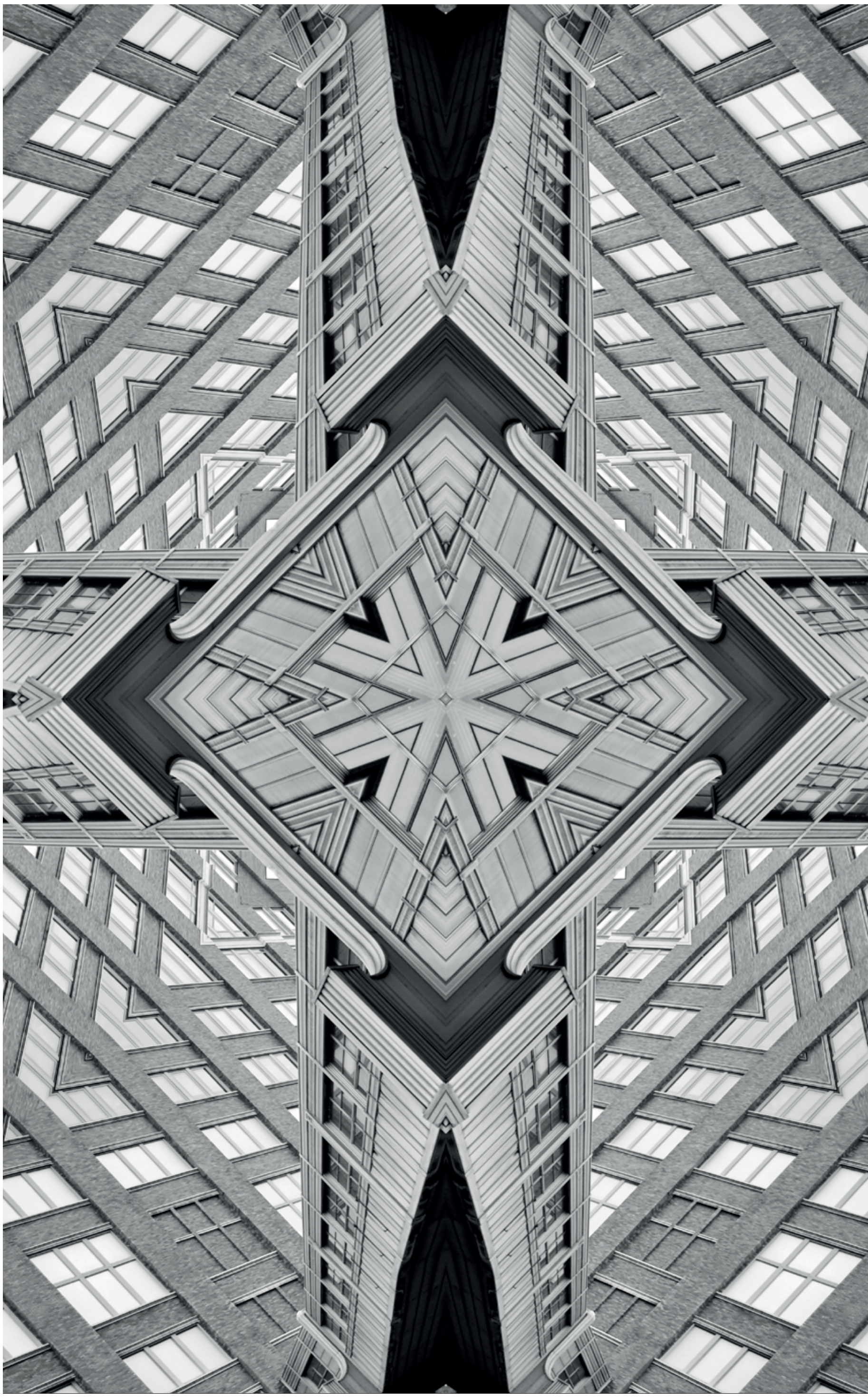
ORF OBSERVER RESEARCH FOUNDATION

Issue Brief

ISSUE NO. 768
DECEMBER 2024



Emerging Technologies in the Development and Delivery of CBRN Threats

Shravishtha Ajaykumar

Abstract

Non-conventional weapons, specifically, Chemical, Biological, Radiological and Nuclear (CBRN), pose threats to civilian safety, national security, and environmental sustainability. These threats are amplified by the use of emerging technologies such as Large Language Models, 3D printing, and drones, which can make the development and deployment of CBRN weapons easier and the implementation of countermeasures more challenging. This brief discusses emerging CBRN threats, focusing on the challenges posed by new technologies, and offers recommendations to mitigate such risks, including domestic regulation and global collaboration.

