropriate treatment according to clinical protocols.
An important additional capability would be the use of a two-way communication system. The UAV could carry a small communication device, allowing the casualty or a responder to communicate with the medical team and receive instructions concerning retrieval and subsequent treatment.
The system could also incorporate a delivery confirmation mechanism, providing the command centre with information about the aircraft's position, package release, successful retrieval and mission completion. An important operational distinction is that the UAV should deliver medical countermeasures, not make clinical decisions. Agent identification, antidote selection and treatment decisions must remain under the responsibility of appropriately trained medical personnel.

Future developments: integration with autonomous CBRN systems

The future potential of UAV medical delivery extends beyond the transportation of antidotes.
An integrated system could combine aerial reconnaissance, chemical detection, casualty identification, medical supply delivery and robotic ground platforms.
A particularly interesting development is the integration of aerial and ground-based unmanned systems. A UAV could identify a casualty and deliver a medical package to a designated retrieval location, while an unmanned ground vehicle could subsequently transport medical equipment or support casualty evacuation.
A relevant development was published by Schmidbauer and colleagues in August 2026. Their paper, Proof-of-concept of an autonomous medical

evacuation system integrating ground and aerial unmanned platforms with robot-assisted patient care for military and civilian CBRN emergencies, describes an integrated approach involving aerial and ground transport, patient monitoring, telemedical communication and robotic intervention under human clinical supervision[19].
Although this system addresses a considerably broader capability than antidote delivery, it provides an interesting direction for future CBRN medical response development.
In particular, the combination of UAVs, autonomous ground vehicles and telemedicine could help overcome some of the limitations of conventional medical response in highly contaminated or inaccessible environments.



Conclusions

The delivery of CWA antidotes by UAVs represents a promising but insufficiently validated application of unmanned technology in CBRN emergency medicine. Commercially available payload-release mechanisms, enclosed containers, winch systems and dedicated medical cargo UAVs already provide several of the necessary technological components. Chinese manufacturers, particularly CZI, offer commercially available payload-release equipment that could be considered for experimental adaptation. The development of dedicated medical cargo platforms in China also demonstrates that UAV-based medical logistics is progressing towards operational implementation.
Nevertheless, the successful delivery of antidotes in a CWA incident requires considerably more than adequate payload capacity and flight range. Navigation reliability, GNSS-denied operation, package integrity, delivery accuracy, contamination control, rotor downwash, environmental conditions and regulatory compliance must all be addressed. Of the available approaches, a protected medical capsule delivered by a UAV using a controlled winch or release mechanism appears particularly promising. It could reduce the risks associated with free-fall delivery and minimize the need for the aircraft to approach contaminated surfaces. The most realistic initial application would be the delivery of nerve-agent autoinjectors to designated casualty collection points or forward CBRN medical teams. Subsequent development could involve larger medical packages and integration with autonomous ground-based systems.
Ultimately, UAVs should be considered an additional medical logistics capability within an integrated CBRN response system, rather than a replacement for conventional first responders or medical teams. The next essential step should be controlled field testing under simulated CBRN conditions, assessing delivery accuracy, package integrity, navigation reliability, retrieval time and the possibility of secondary contamination. Such testing would establish whether UAV-delivered antidotes can provide a measurable improvement in casualty management during real-world CWA incidents.

[19] W. Schmidbauer, C. Jänig, J. Backus, *et al.* Proof-of-concept of an autonomous medical evacuation system integrating ground and aerial unmanned platforms with robot-assisted patient care for military and civilian CBRN emergencies. *AS* (2026). Available from https://doi.org/10.1007/s42401-026-00531-9

CBRN Toolkit

Source: https://unicri.org/sites/default/files/2025-04/CBRN%20Toolkit.pdf



CBRN incidents, with their unpredictable and potentially catastrophic impacts, demand more than conventional emergency response mechanisms. Addressing these challenges requires advanced tools and frameworks that empower strategic-level decision-makers to navigate uncertainties and mitigate evolving risks. In this context, the Toolkit on effective CBRN planning and response for policymakers and CBRN managers emerges as an essential resource, offering a holistic and proactive approach rooted in advanced preparedness, strategic foresight, and collaborative action.

This comprehensive guide results from an extensive collaborative effort that brings together diverse expertise, rigorous research, field missions, and lessons learned from past incidents. Its development involved contributions from regional governments, international organizations such as WHO, IAEA, and OPCW, and local stakeholders across Southeast Asia and East Central Africa. Workshops held in Manila and Nairobi provided invaluable insights from practitioners in varied contexts, ensuring that the Toolkit addresses critical preparedness gaps and reflects the realities of managing CBRN risks on the ground.

What distinguishes this Toolkit is its recognition that effective CBRN management is not confined to rigid protocols but instead relies on the creation of dynamic, adaptive systems capable of responding to emerging and unpredictable challenges. Its two-part structure – first focusing on planning and then on response actions – underscores the critical importance of preparation as a foundation for effective crisis management.

Successful CBRN management begins long before an incident occurs, involving strategic planning, training, and the establishment of governance frameworks that enable rapid and coordinated responses.

For policymakers, emergency managers, and CBRN professionals, this Toolkit serves as a strategic companion, offering actionable guidance while simplifying complex processes. It stands as a testament to the necessity of collective preparedness in addressing risks that transcend borders.

This Toolkit is more than a reference document; it is a call to action for leaders at all levels to collaborate toward a safer, more secure future. It is with great pride and confidence that I commend this document to you, trusting it will serve as a valuable resource in strengthening CBRN preparedness and response.

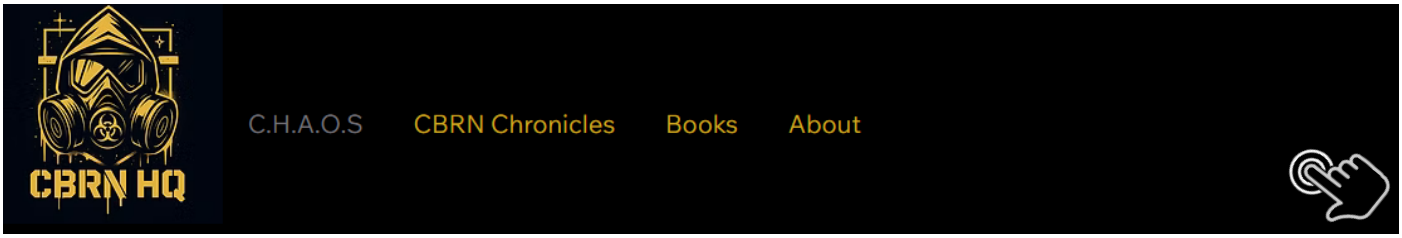
This initiative would not have been possible without the generous support and funding of the Bureau of International Security and Nonproliferation, Department of State of the United States of America. We extend our sincere gratitude for their invaluable contribution to this initiative.

Leif Villadsen
UNICRI Acting Director

Example of the risk matrix for various CBRN threats

THREAT	LIKELIHOOD (1–5)	IMPACT (1–5)	RISK SCORE (LIKELIHOOD X IMPACT)	DESCRIPTION
Chemical spill in a populated area	4	4	16	A spill of industrial chemicals (e.g., chlorine gas) due to equipment failure or sabotage in a densely populated urban area. Likely occurrence with major health and environmental impacts.
Theft of radiological material	3	3	9	Theft of radiological materials from poorly secured facilities. Moderate likelihood with localized health risks and potential public panic.
Biological attack with anthrax	2	5	10	Deliberate release of anthrax spores in a metropolitan area. Unlikely but catastrophic impact if it occurs, causing widespread fatalities and public health crises.
Improper disposal of radiological waste	2	3	6	Negligent disposal of radiological waste causing limited exposure in a rural area. Low likelihood and moderate localized impact.
Nuclear plant failure	1	5	5	Significant accident at a nuclear plant causing widespread radiation exposure. Very low likelihood due to stringent safety measures but catastrophic impact if it happens.

An interesting website



Yemen: Suspected Chemical Warfare Agents in Houthi Attacks

Source: https://euro-sd.com/2026/11/articles/armament/54529/yemen-chemical-warfare-houthi/

Nov 04 – International intelligence agencies are examining reports of the possible use of artillery shells containing toxic or chemical substances by the Houthis in Yemen. During attacks in Taiz Governorate in late October 2026, several people reportedly suffered from breathing difficulties, symptoms of suffocation and loss of consciousness. So far, no independent analysis of the ammunition used or the substances released has been conducted. According to the internationally recognised Yemeni government and military officials, Houthi forces used artillery shells in Taiz Governorate in late October that may have contained toxic or chemical substances. Reports indicate that civilians and combatants subsequently experienced respiratory problems, symptoms of suffocation and loss of consciousness. The allegations are currently under investigation. According to reports, local authorities in Taiz and the Yemeni armed forces have launched emergency investigations. At the same time, they have called on the United Nations and the Organisation for the Prohibition of Chemical Weapons (OPCW) to send experts to conduct an independent investigation.



Origin and Composition Remain Unclear

So far, there has been no independent confirmation of which substances were released during the alleged incidents. There is also no conclusive evidence as to whether the symptoms were actually caused by chemical warfare agents or whether such substances were contained in the artillery shells.

The origin of the suspected substances also remains unclear. A reliable assessment would require, among other things, forensic examinations of the ammunition and any possible chemical residues. The Houthi authorities and groups aligned with them have rejected the allegations or offered alternative explanations. According to their claims, industrial facilities or paint factories may have been responsible for releasing toxic substances. These facilities were allegedly hit during attacks by coalition forces or opposing troops.

USE OF CHEMICAL WEAPONS IN THE MIDDLE EAST

Across the region, some states and armed groups have reportedly used chemical weapons, including mustard gas, sarin, chlorine and phosgene

1963–67
EGYPT IN YEMEN
Egyptian forces bombed royalist-held villages during the North Yemen Civil War with chemical munitions, including mustard gas and phosgene

1980–88
SADDAM HUSSEIN'S IRAQ VS. IRAN
Iraqi forces used mustard gas and nerve agents, including tabun and sarin, against Iranian troops and civilians during the Iran–Iraq war. UN missions repeatedly confirmed the attacks

1987–88
SADDAM HUSSEIN'S IRAQ VS. KURDS
During the Anfal campaign, Iraq used chemical weapons against Kurdish villages. The 1988 Halabja attack killed an estimated 3,500–5,000 civilians and injured thousands more, resulting in long-term health consequences

1980–88
IRAN IN IRAQ
US and other sources reported that Iran have used limited quantities of mustard gas and cyanide against Iraqi troops late in the war, though Tehran denies this

1935–1936
Italy launched a massive chemical attack during the Second Italo-Ethiopian War.



2008–09
ISRAEL IN GAZA
Israel used white phosphorus munitions during its Gaza offensive. Classified as an incendiary weapon, white phosphorus can cause severe burns and fires and using it deliberately for its toxic or caustic effects against people could amount to chemical warfare

2011–2024
BASHAR ASSAD'S SYRIA IN CIVIL WAR
Assad's forces were implicated in repeated chemical attacks during the civil war, including the 2013 Ghouta sarin attack. UN investigators found "clear and convincing evidence" that sarin-filled rockets were used in the Syrian Arab Republic

2014–2017
DAESH IN IRAQ AND SYRIA
Daesh developed a rudimentary chemical program using chlorine and low-grade sulfur mustard, deploying them in dozens of attacks in Iraq and Syria, according to OPCW findings and other monitoring groups

2023–PRESENT
ISRAEL IN LEBANON
Human-rights groups and Lebanese authorities have accused Israel of using white phosphorus over souther Lebanon and spraying concentrated glyphosate herbicide above safety standards near border villages

Sources: OPCW, Human Rights Watch, WHO, Arab News

ARAB NEWS

The appeal to the UN and the OPCW aims to have the allegations investigated by independent experts. Only an analysis of the ammunition used, the residues and the medical findings could establish whether chemical substances were actually released and what caused the reported symptoms.

Until then, the alleged use of chemical warfare agents by the Houthis remains an unverified accusation. The alternative explanations put forward by Houthi-affiliated sources have likewise not been independently substantiated.

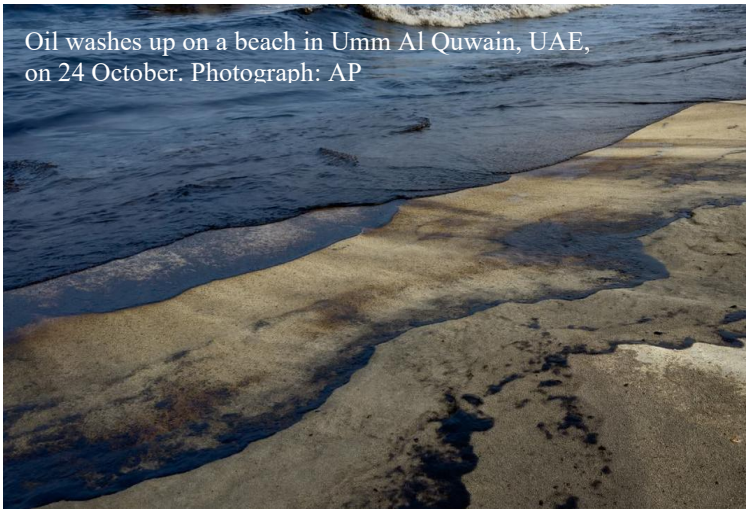
JCBRN Defense CoE publications



Many interesting CBRN topics are available (PDF format).