Attribution: Shravishtha Ajaykumar, "Emerging Technologies in the Development and Delivery of CBRN Threats," *ORF Issue Brief No. 768*, December 2024, Observer Research Foundation.

Introduction

The threat of Chemical, Biological, Radiological and Nuclear (CBRN) terrorism gained global attention in the late 20th-century as non-state actors began to explore its potential. One of the most notable incidents in the use of chemical weapons occurred in 1995, when the Japanese cult Aum Shinrikyo carried out a sarin gas attack on Tokyo's subway system[1] that killed 13 people and injured thousands. Such incidents highlight the vulnerability of civilians to chemical terrorism and demand the attention of stakeholders.[2]

In 2001, the biological agent anthrax was used to lace letters mailed to various media outlets and government offices.[3] These attacks, occurring shortly after 9/11, intensified global fears about non-state actors acquiring and using biological agents. Although the attacks were limited in scope, they showed how biological materials could be weaponised and used to cause widespread fear.

The threats posed by CBRN materials persist, with CBRN threats being used as tools for strategy, deterrence, and conflict. For instance, in the Russian-Ukraine war, Russia has made repeated threats to use nuclear weapons, particularly to deter NATO intervention.[4] More recently, non-state organisations like the Islamic State (IS) and Al-Qaeda have expressed their interest in CBRN capabilities.[a,5,6]

CBRN threats are also frequently used in high-conflict spaces. The collapse of state control in certain regions has exacerbated concerns that chemical weapons might fall into the hands of terrorists. In Syria, both the state and Daesh have used chemical weapons, including sarin and chlorine.[7]

[a] The sentiment was shared by stakeholders interviewed by the author, including Col (Dr) Ram Athavale, (Retd), expert in CBRN security.

Emerging Technologies and CBRN Threats

CBRN threats are not as direct as the use of conventional weapons. That the materials can be used without a 'launch' or a 'trigger' and are easily accessible add to the threat dynamics. They are also distinct from conventional terrorism because of their potential to cause large-scale destruction, long-term health effects, and environmental damage. These weapons also have a psychological impact, fostering fear, uncertainty, and panic. Therefore, CBRN threats are often referred to as low-probability, high-impact threats. They can manifest in three ways:

- A direct CBRN attack on people or the environment
- An explosive or cyberattack on critical infrastructure or supply chains that may host CBRN materials
- A natural disaster or act of negligence that may result in a leak of CBRN materials

Compounding the concerns are emerging technologies and their disruptive capacity; what were previously low-probability threats have become easier to access, develop, and deploy. This shift necessitates a re-evaluation and adaption of security measures to effectively address the risks posed by these new technologies. Emerging technologies impact two variables in the equation of CBRN threats: knowledge and development, such as through Large Language Models (LLMs), additive manufacturing, and development of agents using technologies such as CRISPR; and delivery systems, primarily through drones.

Table 1: Emerging Technologies and Their Impact on CBRN Security

Emerging Technology	Nuclear Security	Radiological Security	Biological Security	Chemical Security
Knowledge and Development				
LLMs and Artificial Intelligence (AI)	AI could optimise nuclear threat detection, help target nuclear sites, and enable the development of nuclear weaponry.	Could provide knowledge on radiological dispersal devices and improvised radiological bombs.	LLMs and AI can facilitate the design of biological agents, including viruses, bacteria, and toxins.	LLMs can generate chemical agents' structural analogues, aiding in the production of toxic substances (e.g., VX nerve agent).
3D Printing	Can produce components for nuclear weapons or delivery systems, though highly regulated.	Can be used to create radiological dispersal devices or other components of a dirty bomb.	Can manufacture parts for biological agent delivery systems or biological weapons.	Can be used to create devices for chemical dispersal or delivery systems.
Synthetic Biology (e.g., CRISPR)	It has no direct impact on nuclear security.	It has no direct impact on radiological security.	CRISPR can be used to engineer pathogens, making them more virulent or resistant to treatments, raising the threat of biological warfare.	CRISPR could assist in modifying organisms to produce bio-chemical toxins.