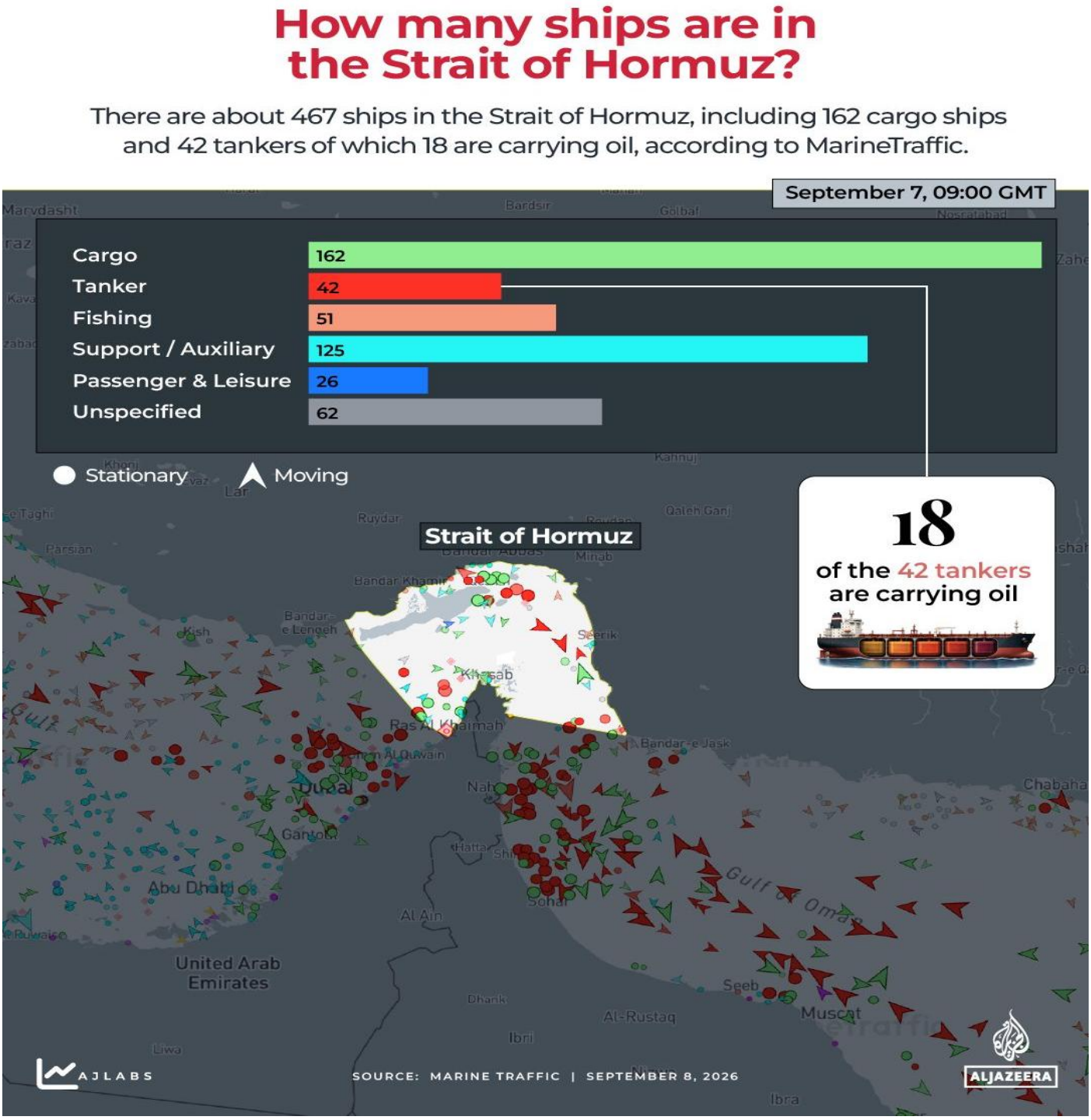
Marine Pollution in the Strait of Hormuz and the Persian Gulf: Tanker Attacks, Oil Spills and Threats to Desalination Infrastructure

By the Editor | Environmental and water-security assessment | November 2026


Oil washes up on a beach in Umm Al Quwain, UAE, on 24 October. Photograph: AP

The Strait of Hormuz and the wider Persian Gulf are experiencing a serious and growing marine pollution problem associated with the ongoing armed conflict and attacks on commercial shipping. Tankers struck by missiles, unidentified projectiles and reportedly naval mines have contributed to oil releases, while other maritime incidents have caused additional damage to the marine environment. Satellite observations published in November 2026 indicate that approximately **540 oil slicks** have been identified across the region since the conflict began in February. Greenpeace estimates that the affected marine area

extends to approximately 20,000 km². These figures demonstrate the scale of the pollution problem, although they do not establish that every detected slick resulted from a tanker attack[20].



[20] L. Tondo. Oil slicks seen from space: the devastating impact of boat strikes on fragile Gulf ecosystems. The Guardian (November 12, 2026). Available from https://www.theguardian.com/world/2026/nov/12/oil-slicks-seen-from-space-the-devastating-impact-of-boat-strikes-on-fragile-gulf-ecosystems

The environmental consequences extend beyond visible oil slicks. Hydrocarbon contamination can affect fish, seabirds, marine mammals and sea turtles through direct contact, ingestion and inhalation of volatile compounds. Particularly vulnerable habitats include coral reefs, mangroves, seagrass beds and coastal sediments, where pollutants may persist and cause long-term ecological damage. Contamination can also affect fisheries, seafood safety, tourism and the livelihoods of coastal communities. The semi-enclosed character of the Persian Gulf, its shallow waters and relatively restricted exchange with the open ocean increase concerns about the persistence and cumulative effects of pollution[21].

Threats to desalination plants and drinking-water security

One of the most consequential and potentially underestimated effects of marine pollution is its impact on seawater desalination infrastructure. The Gulf states depend heavily on desalination to provide drinking water, making the protection of seawater intakes a critical national-security and public-health priority. The United Arab Emirates, for example, obtains more than 80% of its potable water from desalination. Saudi Arabia, Kuwait, Qatar, Bahrain, Oman and Iran also rely substantially on desalinated seawater, although the degree of dependence varies between countries. Consequently, an oil spill that might otherwise be regarded as an environmental incident can develop into a serious water-security emergency[22].

Desalination plants are particularly vulnerable because they continuously draw large volumes of seawater through intake systems. If an oil slick approaches an intake, hydrocarbons may enter the pretreatment stages and interfere with filtration, coagulation and other treatment processes. Oil and associated organic contaminants can foul filters and membranes, impair reverse-osmosis performance, increase maintenance requirements and, under certain circumstances, damage sensitive equipment. Although modern treatment systems provide multiple barriers, they should not be regarded as an absolute guarantee against contamination. The appropriate response to a credible threat is early detection, assessment of the contaminant plume and, where necessary, precautionary suspension of seawater intake until conditions are considered safe[22].

A particularly relevant example emerged in October 2026, when an oil slick associated with the damaged tanker *Gem No. 2* raised concerns about the Naqa'a desalination plant near the border between Umm Al Quwain and Ras Al Khaimah in the UAE. Reuters reported that the slick had approached approximately two kilometers from the plant. Although authorities had not announced a shutdown, the incident demonstrated how an oil spill can threaten essential water infrastructure without physically damaging the facility itself. The proximity of the contamination to seawater intake was the principal concern[23].

[21] Alia Chughtai and Marium Ali. Why US-Iran war over Hormuz is threatening the Gulf's waters. Aljazeera (September 09, 2026). Available from https://www.aljazeera.com/news/2026/9/9/why-us-iran-war-over-hormuz-is-threatening-the-gulfs-waters

[22] N. Ramnauth, A. Culot, T. Dobbelaere, et al E. (2026). Oil spill vulnerability in the Arabian/Persian Gulf threatens regional water security and global energy supply. *Earth's Future*, 14, e2026EF008477. https://doi.org/10.1029/2026EF008477

[23] F. Maccioni. Explainer: How could the oil spill off the UAE coast affect desalination plants? Reuters (October 29, 2026). Available from https://www.reuters.com/legal/litigation/how-could-oil-spill-off-uae-coast-affect-desalination-plants-2026-10-29/

The consequences of a desalination plant shutdown could be substantial. Even a temporary interruption may reduce the availability of potable water, particularly where storage capacity is limited and alternative freshwater resources are scarce. Hospitals, emergency services, military installations, industrial facilities and densely populated urban areas could all be affected. In a prolonged crisis, authorities might have to introduce water rationing, mobilize emergency water supplies, transport potable water by tanker or activate interconnections with alternative supply systems. Simultaneous disruption of several plants could create a regional emergency, particularly if electricity supply, port operations and transport infrastructure were also affected.

Historical experience reinforces these concerns. During the 1991 Gulf War oil spill, desalination plants in Saudi Arabia and Kuwait were shut down because of the threat of contamination. A separate incident in Sharjah in 1997 involved diesel reaching a desalination plant's intake and contaminating the water supply of an estimated half a million people. These examples illustrate that marine pollution can translate directly into a drinking-water emergency.



Operational priorities and protective measures

Protection of desalination infrastructure should therefore be integrated into national CBRN, environmental emergency and critical-infrastructure protection plans. Continuous satellite surveillance, aerial monitoring, coastal sensors and oil-spill trajectory modelling should be used to identify contamination early and estimate its potential movement towards seawater intakes. Monitoring should include not only visible surface oil but also relevant water-quality parameters and chemical analyses of potentially contaminated seawater.

Desalination operators should establish predefined thresholds and procedures for restricting or suspending intake operations, supported by rapid communication with maritime authorities, environmental agencies and emergency-management organizations. Physical protection measures may include appropriately designed floating containment booms, intake protection systems and alternative intake arrangements where technically feasible. However, these measures must be selected according to the

characteristics of the spill, sea conditions and plant design. Emergency planning should also include alternative water supplies, strategic potable-water reserves, mutual assistance between neighboring jurisdictions and arrangements for prioritizing hospitals and other essential services.
Particular attention should be given to the possibility of multiple simultaneous incidents. A coordinated campaign against tankers, ports, oil terminals, power stations and desalination facilities could produce cascading effects involving marine pollution, electricity disruption, drinking-water shortages and public-health consequences. Such a scenario should be considered not simply as an environmental disaster but as a complex, cross-border critical-infrastructure emergency.

Conclusion

The pollution affecting the Strait of Hormuz and the Persian Gulf represents a serious environmental and strategic-security concern. The repeated damage to commercial vessels and the accumulation of oil slicks threaten marine ecosystems, fisheries and coastal communities. However, the potential disruption of desalination infrastructure may constitute an even more immediate threat to human security. In a region where drinking water production is heavily dependent on seawater desalination, the contamination of intake systems could turn a maritime incident into a major public-health and humanitarian emergency. The protection of desalination plants, continuous monitoring of seawater quality, rapid oil-spill response and regional coordination should therefore be treated as essential components of emergency preparedness.

CBRN Supply Chains: The Strategic Enablers Missing from Resilience

By Professor David Crouch and Natascha McVeigh

Source: https://www.rusi.org/explore-our-research/publications/commentary/cbrn-supply-chains-strategic-enablers-missing-resilience



Nov 16 – CBRN preparedness depends on dispersed supply chains. Resilience frameworks should recognise them as strategic enablers, even if they are not critical infrastructure. National resilience strategies place significant emphasis on protecting Critical National Infrastructure, recognising that disruption to essential services can have profound consequences for national security, public safety and economic stability. The UK Government Resilience Framework advocates a whole-of-society approach to resilience and highlights the need to understand systemic interdependencies that could affect national preparedness and response capability.

Recent events, including the Covid-19 pandemic, geopolitical instability and

global supply chain disruptions, have demonstrated how rapidly shortages of critical materials, components and specialised products can emerge. The strategic significance of resilience has been reinforced through the Integrated Review Refresh 2023, which emphasises the challenges posed by strategic competition, economic coercion and vulnerabilities associated with globally interconnected systems.

Increasingly, resilience debates are shifting from protecting individual assets towards understanding the interconnected networks that support national capability. Both the EU and NATO have recognised the growing importance of resilience across interconnected sectors, industrial ecosystems and supply networks. The EU's resilience framework specifically acknowledges that increasingly interconnected societies require resilience measures extending beyond the protection of individual infrastructure assets, while NATO emphasises that resilient civil systems are fundamental to both societal and military preparedness.

This challenge is particularly relevant in the CBRN (chemical, biological, radiological and nuclear) domain, where preparedness and response capabilities depend on complex, interconnected and often globally distributed industrial networks. An important policy question therefore emerges: should CBRN supply chains be considered critical infrastructure in their own right, or should they be recognised differently within resilience frameworks?

The answer may lie between these two positions. While CBRN supply chains may not fit traditional critical infrastructure definitions, they should be recognised as strategic enablers whose disruption could significantly degrade national preparedness, emergency response capability and operational resilience.