Emerging Technology	Nuclear Security	Radiological Security	Biological Security	Chemical Security
Cyber Technologies	Cyberattacks could disrupt nuclear plant operations, potentially releasing nuclear materials.	Cyberattacks could compromise security at radiological sites, allowing access to or releasing radioactive materials.	Cyberattacks could target labs or production facilities, releasing or altering biological agents.	Cyberattacks could turn off chemical containment systems, leading to the release of toxic substances or disrupting monitoring systems.
Delivery Systems				
Uncrewed Aerial and Ground Vehicles (Drones)	Drones could be adapted to deliver nuclear payloads or to bypass security at nuclear plants.	Drones can be used to deliver radiological dispersal devices or conduct surveillance on radiological sites.	Drones can deliver biological agents, bypassing security to release pathogens in populated areas.	Drones could carry chemical agents for precise, widespread delivery in a CBRN attack.

Source: Author's own, based on interviews with stakeholders.

Knowledge and Development

LLMs and the Democratisation of Knowledge and Accessibility

A primary concern around the use of emerging technologies is the increased accessibility that they allow to information and materials that can enable CBRN attacks. Recent developments in LLMs have complicated the landscape of CBRN terrorism. LLMs provide easy access to otherwise publicly available but hard-to-find information, effectively democratising scientific knowledge. This enables terrorists to bypass conventional intermediaries or online groups and directly obtain the instructions that they need for the production of CBRN weapons.[8] Although no agency has yet announced the development of new bio-agents or chemical compounds through the use of AI for warfare, the risk they pose remains urgent.[9]

For example, Chemical Language Models (CLMs) can generate molecules with targeted properties.[10] Experiments have demonstrated that LLMs have been validated to work with datasets that are assembled from toxic substances such that they design structural analogues for highly reactive members of such agents—for example, torture agents like the VX[b] nerve agent as weaponised by doomsday cults like Aum Shinrikyo.[11] If known, a future terrorist or cell could easily manufacture more sophisticated chemical agents.

LLMs have already been shown to aid in the biological warfare design of biological agents. LLMs can also provide an audience with little expertise fundamental details about laboratory devices, DNA sequences, and reverse genetics on influenza viruses.[12] Moreover, models such as ProtGPT2 and ProGen,[c] used for protein design, could be used to alter the protein structures of toxins such as ricin, thus providing future agents with formulations that escape detection and might constitute a grave threat.[13]

3D Printing

While commonly accessible materials are a greater risk, even parts of devices that were previously behind heavy barriers are more easily accessible. The protection levels associated with CBRN materials, including complex supply chains, are being overcome through the use of additive manufacturing (more commonly known as 3D printing).[14] Additive manufacturing has made it easier for non-authorised parties to independently manufacture components such as detonators or dispersal devices for chemical and radiological weapons.[15] The use of 3D printing weapons is not uncommon and has been seen in many non-state actors. Even larger groups like Al-Shabaab have been reported to use 3D printing to manufacture weapons and explosives.[16]

Large-scale CBRN attacks using 3D-printed components are yet to be recorded; however, terrorists have expressed an interest in using other forms of 3D-printing technology in their armaments.[d,17] As terrorist groups begin to use weapons such as 3D-printed firearms or explosive devices, they will likely make the leap to target CBRN delivery systems.

[b] Short for venomous agent X—a nerve agent more toxic than sarin.

[c] LLMs that are used to study the protein breakdowns of biological and chemical agents.

[d] Many individual and non-state actors, globally, have used 3D printing to manufacture weapons. While they have not been used to print WMD weapons so far, experts are concerned on the inaibility to detect 3D printed weapons that are usually made of plastic and lighter than metal, or undetectable by metal detectors.