Invisible Dependencies

CBRN capability is often viewed through the lens of frontline assets, including detection equipment, respiratory protective equipment, medical countermeasures, specialist laboratories and decontamination systems. Yet these capabilities depend upon extensive supply chains that frequently remain outside national resilience discussions.

Modern CBRN systems are rarely manufactured within a single organisation or country. Their production relies upon specialist components, proprietary technologies, precursor chemicals, advanced electronics and niche manufacturing processes distributed across multiple suppliers and jurisdictions. In many cases, these supply chains contain hidden vulnerabilities arising from supplier concentration, limited manufacturing capacity, long lead times and reliance on overseas suppliers.

These risks are amplified because many CBRN products exist within relatively small and specialised markets. Unlike commercially competitive sectors characterised by significant redundancy, specialist CBRN equipment often depends on a limited number of suppliers possessing unique expertise, manufacturing capability or intellectual property. Should disruption occur, alternative sources may not exist or may require lengthy qualification processes before they become operationally viable.

As a result, vulnerabilities may emerge several tiers below the end user, creating resilience challenges that are difficult to identify through conventional procurement and assurance mechanisms. This concern is consistent with the National Risk Register, which identifies supply chain disruption, pandemics, cyber incidents and geopolitical instability as significant risks capable of affecting critical national functions.

The Semiconductor Example

Semiconductors provide a compelling illustration of this challenge. Many CBRN capabilities depend directly upon advanced electronics, including radiation detectors, chemical identification systems, bio-surveillance platforms, autonomous

monitoring technologies and secure communications networks.

However, semiconductor manufacturing relies upon highly complex international supply chains involving rare gases, ultrapure chemicals, specialist manufacturing equipment and globally dispersed production facilities. The OECD has noted that while globalisation has improved efficiency and reduced costs, it has also increased exposure to supplier concentration, systemic shocks and strategic dependencies within critical supply chains. An October 2026 analysis by the Semiconductor Industry Association highlights that semiconductor production depends upon a highly interconnected, multitiered global supply chain, with many critical vulnerabilities residing deep within upstream suppliers of materials, equipment and subcomponents. Recognising these dependencies, the US government has explicitly identified semiconductors as essential to national security, defence capability and critical infrastructure resilience. Modern military systems, communications networks, critical infrastructure and advanced security technologies all depend upon assured semiconductor availability.

The broader importance of supply chain security was also recognised in Executive Order 14017: America's Supply Chains, which identified resilient and diversified supply chains as essential for managing biological threats, geopolitical disruption and national security challenges.

For the CBRN community, the implications are significant. Semiconductor shortages may not initially appear to be a CBRN issue, yet they can directly affect the production, maintenance and sustainment of radiation detectors, chemical sensors and biological surveillance systems. The vulnerability therefore exists not solely within the CBRN sector itself, but within the broader industrial ecosystem upon which CBRN capability depends.

The resilience of a radiation detector may ultimately depend less on the detector manufacturer than on a global network of semiconductor fabricators, chemical producers and specialist component suppliers.

Strategic Vulnerabilities in the UK Context

The UK possesses significant expertise across defence, security and emergency preparedness. Nevertheless, many CBRN capabilities rely upon highly specialised industrial partners and international supply networks.

Detection technologies frequently incorporate globally sourced electronic components and sensors. Pharmaceutical countermeasures depend upon complex supply chains that support active pharmaceutical ingredients, precursor chemicals and specialist manufacturing processes. The UK Biological Security Strategy highlights the importance of maintaining resilient access to diagnostics, surveillance capabilities, medical countermeasures and supporting industrial capacity during emergencies.

Similarly, personal protective equipment (PPE), often considered a relatively straightforward commodity, demonstrated considerable vulnerability during the Covid-19 pandemic. The National Audit Office found that unprecedented global demand, export restrictions and disruption to international supply chains created significant challenges for the procurement and distribution of PPE despite existing stockpiles and contingency arrangements.

These experiences demonstrate that the resilience of national CBRN capability is closely linked to the resilience of underlying industrial systems. National preparedness may therefore depend as much upon the robustness of supply chains as upon the availability of frontline response assets.

Learning from International Practice

International organisations and governments are increasingly recognising the importance of supply chain security and strategic dependency management.

The NATO resilience agenda places growing emphasis on the role of civil preparedness, industrial capacity and interconnected support systems in maintaining operational effectiveness. NATO's resilience framework explicitly recognises that military capability depends upon broader societal and industrial resilience. Similarly, the EU's Directive (EU) 2022/2557 on the Resilience of Critical Entities reflects a shift away from protecting infrastructure assets in isolation towards understanding how interconnected systems support the delivery of essential services. The Directive acknowledges that increasingly interconnected societies require resilience measures extending beyond physical infrastructure protection alone.

Despite these developments, relatively little policy attention has focused specifically on CBRN-enabling supply chains. As a result, critical dependencies may remain poorly understood until they are exposed during periods of crisis.

From Vulnerability to Resilience

Recognising CBRN supply chains as strategic enablers should not necessarily result in their designation as critical infrastructure. Instead, it should encourage a more sophisticated approach to resilience management.

The first requirement is improved supply chain visibility. Many organisations understand their Tier 1 suppliers but possess only limited awareness of dependencies located further upstream. Mapping multitier supply chains would improve identification of chokepoints, concentration risks and strategic dependencies. Such an approach aligns with the principles of the UK Government Resilience Framework, which emphasises anticipation, preparedness, adaptation and the management of cross-sector interdependencies. Second, resilience planning should extend beyond stockpiling finished products. While strategic reserves remain important, governments should also focus on maintaining industrial capacity, preserving critical skills and ensuring continuity of manufacturing during periods of disruption.

Third, procurement frameworks should place greater emphasis on supply chain transparency and resilience. Research by the OECD suggests that improved supply chain visibility, diversification and strategic inventory management are important mechanisms for reducing vulnerability to systemic disruption.

Policy Recommendations

Three practical measures could strengthen national resilience. First, governments should establish a dedicated CBRN Supply Chain Intelligence Function responsible for dependency mapping, horizon scanning and vulnerability assessment. Second, resilience frameworks should introduce a formal category of Strategic Enablers to recognise functions that may not constitute critical infrastructure in their own right but which remain essential to preparedness, response and recovery. Third, procurement and assurance processes should require greater multitier supply chain visibility, enabling hidden dependencies and systemic risks to be identified before they affect operational capability.

Conclusion

The central question is not whether CBRN supply chains should be formally designated as critical infrastructure. Rather, it is whether governments adequately recognise their role as strategic enablers of national resilience.

CBRN capabilities do not exist in isolation. They rely upon complex industrial networks, specialist manufacturers and globally distributed supply chains extending far beyond the traditional boundaries of the sector. This is particularly evident in biological preparedness, where resilience depends not only upon frontline response organisations but also upon robust supply chains supporting diagnostics, surveillance systems and medical countermeasures. As recognised in both the Integrated Review

Refresh 2023 and the UK Government Resilience Framework, national resilience increasingly depends upon understanding and managing the complex interdependencies that underpin critical capabilities. If resilience planning is to keep pace with an increasingly interconnected world, policymakers must look beyond critical infrastructure itself and towards the strategic enablers that support it. Failure to do so risks discovering during a future crisis that the weakest point in national CBRN preparedness was never the frontline capability, but the unseen supply chains upon which it depended.

Professor David Crouch is a globally recognised authority in Chemical, Biological, Radiological, and Nuclear (CBRN) defence and civil nuclear safety, with over 30 years' experience across defence, security, and the civil nuclear sectors. He is Director of the CBRN & Survivability Group at Cranfield University, Technical Director at United CBRN Ltd, and a Visiting Professor at the University of Hertfordshire. He previously held senior global product leadership roles at 3M and Scott Safety, driving innovation in respiratory and CBRN protective technologies. A Senior Associate Fellow at the RUSI, David is an active member of its Proliferation and Nuclear policy team and a key contributor to Project Anthracite, focused on DPRK chemical weapons capabilities and counter-proliferation. He is a former Chairman of CBRN UK and continues to advise industry and government as a member of the ADS Security Sector Council. David plays a leading role in international standards development through ISO, CEN, and BSI, and directs the UK Ministry of Defence's Counter CBRN Professional Education Programme at the UK Defence Academy, working with NATO, WHO, and the European Commission. A published author and recognised thought leader, he advances resilience for defence, security, and civil nuclear communities worldwide. He is a Fellow of seven leading international organisations spanning resilience, leadership, education, and science - including SFHEA, FSRP, FEPS, FISRM, FCMI, FICPEM, and FRSC, and holds Chartered status as a Chemist, Scientist, Manager, and Security Professional.
Natascha McVeigh is the Senior Lecturer in Crisis & Disaster Management, University of Lincoln, with a specialism in grey zone warfare and hybrid threats to critical infrastructure.

Wet Chemical Decontamination Preserves Ex Vivo Skin Friction Ridges for Post-Mortem Fingerprinting

Source: https://bioengineer.org/wet-chemical-decontamination-preserves-ex-vivo-skin-friction-ridges-for-post-mortem-fingerprinting/

Nov 12 – Rigorous immersion in chemical decontaminants does not destroy the microscopic structural integrity of human skin or prevent post-mortem forensic identification through powder-based fingerprint recovery, according to an experimental investigation evaluating methods for handling contaminated decedents. In mass casualty events involving chemical, biological, radiological, or nuclear agents, as well as hazardous material spills, decontamination is critical to protect emergency first responders and medical personnel from severe secondary exposure. While living casualties are prioritized for time-consuming decontamination techniques, deceased victims also require decontamination when persistent toxic agents are present. Forensic specialists must nevertheless extract reliable physical identifiers from human remains, particularly friction ridge impressions, which serve alongside dental examination and DNA profiling as internationally recognized gold standards for victim identification.

To determine whether aggressive wet decontamination procedures compromise friction ridge detail, researchers conducted a prospective experimental study using surgically amputated human extremities as an ex vivo skin model. The research team evaluated eight distinct deconta-

mination protocols across 22 clean limb specimens, comprising two upper extremities and 20 lower extremities collected following institutional ethical approval. Under relevant Hungarian health regulations, surgical tissue remnants undergo mandatory histological examination, permitting the selective acquisition of limbs with intact palmar or plantar surfaces across at least three digits. The anatomical friction ridges present on the volar surfaces of the human foot and toes possess identical morphological characteristics to those found on the fingers and palms, establishing both anatomical sites as fully viable substrates for forensic pattern comparison and personal identification.

The experimental protocol tested six chemical formulations spanning varied operational concentrations and disinfectant mechanisms: household bleach prepared as sodium hypochlorite solutions at concentrations of 1 percent, 5 percent, and 10 percent; Bradolin, an alcohol-based surface disinfectant; Incidin Extra N, an aldehyde-free industrial surface cleaner evaluated at a 5 percent concentration; Neomagnol, an active chloramine B preparation tested at 10 percent; and Solumium, a stabilized chlorine dioxide formulation. These agents were selected because they represent commercially accessible, high-volume chemicals possessing verified antimicrobial action or established capability for neutralizing persistent chemical warfare agents. Readily soluble agents with minimal expected skin reactivity, such as basic soapy water, were omitted because their potential to disrupt structural surface ridges was considered negligible under practical emergency response conditions.

Individual digits were surgically separated at the metatarso-phalangeal or metacarpo-phalangeal joints in a controlled autopsy suite maintained between 19 and 21 degrees Celsius. Before applying chemical treatments, baseline exemplar prints were gathered from every digit using two parallel collection modalities: traditional dusting-lifting using camel-hair brushes, black latent print powder, and lifting tape, alongside optical scanning conducted at 500 pixels per inch using an automated live fingerprint scanner. Selected digits were then completely submerged for 15 or 30 minutes in 50 milliliters of freshly mixed chemical decontaminant inside laboratory containers. Although prolonged immersion represents an unusually rigorous procedure compared with field washing, the investigators intentionally utilized this aggressive exposure to maximize the detection of any latent chemical destruction or ridge degradation.

Following chemical immersion, the specimens were dried with paper towels, and fingerprint collection was repeated under identical technical conditions. To evaluate potential delayed structural breakdown, three specific lower-extremity specimens treated with 1 percent bleach were stored in a refrigerated morgue environment at 4 degrees Celsius for 44 hours before undergoing delayed secondary fingerprinting. To provide a rigorous, objective assessment, all exemplar prints were masked with randomized alphanumeric identification codes and submitted to an independent examiner at the Hungarian Institute of Forensic Sciences. The blinded examiner graded print clarity across an established four-point forensic scale ranging from insufficient prints lacking identifiable minutiae to perfect prints displaying sharp friction ridges and level-three ridge details.

Comparative evaluation demonstrated that all eight wet decontamination methods preserved the underlying anatomical skin structure, leaving friction ridges intact and suitable for personal identification when processed with appropriate recovery tools. However, diagnostic performance diverged sharply between the two fingerprinting modalities. Across the total dataset of 114 exemplar prints, optical live scanning failed to produce usable images in 55 instances, whereas the conventional powder dusting-and-lifting technique resulted in only 10 insufficient prints. Notably, every print that

failed under powder lifting was also classified as insufficient by optical scanning, and no specimen yielded a successful scan while proving unreadable by dusting-lifting. Statistical evaluation using McNemar's test demonstrated that powder-based lifting was significantly superior to optical live scanning ($p < 0.0001$).

Because multiple digits were collected from each of the 22 amputated limbs, the researchers implemented a Generalized Estimating Equations model with a binomial logit link and exchangeable working correlation structure to account for hierarchical intra-limb clustering. This statistical validation confirmed that the superiority of the dusting-and-lifting modality over optical scanning remained robust and statistically significant (beta = -2.28, robust standard error = 0.33, Wald z = -6.86, $p < 0.0001$). The marked drop in optical scanner performance was heavily influenced by specific chemical exposures. While solutions such as Bradolin, 5 percent Incidin, and 10 percent Neomagnol caused no deteriorative effects on exemplar prints and frequently enhanced ridge sharpness, bleach at a 10 percent concentration produced a dramatic drop in optical scanning capability (Wilcoxon signed-rank test, $p < 0.001$) while causing no significant negative change in dusting-lifting scores ($p = 0.317$).

Under 10 percent bleach immersion, the friction ridges became entirely undetectable to the optical live scanner, and the skin exhibited visible yellowish macroscopic surface discoloration. In contrast, 1 percent bleach caused notable degradation on scanned prints without impairing dusted prints, whereas 5 percent bleach produced no deteriorative effects on either modality and even improved ridge sharpness in certain trials. Delayed evaluation after 44 hours of refrigerated storage demonstrated no delayed structural degradation, with one specimen yielding its sharpest ridge contrast after the storage interval. Optical scanning was similarly impeded following treatment with chlorine dioxide, which caused a mild reduction in scan quality while leaving dusting-lifting prints fully preserved or noticeably sharpened.

Microscopic histological evaluation of skin biopsies stained with hematoxylin and eosin revealed that the decontaminants did not produce definitive chemical destruction or deep cytological lysis. Although histological alterations were recorded in multiple specimens, native untreated control samples frequently exhibited similar microstructural alterations, indicating that tissue changes stemmed primarily from pre-analytical factors, such as post-surgical tissue decay or tissue hydration during fluid immersion, rather than direct caustic destruction. Fisher's exact test identified a strong association between histological structural alterations and fingerprint insufficiency ($p = 0.0017$, odds ratio = 6.4), showing that pre-existing tissue changes multiplied the likelihood of unreadable prints sixfold.

The failure of optical scanning in the presence of intact physical ridges is primarily attributed to surface biochemical alterations rather than anatomical tissue destruction. Optical scanners depend on epidermal light-scattering properties and surface moisture balance, which are disrupted when alkaline sodium hypochlorite induces saponification of epidermal fatty acids or when chlorine dioxide alters superficial lipids. Furthermore, the removal of loose keratin debris and the mechanical softening of the stratum corneum during fluid immersion explain why chemical washing often enhanced powder adhesion. While ex vivo surgical tissues do not fully capture post-mortem decomposition or actual chemical warfare contaminants, these findings confirm that emergency responders can deploy aggressive wet decontamination without destroying essential post-mortem biometric evidence, provided forensic teams prioritize powder-based lifting over optical scanners. Beyond personal identification, disaster response operations require careful sequencing to protect criminal investigations. Because wet deconta-

mination can wash away material remnants, fragments, or forensic residues critical for investigating events such as terrorist attacks, investigators must document and collect perishable forensic traces before immersing remains. Definitive victim identification and autopsies are conducted afterward. Operational planners must also consider secondary contamination risks inherent to collection modalities. Although optical scanners yield instantly secure digital files, the resulting images frequently degraded following chemical washing. Conversely, powder-based lifting remained highly reliable across all tested decontaminants, but handling physical lifting tape carries a risk of disseminating hazardous agents if previous decontamination was incomplete. The researchers suggest that immediately photographing lifted exemplar prints resolves this dilemma, converting physical tape impressions into safe, non-hazardous digital files for forensic comparison.

Decontaminating deceased victims is essential in incidents involving persistent CBRN agents, because decedents cannot utilize self-decontamination kits. Radioactive materials can remain hazardous over physical and biological half-lives ranging from hours to years, while chemical warfare agents, including Novichok variants A-230, A-232, and A-234, as well as VX and HD, persist in various matrices for days to weeks. Furthermore, highly persistent microbiological agents such as Bacillus anthracis spores can survive in the environment for several years. Managing these threats also introduces serious ethical considerations regarding human dignity and respectful treatment of the deceased. The authors emphasize that post-mortem decontamination should be performed only when justified by contamination risks, using proportionate procedures that minimize unnecessary damage to remains while balancing responder safety with forensic identification.

The unexpected divergence in scanner performance between 1 percent and 5 percent bleach solutions highlights the need for broader testing across diverse commercial formulations. Because variations in formulation and chemical properties may contribute to differing surface effects, future studies should directly measure relevant physicochemical properties under controlled laboratory conditions. Expanding experimental designs across varied decontamination protocols, exposure conditions, and fingerprint recovery techniques will help emergency personnel integrate decontamination and victim identification into a unified, evidence-based forensic workflow.

Article References: Farkas, C. B., Roskó, R., Vajda, A., & Petretei, D. (2026). Effects of various wet decontaminants on ex vivo fingerprinting. *Egyptian Journal of Forensic Sciences, 16*(1), Article 96. https://doi.org/10.1186/s41935-026-00596-9

Hospital Planning and Response for Sudden Chemical Mass Casualty Incidents



14

Mauricio Lynn
University of Miami Miller School of Medicine, Jackson Memorial Hospital, Department of Surgery, Miami, FL, USA

Assumptions

• Sudden exposure of multiple people to a chemical agent may be classified as a sudden chemical mass casualty incident (SCMCI).
• The vast majority of the contaminated patients will be mildly contaminated ("walking wounded").
• The majority of contaminated patients will self-evacuate or be transported by no rescue personnel to local hospitals.
• Although decontamination at the scene is desirable, it is time consuming in an unplanned, sudden event, and therefore unrealistic.
• Most critical patients, usually those with respiratory distress, will probably expire by the time scene decontamination is available. Therefore, critical contaminated patients should be transported rapidly to hospitals by first responders who must have personal protective equipment (PPE). Removal of all clothing may reduce contamination by 80–90% and should be done prior to getting into the ambulance. Once in the ambulance, patient can be kept covered and warm with blankets and sheets.
• High probability that a large number of self-evacuated patients will food the hospital campus.
• Hospitals should plan to prevent patient fooding, have a decontamination facility, and further manage patients from a SCMCI.

Review Highlights Governance Strengths and Operational Gaps in Lebanon CBRN Preparedness

Source: https://bioengineer.org/review-highlights-governance-strengths-and-operational-gaps-in-lebanon-cbrn-preparedness/



Nov 18 – A comprehensive narrative review evaluating Lebanon's health sector preparedness for chemical, biological, radiological, and nuclear (CBRN) emergencies has identified significant progress in high-level strategic governance alongside critical gaps in operational execution, resource availability, and legal backing. Published in the International Journal of Emergency Medicine, the study represents the first system-level synthesis of national CBRN readiness in the country. Researchers synthesized evidence across peer-reviewed and grey literature to examine how effectively Lebanon can anticipate, manage, and mitigate hazardous public health crises across eight core domains. The findings reveal that while national institutions have demonstrated notable engagement with global safety guidelines, established executive governance structures, and conducted multi-sectoral simulation initiatives, day-to-day emergency readiness remains compromised by severe resource deficits, fragmented agency coordination, legislative inaction, and heavy reliance on external donor support. Overall, strategic planning and governance capacities proved stronger than operational response and real-time surveillance functions.

Lebanon occupies a geopolitically vulnerable position along the eastern Mediterranean coast, encompassing approximately six million people exposed to recurrent natural hazards and political instability. The review documents that the country holds a position that thrusts the threat of chronic catastrophes upon its shores, having endured multiple major disasters that debilitated its healthcare system. Among these was the 2020 Beirut Port explosion, recognized as one of the most destructive chemical explosions in history, which caused massive casualties and severe physical damage to hospital infrastructure. The health sector faced further devastation during the 2024 conflict, which involved the use

of white phosphorus, caused approximately 4,285 deaths, and severely debilitated national medical capabilities. Concurrently, emergencies from communicable diseases have posed recurring threats to public health, with the coronavirus disease 2019 (COVID-19) pandemic and a 2022 cholera outbreak straining clinical facilities. Inadequate hospital preparedness remains a documented concern, posing severe public health risks for a lower-middle-income nation facing disproportionate disaster-related mortality.

To evaluate national readiness, the researchers conducted a comprehensive literature search across MEDLINE-Ovid for peer-reviewed studies published in English between 2000 and 2026. The search utilized Medical Subject Headings including “Lebanon” and “Disaster Planning,” alongside relevant keywords such as “health sector preparedness” and “CBRN.” To ensure an inclusive dataset, investigators performed manual searches for grey literature using Google and cross-referenced bibliographies of selected articles. Studies were included if they examined the management, preparedness, and response to CBRN hazards within Lebanon, while non-Lebanon studies were excluded. Screening yielded 87 peer-reviewed articles and 36 grey literature records, with ten sources meeting final inclusion criteria: three peer-reviewed papers and seven grey literature documents. Two peer-reviewed sources, representing 20 percent of the sample, addressed hospital facilities—one describing a CBRN assessment tool developed via an expert panel modified Delphi consensus process, and another using a cross-sectional survey to assess emergency department preparedness for CBRNe incidents.

The remaining eight sources, comprising 80 percent of the evidence base, evaluated broader system-level capacities. Two sources examined compliance with global health security guidelines, including a mixed-methods academic paper and an official self-assessment report submitted to the World Health Organization. Two grey literature sources analyzed governance frameworks, encompassing a national report on nuclear safety and radiation oversight and a handbook outlining central operational coordination. Four grey literature documents addressed applied emergency response: two covering field exercises—one providing guidance for a CBRN counter-terrorism drill and another outlining a planned national simulation—and two case studies from the International Federation of Red Cross and Red Crescent Societies analyzing the 2020 Beirut Port explosion. The authors synthesized findings across eight domains deductively adapted from World Health Organization State Party Self-Assessment Annual Reporting (SPAR) capacities: International Frameworks; National Bodies, Strategies, and Regulations; Coordination; Early Warning, Alert and Response Systems (EWARS) and Information Management; Material Resources; Human Resources; Prehospital and Emergency Medical Services; and Hospitals.

National CBRN governance is distributed across multiple governmental, scientific, and security bodies. The National CBRN Commission, established in 2013 under the Prime Minister’s Office, spearheads national preparedness policy, regulations, and strategic planning. However, the commission is composed exclusively of governmental ministries, technical entities, security agencies, the Lebanese Army, and the Lebanese Atomic Energy Commission (LAEC), omitting non-governmental operational actors such as the Lebanese Red Cross and private hospital representatives. Ionizing radiation regulation is led by the LAEC, created under decree-law 105/1983 within the National Council for Scientific Research, handling source registration, licensing, and safety inspections. Operational incident management relies on a broader network: the Ministry of Public Health deploys multi-agency Hazmat teams, while the Lebanese Army executes nuclear source detection alongside police and Civil Defense. Governance functions primarily through executive decrees, strategies, and donor-funded action plans rather than statutory legislation. Although Parliament ratified the Convention on Nuclear Safety, dedicated International Health Regulations legislation drafted in 2016 remains unratified.

Furthermore, all identified resources, specialized training, and governance mechanisms remain concentrated in Beirut, lacking territorial decentralization.

Multi-sectoral coordination and surveillance capabilities demonstrate notable institutional achievements alongside persistent operational integration gaps. Lebanon ratified the International Health Regulations in 2007, with the Ministry of Public Health acting as national focal point. In the 2025 self-assessment, focal point functions and emergency preparedness planning both achieved scores of 80 percent. Conversely, multi-sectoral coordination scored 60 percent, reflecting heavy reliance on the health ministry and limited participation from non-health sectors. Operational coordination is tested through biennial European Union-supported "ARZ" field exercises led by the commission, integrating security forces, the LAEC, first responders, and hospitals. Early warning and surveillance systems, overseen by the ministry's Public Health Emergency Operation Centre (PHEOC) and Epidemiological Surveillance Unit, achieved a 2024 surveillance score of 60 percent, comprising 40 percent for early warning and 80 percent for event management. PHEOC connects peripheral facilities to coordinate responses during mass casualty events. However, a 2026 study revealed that 50 percent of surveyed emergency departments lacked adequate communications with external agencies during emergencies.

Material resource constraints constitute a severe vulnerability within the national preparedness framework. Although the Ministry of Public Health submitted scores of 80 percent for both International Health Regulations financing and chemical event resource capacity, chronic economic instability has created severe deficits in funding, medical supplies, and basic infrastructure. Health facilities experience chronic disruptions in electricity, fuel, and internet connectivity, which impede operational consistency. **Specialized CBRN infrastructure is acutely lacking across the health sector, with pronounced deficits in decontamination units, negative-pressure isolation facilities, and personal protective equipment.** Furthermore, limited domestic pharmaceutical stockpiles create heavy reliance on imported medications, heightening system vulnerability during acute supply-chain breakdowns. Because domestic budgetary mechanisms do not mandate dedicated funding for CBRN preparedness, national initiatives—including training drills, personal protective equipment procurement, and equipment acquisition—depend overwhelmingly on external international assistance, specifically donor funding from the European Union and the World Health Organization.