3D printing, through computer-aided design, could equip terrorists to respond to the challenges posed by CBRN. 3D-printing technologies allow the designer or creator to rework the designs, use different versions, and innovate to produce weapons components. The open-source publication of this technical knowledge has further democratised technologies, allowing small, motivated groups that never had the infrastructure and expertise for CBRN operations to become capable developing and deploying these technologies. This democratisation of weapon-making tools raises the alarm for future CBRN incidents.[18]

Advancements in Toxin and Explosive Development

The development of new biological and chemical toxins is increasingly becoming a concern with the use of AI. Besides AI, synthetic biology, particularly the gene-editing technology CRISPR, has implications for the future of biological warfare. CRISPR, which is used to help address drug resistance in viruses, can also assist in making viruses more virulent and resistant to treatment.[19] This has raised concerns about malicious actors being able to engineer pathogens virulent enough to bypass vaccines.

Since biological attacks are difficult to attribute, this increases concerns about their potency, the ability to curb it in time based on response methods, and to limit the spread of such an attack into a more serious outbreak. The Cologne ricin plot of 2018 illustrates this point. The attacker, guided solely by online tutorials, was able to acquire and weaponise ricin, a highly toxic biological agent, with the aim of poisoning "unbelievers" in Germany.[20] They accessed the instructional materials that were distributed through Telegram—a platform commonly used by extremists for secure communication.[21]

Delivery Systems

Drone Technology

Drones are now easily accessible; even drones originally meant to be sold as toys can be enhanced to act as long-range delivery systems. Such drones, whether adapted or engineered, offer terrorists the ability to bypass traditional security measures. Groups like Al-Qaeda have already considered using drones for CBRN-based attacks, as seen in the thwarted plot in Iraq in 2013, where drones were planned to be used to disperse sarin gas and mustard agents.[22]

Equipped with sophisticated navigation systems and capable of carrying payloads, drones could target vulnerable populations or even critical infrastructure such as nuclear reactors or chemical plants.[23] This development complicates traditional counterterrorism measures, as stopping a drone-based CBRN attack requires a different set of security protocols such as drone detection and neutralisation systems.

An example of this is seen in the use of drones by the IS. The IS has allegedly carried out multiple chemical attacks, particularly involving the use of chlorine and mustard gas, in Iraq and Syria.[24] While these chemical weapons were often deployed through traditional means such as mortars or improvised explosive devices (IEDs), the group has also demonstrated an interest in using drones as a delivery platform for CBRN agents.[25] To this end, the IS had repurposed commercially available drones, which were initially intended for surveillance or bombings, to drop chemical agents on their enemies. Although these efforts were experimental, they highlight the potential use of drones even by non-state actors.

Sophisticated Targeting and Automation

AI and automation add another layer to the discernment of the delivery mechanisms for CBRN terrorism. AI can enhance the precision of attacks, enabling terrorists to target critical infrastructure, government facilities, or densely populated areas with greater accuracy. Through machine learning, AI systems can analyse vast amounts of data, identify vulnerabilities in defence systems, and optimise the delivery of CBRN agents to maximise casualties or disruption.[26]

AI could also help automate various stages of an attack, reducing the need for direct human involvement. For instance, an AI-enabled drone swarm could be programmed to release chemical or biological agents in multiple locations, making it harder for security forces to intercept or contain the attack. Moreover, AI-driven cyberattacks could sabotage critical infrastructure during a biological attack, overwhelm response efforts, and exacerbate the damage caused by the initial incident.[27]

State-sponsored CBRN attacks also hint at how more elaborate technologies can be deployed in terrorist activity. One such case is the 2018 Novichok poisoning of Sergei Skripal, where a Russian nerve agent was used in what was ultimately an attempted assassination.[28] Novichok is Russian Cold War-era poison and is an indicator of how sophisticated chemical agents can be leveraged to perform a targeted attack.

Although the Novichok chemical agent was activated by a state, its application within a civilian context raised alarms about the means by which non-state actors and criminal organisations can use advanced technology and chemical agents to harm a large general population. This also emphasises the difficulty of sensing and reacting to chemical weapons in heavily populated areas, where the initial identification of the agent is crucial yet often delayed.