Human resource development represents another critical operational bottleneck. National efforts to build professional capacity have included specialized training across health and non-health sectors. Between 2013 and 2022, donor-funded projects trained more than 340 personnel from first-responder agencies in radiological and nuclear emergency response. The resulting national emergency response team unites members from the Lebanese Army, Civil Defense, Beirut Fire Brigade, Lebanese Red Cross, and Police. A dedicated medical hazardous materials team was established in 2017 and trained for CBRN response, contributing to a reported human resources capacity score of 67 percent in Lebanon's 2024 self-assessment. Nonetheless, the widespread migration of medical practitioners following the 2019 economic crisis has severely challenged the sustainability of these programs. Furthermore, recent empirical data show that healthcare workers in hospital emergency departments report limited basic knowledge of radiation hazards, with the large majority reporting unmet training needs. The review notes that CBRN technical training should ideally be repeated every six to nine months to maintain competence in protective equipment and hazard management.

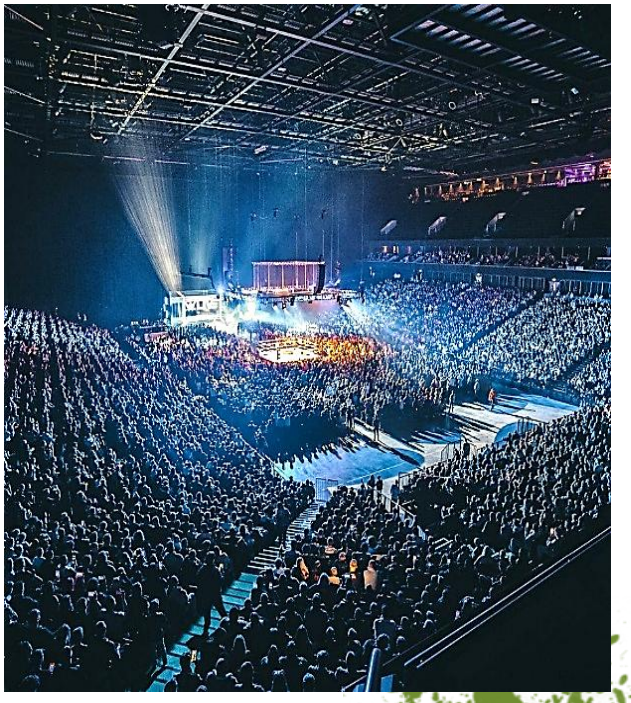
Operational coordination between prehospital emergency services and receiving hospitals reveals a critical decontamination bottleneck. Prehospital response is delivered primarily by Civil Defense and Lebanese Red Cross volunteers, with the Red Cross mobilizing thousands of surge personnel and maintaining a specialized

CBRN unit. While these responders provide ambulance transport, triage, and basic life support, their ability to perform advanced on-site medical care and decontamination remains limited. International guidance identifies decontamination before transit as essential to prevent secondary exposure among patients, responders, and clinical facilities. Because prehospital decontamination is constrained, the decontamination burden shifts entirely to receiving hospitals. Hospitals serve as primary sites for CBRN casualty management, with 17 facilities designated as chemical reference centers. However, 2022 assessments revealed low readiness and widespread gaps across hospital training, surveillance, and decontamination infrastructure. Furthermore, in a highly privatized healthcare sector where preparedness investments receive little reimbursement, hospitals face limited economic incentives to maintain expensive infrastructure, and private facilities experienced severe operational difficulties during the 2020 Beirut Port explosion due to limited supplies.
Regional comparisons contextualize Lebanon's decontamination deficiencies: on the 2024 self-assessment for infection prevention control and chemical and radiation decontamination, Lebanon scored 40 percent, matching wider patterns in lower-middle-income Eastern Mediterranean countries where Jordan and Egypt scored 60 percent while Morocco scored 20 percent. To address these systemic gaps, the review outlines key policy recommendations: including non-governmental responders such as the Lebanese Red Cross and private hospitals within the National CBRN Commission, expanding operational preparedness and field exercises beyond Beirut into vulnerable regional areas, diversifying national disaster financing to reduce reliance on external donors, and ratifying the pending 2016 draft legislation to place International Health Regulations obligations on a statutory footing. Regarding limitations, the authors emphasize that as a narrative review, no formal critical appraisal of source quality was conducted. Because the evidence base consists of heterogeneous literature and self-assessed national reporting, findings reflect reported institutional capacity rather than independently verified real-world performance.

Article References: Hitti, E., El Zahran, T., Kallab, A., & Farah, L. (2026). A narrative review of CBRN health sector preparedness in Lebanon. *International Journal of Emergency Medicine, 19*(1), Article 268. https://doi.org/10.1186/s12245-026-01379-8

Manchester's Co-op Live evacuated after 'unknown substance' let off in crowd

Source: https://www.bbc.com/news/articles/c9e851dn8516o



Nov 23 – Thousands of people were evacuated from a concert in Manchester on Sunday night after an "unknown substance" was released into the crowd, police said.
The incident happened towards the end of US rapper Don Toliver's show at the Co-op Live arena at about 22:00.
The Northwest Ambulance Service said one person was taken to hospital for further assessment while **more than 88 people were assessed for "eye and respiratory symptoms".** Greater Manchester Police (GMP) said a major incident was declared after reports

of people suffering from the effects of an unknown substance, which **police initially believed to be tear gas.** Police said 12,000 people had been evacuated and one fan told of "distressing scenes" with people "choking" as they left.



Joey Howe said the incident happened 30 or 40 minutes into the concert.

The 22-year-old told BBC Radio Manchester: "I saw a lot of people streaming out and you go into this panic mode and you see a lot of people running out of the venue. "The lights have come on and he is being rushed off stage. "That horrible smell just hit you." He said it was like "time stopped in motion" when "there was nothing going on". "We then decided to go out. People were coming through in wheelchairs choking - it was really distressing," Howe said. "We then decided to leave the venue. It was just really distressing scenes and not something you want to see."

'Screaming in pain'





Jessica Moult-Boffey, of Wigan, said people were "crying" and "screaming in pain" after they had fled the venue. The 23-year-old told the BBC that she went to the exit and saw lads on the bridge which leads into Medlock Square "crying and screaming in pain". The music fan added that they were "asking for help" but there were only two stewards outside. Footage on social media showed emergency services converge on the arena, while some concertgoers were seen coughing as they streamed out of the venue. GMP said more than 12,000 people had been safely evacuated, with several people assessed for side effects. "Our priority was to ensure the safety of every person that was attending the concert," GMP Assistant Chief Constable Steph Parker said. "Several people were treated on site, and one has been taken to hospital at this time. Anyone who has left the event and since become unwell is advised to attend their local hospital.

"We understand the concern that this incident will have raised – particularly those with loved ones at the venue last night – and we'd like to thank everyone for their patience as we dealt with it." She said the declaration of a major incident enabled the emergency services to coordinate a safe response.

EDITOR'S COMMENT: Exposure to CS (2-chlorobenzylidene malononitrile | $C_{10}H_5ClN_2$ | vapor density 6.5 [air=1]), commonly referred to as tear gas, produces rapid irritation of the eyes, skin, and respiratory tract, resulting in lacrimation, blepharospasm, coughing, chest tightness, and a sensation of suffocation. Although symptoms are generally transient following removal from exposure, their severity depends on the concentration, duration, environmental conditions, and individual susceptibility. Exposure in enclosed or poorly ventilated environments, as well as among individuals with asthma or other respiratory conditions, may result in more serious clinical consequences.

In mass-casualty incidents, however, the distinction between simple exposure and actual contamination is operationally important. Following brief outdoor exposure to CS, removal to fresh air may be sufficient, and extensive decontamination may not be necessary. Conversely, persistent symptoms (>30min), visible residue, suspected exposure to CS powder, or release inside an enclosed venue may justify active decontamination. The initial response should prioritize removal from the contaminated environment, prevention of secondary contamination, and assessment of respiratory compromise. Contaminated clothing should be removed carefully, preferably without pulling it over the head, bagged, and isolated. Exposed skin should be decontaminated using an appropriate method; dry decontamination with absorbent material may be considered initially, while persistent skin contamination may require washing with soap and water. Eyes should be irrigated with clean water or saline, and contact lenses removed. Bleach and aggressive rubbing should be avoided.

The Co-op Live incident also underlines the importance of distinguishing CS exposure from an unidentified chemical release. Mass evacuation, triage, casualty separation, ventilation, controlled decontamination, clinical observation, and protection of responders must be coordinated rather than undertaken indiscriminately. Patients with persistent dyspnea, wheezing, chest pain, visual disturbance, significant skin injury, or prolonged symptoms require medical assessment, particularly those with asthma or underlying respiratory disease. In crowded venues, rapid recognition, appropriate decontamination, and clear public instructions may reduce secondary exposure, prevent contaminated clothing or belongings from spreading irritant residues, and maintain confidence in the emergency response.



2026 C²BRNE TERRORISM CONFERENCES



PRO Asia

13-18 December 2026, Hua-Hin, Thailand

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.





The Security Cleared EXPO is a careers fair for individuals who are Security Cleared to DV, SC, CTC, NATO or NPPV levels.

Cheltenham is synonymous with the intelligence community and is an obvious choice for our EXPO, with Cheltenham Racecourse being a perfect venue. The varied work created from Cheltenham and the companies that feed into the intelligence network are far-reaching, which means UK Security Clearances and cyber skills are in high demand. If you are looking to engage with these niche opportunities that are often not available online, then our Cheltenham EXPO should not be missed!

Graduate Students

Current Graduate students or individuals wishing to take courses at the graduate level can pursue the following opportunities:

Master of Professional Studies (MPS) in Security and Terrorism Studies

START offers a fully online Master of Professional Studies (MPS) degree in Security and Terrorism Studies through the University of Maryland's Graduate School. The program prepares students to examine the complex social, political, economic, and psychological underpinnings of terrorist and other asymmetric security threats, and is delivered in a synchronous format using multiple online platforms provided by the University of Maryland, College Park. Learn more about the MPS degree

---

Graduate Certificate in Terrorism Analysis

START offers a fully online Graduate Certificate in Terrorism Analysis hosted through the University of Maryland Graduate School. The flexible program (1-2 academic years) provides participants – both scholars and practitioners – with advanced education on the causes, dynamics and impacts of international and domestic terrorism. Applications for the Graduate Certificate are accepted at two points during each calendar year, in January and July. Learn more about the Graduate Certificate

---

Graduate Certificate in Insider Risk Management and Mitigation

START offers a fully online Graduate Certificate in Insider Risk Management and Mitigation through the University of Maryland's Graduate School. The program provides participants with advanced education on understanding, investigating, and managing insider risks and insider threats, and is delivered in a synchronous format using multiple online platforms provided by the University of Maryland, College Park. Learn more about the Graduate Certificate

---

Internships

Research internships are held every fall, spring, and summer term at the University of Maryland. Students research between 10-20 hours per week throughout their term and can pursue these opportunities for academic credit if desired. Applications for internships are typically due three months before the start date of the internship. Learn more about our internships

---

Study Abroad

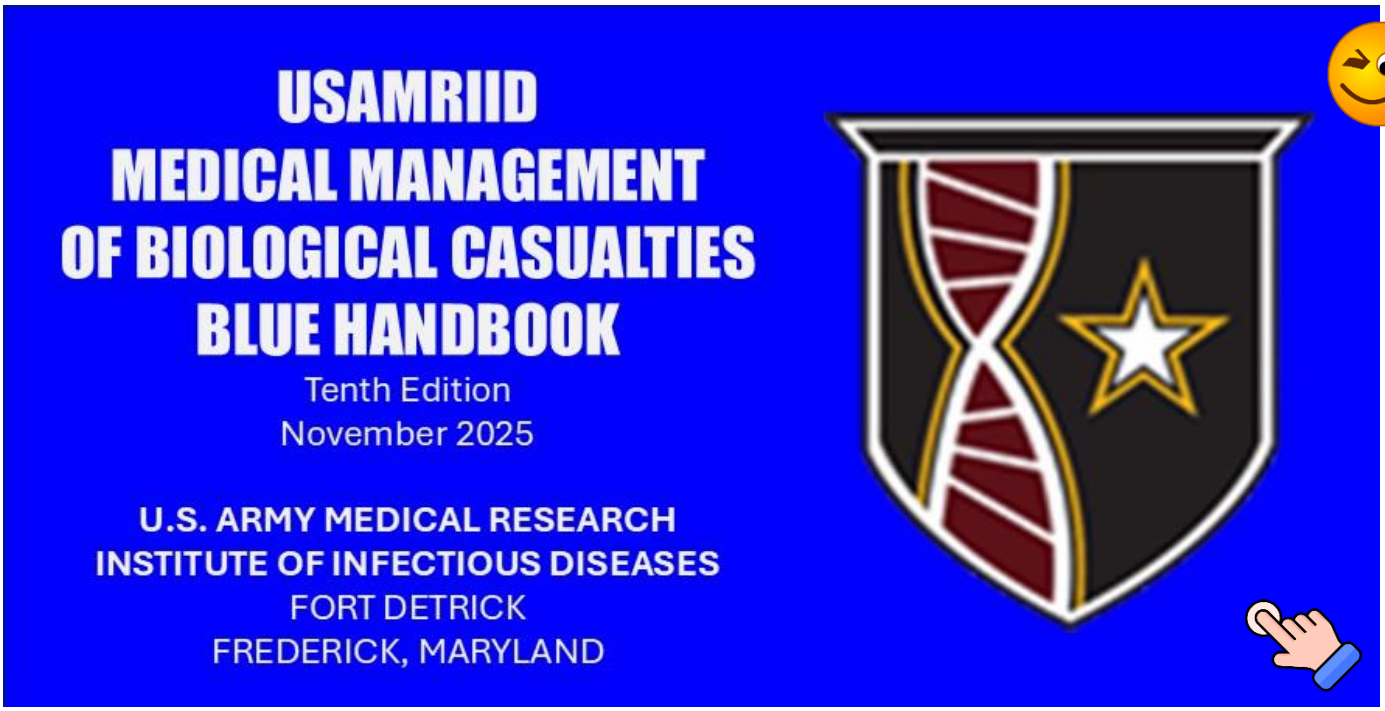
Study Abroad programs are hosted at foreign-based centers affiliated with START. These programs are open to undergraduate and graduate students from any institution and are hosted through START and the University of Maryland Education Abroad Office. Please see the UMD Education Abroad page for more information. Learn more about the programs

---

Online Courses

START continually develops online summer and winter courses in the terrorism studies field. Past courses include: Psychology of Terrorism; Financing of Terrorism and Methods Deployed to Counter Terrorist Financing; Geography of Terrorism and more. These courses are offered through the University of Maryland's Extended Studies and are open to all individuals. Learn more about the courses.