Another critical case was the 2006 poisoning of former FSB agent[e] Alexander Litvinenko, who was administered a lethal dose of polonium-210, a radioactive substance, in what ultimately became a high-profile assassination.[29] Polonium-210 is a rare and highly dangerous isotope, and this case highlights how radioactive materials can be used for targeted attacks, raising concerns about the potential for nuclear or radiological weapons to be deployed covertly.[30]

The dual use of conceiving and developing emerging technologies poses complications in controlling and overseeing the adoption of such technologies. This is because most of the technologies that can be weaponised for a CBRN terrorist attack have simultaneous civilian purposes.[f,31] Therefore, stringent regulations would risk disrupting the progress of even benign endeavours. This inability to regulate only the malicious use of technologies without impacting the intended use and innovation are further exacerbated by the fact that emerging technologies are global in their scale. The easy availability of many technological parts and even know-how across borders makes it arduous, if not impossible, for any state to police or even imply restrictions on the said parts and know-how. While inter-state collaborations are necessary to create workable regulation systems, the differences in countries' laws and regimes may obstruct the possibility of creating a standard system.

[e] Federal Security Service of the Russian Federation

[f] CBRN technologies themselves are dual use; CRISPR is used for improving human health and can be used for increasing virulence in biological threatening agents; chemicals such as chlorine are listed as highly toxic but used in many industrial applications; radiological materials have applications in hospital equipment. Similarly, technologies such as AI are used to increase the accessibility of data or analyse data rapidly; drones are sold as toys and tools in photography.

The dual-use nature of emerging technologies has had an inadvertent impact on CBRN threats. These innovations can potentially enhance the capabilities of terrorist organisations, non-state actors, and non-authorised groups to complicate traditional security frameworks, resulting in gaps in preparedness and response systems. Existing security structures may need help to adapt to these technological advancements.

Lack of Regulation and the Oversight of Emerging Technologies

A pressing challenge is the lack of adequate regulation and oversight surrounding emerging technologies that can be exploited for CBRN purposes. Technologies such as synthetic biology, drone systems, and 3D printing are primarily developed for legitimate commercial or research applications. However, their dual-use nature means that malicious actors can repurpose them for CBRN attacks.

Synthetic Biology and Toxin Development

The threat is particularly severe for synthetic biology. CRISPR-like technologies are advancing much faster than regulatory frameworks can keep up.[32] Most countries still need to establish rigorous mechanisms for controlling the tools in gene editing, enabling relative ease of access for individuals who have only average biological knowledge. Additionally, many biological research tools are shared openly in the scientific community, creating opportunities for biosecurity vulnerabilities.[33]

The lack of global governance means that terrorist groups or lone actors can exploit the technology to create biological weapons, evade detection systems, or engineer pathogens that are resistant to vaccines or treatments. Current biosafety frameworks have been found to be insufficient in monitoring these technologies due to the latter's increasing capacity and use.

In one reported instance, an anthrax outbreak in parts of Kenya in 2016 led to deaths among livestock, and affected a number of people too.[g,34] The Kenyan government and intelligence services suspected a link between the outbreak and terrorist activities, potentially by groups like Al-Shabaab[h] or Islamic State (IS).[35] Reports claimed that Al-Shabaab might have been implicated in the use of anthrax as a form of biological warfare. However, there was little proof to support the accusations besides the Kenyan government's speculation that

[g] Anthrax is caused by the bacterium Bacillus anthracis, which can be fatal to both humans and animals. The disease typically spreads directly from infected animals to uninfected animals through contact with contaminated animal products.

[h] An Islamist terrorist group in east Africa and Somalia.

the territory was a potential arena for IS-supported actions, given the larger involvement of IS in some areas of East Africa and the Horn of Africa. Kenyan authorities and international health organisations like the World Health Organization (WHO) conducted investigations into the outbreak. However, concrete evidence of IS involvement was never publicly presented.[i] One of the challenges in this case was the difficulty in determining the exact source of the anthrax, specifically whether it was naturally occurring in livestock or intentionally introduced as part of a terrorist plot.

Drones

Though many countries have started implementing drone regulations, from determining sizes that need to be registered to restrictions on the depth under which they can operate, effective enforcement remains an issue.[36] The pace at which drone technology is evolving also presents a continued challenge.