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



Medical defense against weaponized pathogens and toxins is an unfamiliar yet vit al subject at all levels of military and civilian healthcare delivery. The U.S. military has pursued research relevant to the medical defense against biological threat agents since World War II, first in concert with an offensive weapons program—then since 1969—as a purely defensive research program. Since that time, there have been significant advancements in research, technology, medical countermeasures, and the threats at large.

There has been a sustained momentum among healthcare providers and planners to better understand the medical management of high consequence infectious disease and toxin exposures to minimize casualties and reduce impact to the community; most recently from the lessons learned in the COVID-19 pandemic of 2020. Diverse measures to enhance readiness have grown over the years to include improvements in face-to-face and virtual training platforms/content, improved and accessible references (print and electronic), and added emphasis on integration into military and civilian training scenarios on a routine basis.

These measures optimize the ability of healthcare personnel (military and civilian) to identify, mitigate, and recover from these threats while maintaining operations in a bio-threat environment. This handbook has been methodically revised and enhanced to provide the reader with the tools and references necessary to medically manage biological casualties and lay the framework to streamline the broad medical response.

Incorporating perspective, capability, and information from across the Department of Defense (DOD) was a focus to move this handbook to be applicable across the services. We welcome feedback and contributions to better expand our collective toolbox to combat these ever-present threats.

The importance of this topic and the relevance of this handbook is self-evident, and it is hoped that through this resource, medical providers/planners will develop a broad understanding of potential biological threats to our military forces and civilian communities, find high yield information for the management of biological casualties, and appreciate the process inherent to a bio-hazard response.

The purpose of this reference is to serve as a concise handbook that can be pulled off the shelf, in a crisis, to guide medical personnel in the prophylaxis, recognition, and management of biological casualties/events. It is designed as a portable handbook and is not intended as a definitive or exhaustive textbook. A more in-depth discussion of the bio-agents covered here may be found in the U.S. Army Surgeon General's Borden Institute Textbook of Military Medicine: Medical Aspects of Biological Warfare (2018) and in relevant infectious disease, tropical medicine, and disaster medicine textbooks.



A new defense technology startup, aiming to produce genetically modified dogs for military and law enforcement use, has launched with $200 million in initial funding. Texas-based Warhound was



conceived by Anduril Industries founder Palmer Luckey and entrepreneur Ben Lamm—the duo behind Colossal Biosciences, a company known for its efforts to revive extinct species.

Japan to draft DNA synthesis rules to prevent bioterror misuse amid AI worries

Source: https://mainichi.jp/english/articles/20261026/p2a/00m/0sc/006000c



In a drill simulating a bioterror attack, firefighters and other emergency responders rescue "injured" people in Kani, Gifu Prefecture, Feb. 3, 2015. (Mainichi)

Oct 27 – Japan's government will draft rules for "contract synthesis," in which specialized companies artificially synthesize DNA on third-party orders for research, to prevent bioterrorism and other misuse amid worries that artificial intelligence (AI) could help design lethal pathogens.

As AI advances make it possible to design viruses and other entities not found in nature, discussions in the United States and Europe on strengthening safety measures are accelerating. In Japan, the Cabinet Office will set up a new expert panel to discuss drafting guidelines for screening dangerous DNA sequences and customers.

Research institutions and pharmaceutical companies specify the DNA sequences they need and ask specialized companies to synthesize them to study how particular genes work or to give organisms new functions. This "contract synthesis" supports life sciences research as well as industries including medicine, drug discovery, agriculture and livestock. According to the Cabinet Office, the top five companies in the United States and Europe account for 50% to 60% of the global market, and Japan also has multiple synthesis companies. At the same time, rapid advances in AI and developments in DNA synthesis technology have heightened concerns that the synthesis could be misused to create dangerous viruses or bacteria. A research team from Stanford University and other institutions in the U.S. announced this year that it had succeeded in

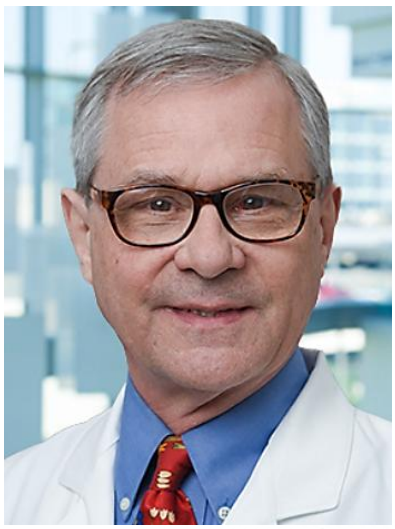
synthesizing DNA based on genetic information designed by AI and creating a virus that does not exist in nature. A research team at the Massachusetts Institute of Technology reported in 2024 that it had divided orders for fragments of the genome sequence of the Spanish flu virus, which killed millions across the world more than 100 years ago, among multiple synthesis companies, and by combining them was able to assemble the genetic information needed to re-create the virus. Screening by synthesis companies serves as a bulwark against misuse. In the United States and Britain, guidelines encourage companies to check whether ordered sequences are related to pathogens or toxins and to confirm customers' intended use. Under a 2025 executive order, the administration of U.S. President Donald Trump required research receiving government grants to use DNA synthesis companies that comply with the guidelines. The European Union is also moving toward legislation. Japan, meanwhile, has had no public rules, leaving the issue to companies' voluntary efforts. To consider how to deal with the issue, the Cabinet Office will establish a new panel of biosecurity experts and others under an expert body on Japan's bioeconomy strategy. With a view to drafting guidelines based on overseas examples, it aims to compile its conclusions in January 2027. Japan's Growth Strategy includes "synthetic biology and biotechnology" among 17 strategic fields, and officials have judged that rulemaking is an urgent task.

According to an Indian research company, the global DNA synthesis market was worth $5.19 billion, or about 820 billion yen, in 2025, and is projected to grow about 4.6-fold in roughly 10 years.

EDITOR'S COMMENT (on the photo accompanying the article): They worry that artificial intelligence (AI) could help design lethal pathogens, but they do not worry about having CBRN First Responders carrying victims in stretchers while donned in Level-A PPE! And this is not the first time, since similar photos and videos have been made public from similar drills in the Tokyo subway and elsewhere. It is so obvious that the people who organized these drills have NEVER been inside a totally encapsulated personal protective ensemble to have a personal experience of how it is to sweat like hell and feel like being inside an oven in a potentially lethal environment. Instead, they order others to do the job while sitting behind their comfortable desks. Include field responders in the planning process – they know best!

In Memoriam: Raymond Fowler, M.D., Professor Emeritus of Emergency Medicine and disaster-response expert

Source: https://www.utsouthwestern.edu/ctplus/stories/2026/obituary-raymond-fowler.html



Nov. 13, 1952 – Oct. 16, 2026

Nov 02 – Raymond Fowler, M.D., FACEP, FAEMS, Professor Emeritus of Emergency Medicine and one of the most respected emergency medicine and EMS physicians of his generation, died Oct. 16.

For almost half a century – the last 25 years at UT Southwestern and Parkland Health – Dr. Fowler helped shape the field of emergency medical services (EMS) as a physician, scientist, educator, author, and disaster-response expert. He helped coordinate medical care and relief services in Dallas following hurricanes Katrina, Gustav, and Harvey.

After joining the UT Southwestern faculty in 2001, Dr. Fowler began practicing emergency medicine at Parkland Health, one of the busiest emergency rooms (ERs) in the country, and served as an Emergency Department medical director and manager at UT Southwestern. Additionally, he held the James M. Atkins, M.D. Distinguished Professorship in Emergency Medical Services.

An engaging speaker and poet, Dr. Fowler recently shared his perspective on caring for patients in the ER: "People do not come to see us when they're having a nice day," he said. "They come with questions that may be very difficult, but that's the reason you get into medicine – to help solve problems of pain and of fear and of facing the unknown."

Beyond his clinical and academic work, Dr. Fowler helped shape the practice of EMS medicine nationally. As a co-founder of the National Association of EMS Physicians, the physician subspecialty organization for EMS medicine, he was its second nationally elected President. He also served as President of the Georgia College of Emergency Physicians and helped establish the EMS State of the Sciences Conference, widely known as the Gathering of Eagles.

Throughout his career, Dr. Fowler worked to improve outcomes across the spectrum of prehospital care, including cardiac arrest, trauma, and behavioral emergencies. As a Principal Investigator on multiple studies and author of numerous book chapters and influential papers in emergency medicine and EMS journals, he brought a distinctive perspective to the evolving clinical practices and broader challenges shaping the field.

In 2012, Dr. Fowler received the Lifetime Achievement Award in Emergency Medical Services from the American College of Emergency Physicians. And just this year, he was presented with the 2026 Ronald D. Stewart Award for long-standing excellence in emergency medical services, the highest honor from the National Association of EMS Physicians.

Dr. Fowler's lifelong leadership, scholarship, and advocacy helped advance emergency medicine and EMS, strengthening the systems that deliver care in critical moments. His legacy endures in the people and institutions carrying that work forward.

Man charged with mailing hundreds of letters containing powder to officials ahead of the election

Source: https://www.pbs.org/newshour/politics/man-charged-with-mailing-hundreds-of-letters-containing-powder-to-officials-ahead-of-the-election

Nov 03 – Federal authorities charged an Oklahoma City man with sending hundreds of letters containing white powder and ominous warnings about treason to public officials ahead of the 2024 and 2026 elections. The powders turned out to be nonhazardous — yeast or flour — though not all letters have been fully tested, the FBI said in a court filing made public Tuesday.

Robin Martin is charged with conveying a hoax and mailing threatening communications.



He was arrested Monday and was expected to make an appearance Tuesday in U.S. District Court in Oklahoma City.

Online records do not list an attorney who could comment on his behalf, and several relatives didn't immediately respond to social media messages seeking comment.

The investigation stretched back to 2024 when election officials in multiple states reported mail with a

white substance and a three-page letter declaring war, the FBI said. Some bore warnings that could only be read under ultraviolet light, such as, "Stay on the right side of history! Your life may depend on it!!"
The sender wrote a return address as "U.S.T.E.A., United States Traitor Elimination Army, Takoma Park, MD."
Investigators believe more than 700 mailings this fall appeared to be associated with the same sender but with a different return address. They were addressed to election officials, members of Congress, pollsters, news media and federal law enforcement, FBI agent David Cole said in an affidavit.
A common message in the 2024 and 2026 mailings was a warning to recipients about upcoming arrests for treason "or worse!!"
"The writer of the letter described perceived issues with the 2020 election, claimed that President Donald Trump won the 2020 election, and voiced concerns regarding some of the same issues recurring in the then-upcoming 2024 election," Cole said.
Federal authorities announced last month that they were investigating letters with "suspicious substances" that had been mailed to congressional and election offices nationwide and urged recipients to treat the mailings as potentially hazardous.
The packages led to the evacuation of election offices in Louisiana and Oklahoma. Numerous states, from Idaho to Florida, said they either received letters or had them intercepted by the Postal Service.
The FBI said it has video evidence of Martin's car stopping in October at mailboxes at Postal Service sites in Oklahoma City, Dallas and San Antonio. Investigators also gleaned his fingerprints from a letter addressed to FBI Director Kash Patel, whose first name was written as "Kashyap."
Walmart records show Martin purchased common household goods, such as turmeric and vinegar, to create invisible ink that could be read with ultraviolet light, the FBI said.
The Democratic Socialists of America apparently assisted the investigation. The FBI said it believes Martin, posing as someone using the name George Livingston, posted a message to a DSA email list in October, warning that members were traitors and eligible for arrest for treason if they vote in the Nov. 3 election.

Homegrown Hazards – The Agroterror Threat

By Jacob Ware

Journal of Strategic Competition | Vol. 2 No. 3 (2026): Influence, Threats, and Coercion
Source: https://strategiccompetition.org/index.php/josc/article/view/31

Abstract
A series of indictments against Chinese nationals over the summer of 2025 drew national attention to the spectre of agroterrorism, a subset of bioterrorism targeting animal and plant life with massive implications for national security. Despite the designation of the Food and Agriculture (FA) sector as one of the sixteen critical infrastructure sectors determined by the National Infrastructure Protection Plan (NIPP), the United States remains woefully unprepared for a targeted act of agroterrorism. This paper explores past case studies of agroterrorism, the vulnerabilities of the American agriculture system, and the potential weaponization of the agricultural sector by terrorists of several stripes.



AI could help make new vaccines. Will people take them?

By Ben Rader

Source: https://thebulletin.org/2026/11/ai-could-help-make-new-vaccines-will-people-take-them/

Nov 05 – A common flu variant tweaked to increase lethality. A synthetic coronavirus programmed to evade current vaccines. A strain of pneumonic plague modified to be resistant to antibiotics. As fears grow that AI has lowered the barriers to engineering pathogens, some experts have been calling for a Manhattan Project-scale effort to counter the potential biological risk. In recent months, philanthropists, entrepreneurs, and government funders—judging the best defense against AI-enabled pandemics to be AI itself—have invested hundreds of millions of dollars in high-tech projects to develop rapid, scalable responses to such scenarios.



Yet, most medical countermeasures cannot protect people if they aren't willing to accept them, and while AI can accelerate their development, it cannot manufacture the trust needed for their successful deployment. The current momentum in biodefense risks overindexing on technical solutions to a human problem.

If an AI-enabled vaccine became available within days of a future outbreak, the question would remain: Will people get it?

Supply-side preparedness

Vaccination campaigns during outbreaks in past decades have sometimes faltered, and factors such as rare adverse events have driven public resistance. Even technological success in the face of a real health crisis is no guarantee of public trust. Yet, recent investments have prioritized these supply-side solutions to biological threats, with large AI companies directing extraordinary capital and compute toward AI-powered preparedness initiatives.

In May, OpenAI launched a dedicated biodefense program that includes investment in the development of AI-designed antibodies against novel pathogens, while Biohub, joined by Meta, Google DeepMind, and federal agencies announced in October a $1.8 billion public-private partnership with the eventual goal of conducting computer-based biological experiments. These efforts reflect a broader push by tech companies and leading scientists to compress the time between the beginning of an outbreak and when governments can mount an effective response.

The new initiatives have been launching at a rapid clip.

The World Health Organization (WHO) announced a target in October to detect novel pathogens within 24 hours of emergence by 2030. Other organizations are developing computer modeling to rapidly assess pathogenicity and virulence digitally. Last year, for example, the company Valthos, said it received $30 million in a funding round led by the OpenAI Startup Fund to build "AI systems to rapidly characterize biological sequences and update

medicines in real time." And multiple startups are proposing to use AI to design vaccines and therapeutics to deploy as soon as "almost instantly." If these solutions work—and hopefully they do—they could yield candidate countermeasures to a newly discovered threat before it spread between more than a handful of people.

While this scenario is far from today's reality, discussions have already begun on designing proper governance and oversight for this future. However, even as biosecurity experts have focused on issues such as how to manage access to AI-response technology or how to equitably distribute any vaccines that result from these rapid efforts, they have rarely addressed public acceptance.

The scientific evidence needed to establish that a countermeasure works may be very different from the evidence the public needs to believe it is safe and necessary. An AI-modeled vaccine may offer what the public perceives as an untested cure to an insignificant threat. That's happened before—even when an outbreak has already caused notable harm. The early waves of COVID devastated communities and the rapid introduction of a safe and effective mRNA vaccine was a marvel of biotechnology. Still, the rollout was met with fierce resistance and it eventually plateaued with around 70 percent of the US population receiving the complete primary vaccine series, below the estimate of upward of 85 percent that Anthony Fauci, a key presidential advisor during the pandemic, suggested would be needed to achieve herd immunity. Since then, demand for updated COVID vaccine formulations has collapsed, driven by a broader vaccine fatigue that is now also manifesting as hesitation in routine childhood immunizations. Vaccines designed to intercept biological threats before they cause widespread harm—the type of rapid response the new crop of biodefense funders hope to enable—may face even greater resistance. In survey research asking Americans if they would accept a Centers for Disease Control and Prevention (CDC)-recommended vaccine for bird flu, a disease that has so far only occasionally infected humans, less than four in 10 said they would.

Why trust in new vaccines can drop

At least three findings suggest that public acceptance of new AI-enabled countermeasures should not be an afterthought. First, novelty carries a penalty. A recent experiment presented adults with a fictitious influenza outbreak and a rapidly developed vaccine. Confidence in both safety and effectiveness was significantly lower for a novel platform than a traditional one. Introducing a trusted messenger did not close the confidence gap. A novel AI-designed product or platform will face this penalty immediately.

Second, confidence rarely returns once lost. Over the fall, OpenAI introduced 722 manuscripts detailing progress on some of the hardest problems in mathematics. The day after the announcement, the company withdrew three of them. For a company using its technology to solve the near-impossible, their success rate was extraordinary. But public health does not get the luxury of retractions. With vaccine and therapeutic introductions, even minor mishaps can cause persistent or permanent declines in confidence, especially when audiences are primed for skepticism. In 2013, the Japanese government suspended their proactive recommendation of the HPV vaccine to investigate unconfirmed media reports of adverse events among recipients. Vaccination rates initially plummeted from about 70 percent to less than 1 percent. Despite over a decade of extensive scientific investigations confirming the vaccine's safety and the government's eventual reinstatement of the recommendation, vaccination rates have yet to fully recover. Third, acceptance can suffer when speed outpaces evidence of harm. In 1976, the federal government mounted a swift and massive

vaccination campaign following a swine flu outbreak at Fort Dix, a US Army base in New Jersey. When the anticipated spread of disease never materialized, rare vaccine side effects became the dominant narrative. Routine influenza vaccination campaigns suffered in the following years, with patients frequently citing the fiasco to justify refusal.

Similarly, measles is now returning to communities that had forgotten its severe impacts, highlighting how vaccine uptake has declined as evidence of a pathogen's harm has become less salient. During COVID, public health authorities had months of accumulating disease burden, public discussion, and clinical evidence before introducing a novel prophylactic countermeasure. AI-driven solutions will usher in an exciting new era of health progress, but they are designed to disrupt this already accelerated timeline, potentially causing evidentiary and technical milestones that far eclipse social ones. Closing these gaps does not require slowing development. Instead, those deploying the capital currently flooding into AI biodefense must expand their definition of success beyond speed and experimental endpoints. This is particularly relevant for the philanthropic sector driving much of this mobilization. Philanthropic goals are already aimed at measurable impact, but translating technical moonshots into real-world outcomes requires social infrastructure.

The good news is frameworks to do this already exist in adjacent fields, with researchers actively developing strategies in behavioral science, community health, and other disciplines. Pre-bunking, for example, works like a cognitive vaccine, introducing individuals to defensive strategies against misinformation prior to exposure to inoculate them against future deception. Similarly, the trusted-messenger model recommends bypassing top-down expert lectures about the merits of vaccination and instead leveraging respected local figures and peers to tackle the underlying causes of hesitancy. Still, changing minds is notoriously difficult, and how contemporary vaccination attitudes will respond to AI countermeasures co-developed with Silicon Valley remains an open question.

Funders seeking to maximize their technical breakthroughs must ensure their capital also flows to this less glamorous work of social preparedness.

Trust in public health sits at historical lows, and trust in AI is lower still. We cannot assume that technical virtue alone will override this deficit. Securing public confidence requires early structural investment in the institutional credibility of the biological AI sector—long before a novel pathogen emerges.

Ben Rader is a computational epidemiologist who serves as the scientific director of Boston Children's Hospital's Innovation and Digital Health Accelerator and an assistant professor at Harvard Medical School. His research focuses on how we can leverage novel technologies to improve public health. He is a former US Army chemical, biological, radiological, and nuclear (CBRN) officer and an alum of the Johns Hopkins Emerging Leaders in Biosecurity Fellowship.

To deter bioterrorism, U.S. imposes new rules on ordering synthetic DNA

By Phie Jacobs

Source: https://www.science.org/content/article/deter-bioterrorism-u-s-imposes-new-rules-ordering-synthetic-dna

Nov 09 – As concerns mount that artificial intelligence could make creating dangerous pathogens even easier, U.S. government–funded scientists who make and manipulate DNA sequences will face tougher regulations.

The National Policy for Nucleic Acid Synthesis Screening, released on 5 November, will for the first time require these researchers to procure synthetic nucleic acids

and benchtop synthesis equipment from U.S.-approved suppliers. Those vendors must verify their customers' identities and screen orders for potentially dangerous sequences that, for example, could encode toxins or pathogens. The policy, whose requirements will roll out in stages over the next 340 days, replaces a voluntary system of self-regulation, and some biosecurity experts view it as an important, if partial, step in the right direction. "It's great, because it does something instead of nothing," says Kevin Esvelt, a biotechnologist and biosecurity expert at the Massachusetts Institute of Technology. "It will make it harder to misuse DNA." Still, some key wording is vague, he and others say, and the policy only applies to federally funded scientists. But Esvelt believes it will spur synthetic biology companies to comply with the screening requirements for all customers, making it more difficult for "competent lone wolves" to obtain synthetic DNA sequences for nefarious purposes. Others caution that the new rules provide an imperfect shield against bioterrorism. "We're only addressing the U.S. with this policy," says Gigi Gronvall, an immunologist and biosecurity expert at Johns Hopkins University. Gronvall also worries that by focusing on synthetic DNA, the regulations do not address other ways a would-be bioterrorist could create a dangerous pathogen. "There's all kinds of other ways to manipulate DNA that do not require you to make it from scratch," she says.

Scientists have been making synthetic DNA for decades, but advances in technology over the past few decades have made it possible to produce longer and longer sequences that can be assembled into genes or even whole bacterial and viral genomes. Biology labs frequently order these sequences online from synthetic biology companies, but benchtop DNA synthesizers now enable scientists to create what they want in-house, further eroding obstacles to bioterrorism. In 2010, the U.S. government released guidelines for synthetic biology companies, recommending they vet customers and screen orders for potentially dangerous DNA sequences. The guidelines were voluntary, and various biosafety groups have called for greater oversight. But many companies—most notably the members of an industry group called the International Gene Synthesis Consortium, which is responsible for most DNA synthesis worldwide—agreed to comply anyway. Now, "Screening moves from voluntary to verified," says Drew Endy, a synthetic biology researcher at Stanford University. That's "a real step forward."

But Esvelt points out the policy only requires screening for DNA sequences 50 base pairs or longer. A would-be bioterrorist, he argues, could easily stitch together a dangerous sequence from much smaller fragments ordered from multiple different suppliers. Esvelt says he has built an algorithm capable of screening sequences as short as 30 base pairs for their risk potential and made it freely available. "That's the main flaw in an otherwise pretty great policy," he says. "Don't bother building a fence if there's going to be an obvious huge gap in it."

Another concern is that the policy requires DNA synthesis companies to verify customers' identities, Esvelt notes, but doesn't explain in detail how: "It's very underspecified in that regard." Gronvall also points out the policy only applies to newly built DNA synthesis equipment, leaving countless existing benchtop machines open to misuse. "These things are everywhere," she says. And although the policy encourages manufacturers to offer trade-in or buy-back programs for now obsolete machines, it doesn't mandate them.

The policy places the onus on the National Institute of Standards and Technology (NIST) to ensure the new regulations are correctly enforced—without necessarily providing the resources for them to do so. "NIST is being asked to do a lot of work here, on a short clock, only if money is available," Endy says. "I'm guessing they don't have the money."

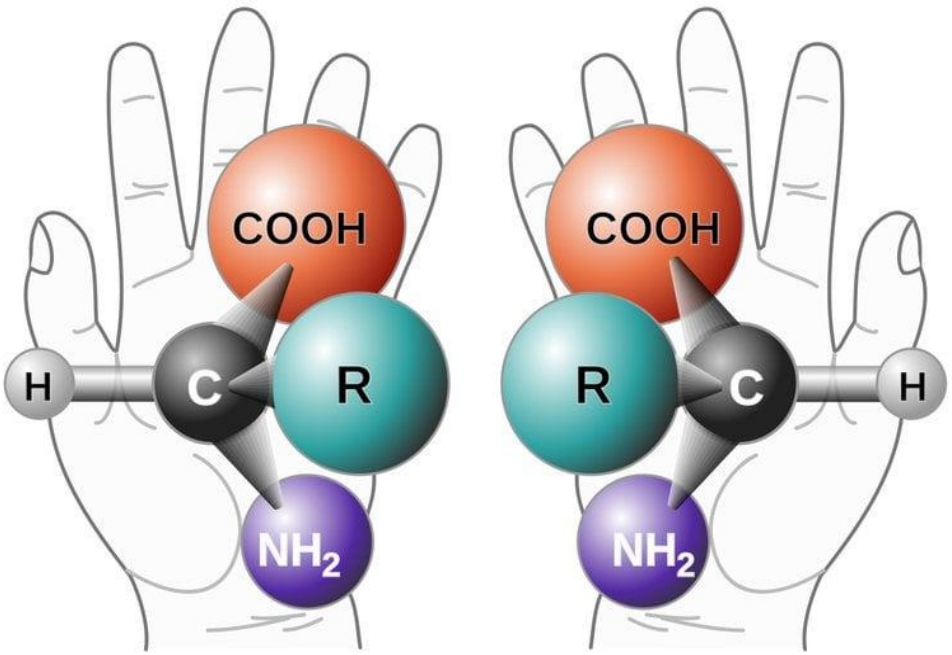
Esvelt also predicts the policy will create additional work for

institutional biosafety officers: “I think the greatest flaw in this policy is that it doesn’t come bundled with extra funds for institutional biosafety committees and biosafety officers, who do very important work and are dramatically underfunded.”
Gronvall, for her part, thinks too much emphasis has been placed on trying to prevent a specific type of bioterror threat, noting that screening for synthetic DNA, though necessary, is “just one tool.” More resources, she argues, should be devoted to vaccine development, hospital preparedness, and other measures that will be necessary to respond to future pandemics—be they natural or humanmade.

Scientists Fear 'Mirror Life' Could End Humanity, But We May Now Be Able to Detect It

By David Nield
Source: https://www.sciencealert.com/scientists-fear-mirror-life-could-end-humanity-but-we-may-now-be-able-to-detect-it

Nov 14 – Many scientists are seriously worried about the potential threat of 'mirror life': hypothetical organisms built from molecules that are flipped from what we find in nature.
Many of life's basic building blocks, including DNA and amino acids, have a certain 'left- or right-handedness'.
If that were to be flipped, like a DNA double helix twisting to the left instead of the right, then these looking-glass versions of life could sneak past the biological defenses of animals, plants, and humans.
It's worth emphasizing that mirror life hasn't been discovered or developed yet.

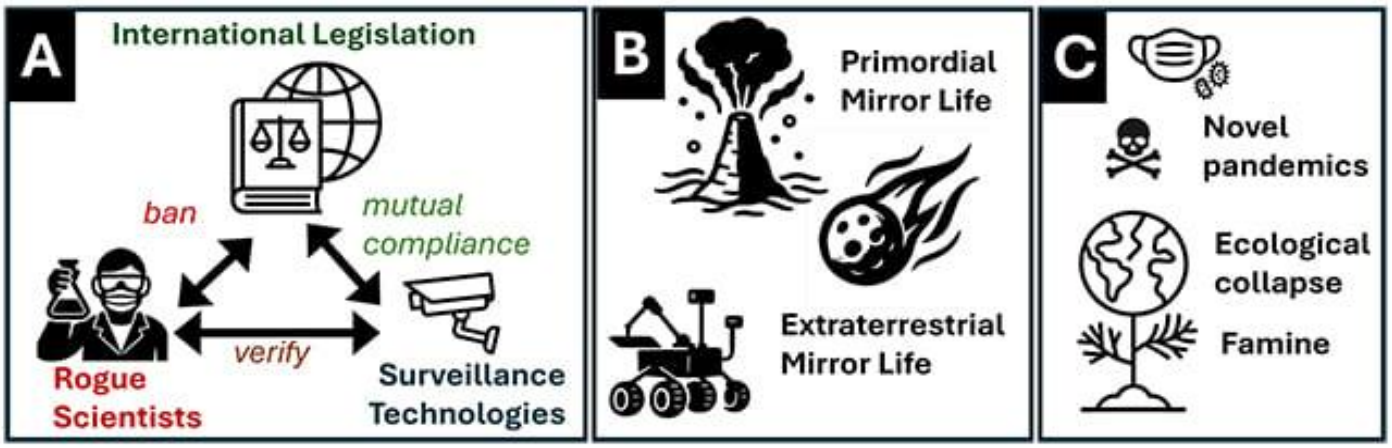


A left-handed and a right-handed amino acid. All amino acids on Earth are left-handed. (NASA)

However, researchers from the University of Strathclyde and Durham University in the UK have published a possible method of detecting the threat in *Royal Society Open Science*.

The method is based on circularly polarized luminescence (CPL), a special property of light that can reveal something's handedness (also called its chirality) by the way its waves twist like a corkscrew as they travel.
"Mirror life presents a low-likelihood but high-severity global biosecurity threat that has attracted the attention of bioscientists, governments and international security organizations," write the researchers in their published paper.

"In this perspective, we have set out the first known assay principle to discriminate against mirror life."



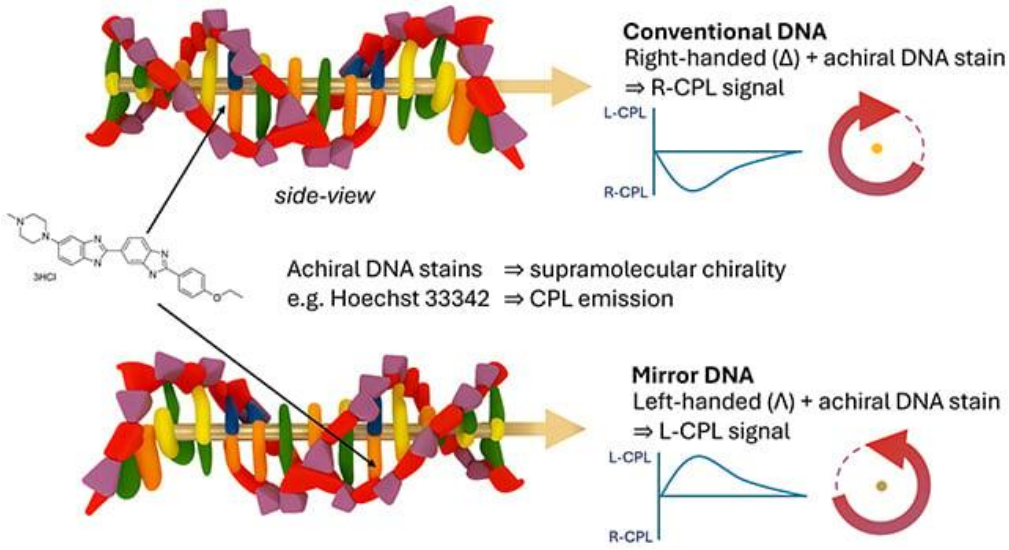
The researchers identified some potential sources and consequences of mirror life. (MacKenzie et al., *R. Soc. Open Sci.*, 2026)

Circularly polarised light isn't new – it's used in some cinema 3D glasses, for example – but here the researchers suggest that by adding fluorescent probes to a sample, then measuring the way that light spirals from it, mirror life could be detected.

No tests were run for this study, but the authors describe how existing CPL detection technology could be adapted into cameras, microscopes, and other types of scanners looking for reversed molecular structures.

"Assuming that mirror life is chemically analogous to conventional terrestrial life, these CPL signals could, in principle, be used to assess chirality and thereby provide a method for screening against mirror life," write the researchers in their published paper.

One of the key benefits of CPL detection is that mirror-life organisms wouldn't need to be developed to test it, and the study team also suggests that several different probes could be used in tandem to reduce the chances of false positives.



A DNA helix is one of the molecular building blocks that could be reversed. (MacKenzie et al., *R. Soc. Open Sci.*, 2026)

Next, the researchers want to put some of these probes to the test on ordinary cells, which will tell us more about how their flipped versions could be detected. There's still plenty of work to do in fine-tuning the light detection and fluorescent staining parts of the process. "We encourage other researchers who are experts in these techniques to consider how methods and equipment could be adapted and used for screening against mirror life, and where complementary analysis may be practicable," write the researchers. Part of the problem in preparing for any mirror life threat is that it doesn't exist yet – or at least we

haven't found it. In addition to being developed in biological labs, the researchers suggest it might be present on other planets or even in isolated parts of Earth, though they see these as much less likely.

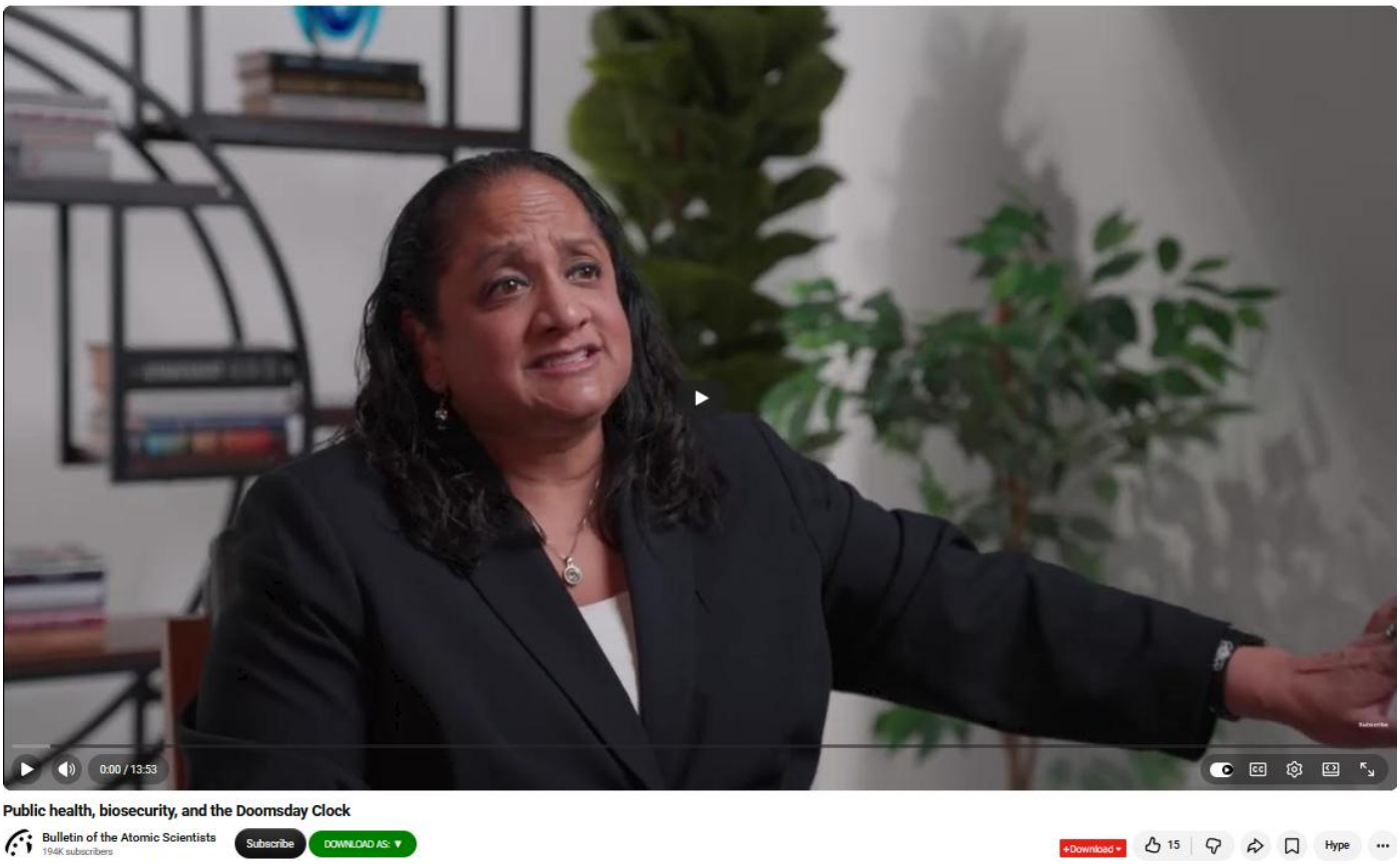
One of the biggest concerns is around mirror life bacteria, which might be able to render existing drugs useless – set up as they are for a certain molecular chirality – and lead to global pandemics that can't be controlled.

Several scientific and regulatory bodies have now recognized the potential danger of mirror life and are calling for tight restrictions on the development of mirror bacteria in the lab – though of course there might always be bad actors who ignore the rules.

Our best way of protecting ourselves is to build detectors and countermeasures before mirror life appears – and this study is a notable step towards that.

"The CPL method could provide a first-line assay for identifying extant mirror life biohazards, while also offering a foundation for bio-surveillance efforts that would likely be necessary for practical safeguarding against artificial mirror life," write the researchers.

●▶ The research has been published in *Royal Society Open Science*.



Asha M. George, DrPH, is the WMD Co-Chair of the National Security Reform Commission. Previously, she served as Executive Director of the Bipartisan Commission on Biodefense and in the US House of Representatives as subcommittee staff director and senior professional staff at the Committee on Homeland Security.



Rue de la Vacherie, 78 | B5060 SAMBREVILLE (Auvelais) | Belgium
https://www.ici-belgium.be/