Autonomous weapons systems, particularly drones, pose threats as they are less human controlled and risks associated with the identical targeted CBRN payloads are high; there is an urgent need for human interventions to regulate these systems properly.[37] Existing automated weapons could introduce a range of complications regarding the loss of human control over critical decisions, with critical implications in applications of weapons of mass destruction. The delivery of CBRN agents by these systems would allow them to be used without proper verification or sanctioning, which could have catastrophic consequences.[38] This also includes accidental use, miscalculation, or the hacking of systems. These factors necessitate resilient international regulation, ethical guidance, and transparency in monitoring systems to avert their misuse. The absence of regulation can lead to the unfettered proliferation of automated weapons that can be used to attack global stability and exacerbate the effects of warfare using weapons of mass destruction.

Gaps in Detection and Response Systems

Cyberattacks in the CBRN context add another layer of complexity. For example, a cyberterrorist can disrupt the computer system that operates critical stations managing the storage or transport of hazardous materials to result in the release of these materials. Targeting emergency response systems in a coordinated manner could cause delays or the cessation of mitigation efforts during a CBRN event. The principles of anonymity in cyberattacks also impact taking responsibility, further complicating preventive measures and pass-through efforts in case of the incidents.[39]

[i] The example was also shared with the author in an interview with Col (Dr) Ram Athavale (Retd), CBRN Security Expert.

Synthetic biology, which enables the manipulation of genetic material to create or alter organisms, presents new challenges for detecting and preventing biological terrorism. Unlike conventional biological weapons that rely on naturally occurring pathogens, synthetic biology permits the design of entirely new or modified agents that could evade current detection systems' sensitivity and specificity.[40] Engineered pathogens would be capable of escaping vaccine treatments or surveillance systems, thus challenging containment measures against outbreaks as they occur. While highly sophisticated sensors and detection tools are available against agents like *Bacillus anthracis* or variola, these systems can only promise that they will be effective against genetically modified organisms or pathogens that produce slower evidence of disease. This presents a gap in the real-time and rapid containment and neutralisation of response systems for any bioterrorism CBRN event.[41]

Chemical detection systems that correspond to known agents such as sarin, VX, or mustard gas also use new delivery methods. The use of micro-determined mechanisms for chemical agents, particularly in drones, complicates their detection and interception. Some classical defence systems, such as ground-based sensors and manual monitoring, are not in a position to detect and neutralise chemical agents dispatched in drone swarms or automated systems in time to avert the full severity of the attack.[42]

Detection systems can also be used to identify radiological bombs as having qualities that may cause panic and require the impacted area to be closed down as in the case of a nuclear attack. The use of dirty bombs with detection systems that may misread or misattribute the levels of concern—be it lowered concern in terms of biological or chemical release or increased concern with respect to a radiological bomb—highlights the need to improve current detection methods to ensure that they align with how information is shared with the public.[43]

Insufficient Integration of AI and Data Analytics in CBRN Defence

Emerging technologies like AI and machine learning offer great potential for improving CBRN defence systems, but these technologies need to be fully integrated into current security frameworks. AI could enhance detection, surveillance, and response capabilities by analysing large volumes of data in real time, identifying patterns indicative of CBRN threats, and optimising response strategies.[44]

However, there is still a substantial gap between the potential of AI and its actual implementation in national security and critical infrastructures. Most CBRN defence systems rely on manual monitoring and threat assessment processes, are prone to human error, and responds slowly to rapidly evolving situations. Adversaries are also leveraging AI and machine learning. Terrorist groups could use AI to automate attack planning, identify vulnerabilities in critical infrastructure, and deploy AI-powered drones in coordinated CBRN attacks. Therefore, security stakeholders need to prioritise adapting to and regulating these technologies.

Cybersecurity Gaps in CBRN Infrastructure

Another emerging concern in CBRN terrorism is the integration of cyber capabilities and AI into attack strategies. Terrorist groups could exploit vulnerabilities in critical infrastructure systems through cyberattacks to release CBRN materials. This could lead to widespread contamination without the need for direct human involvement, making it harder to trace the source of the attack.[45]

Machine Learning algorithms could also optimise the deployment of CBRN agents. For example, AI could identify weak points in infrastructure or determine the most effective timing and location for an attack. AI-driven drones or robots could also autonomously deliver CBRN agents, reducing the need for human involvement and increasing the likelihood of success.[46] The growing accessibility of knowledge through AI models, online tutorials, and encrypted communication platforms makes it easier for terrorists to develop chemical and biological weapons. While technical limitations exist in mastering and weaponising CBRN materials, emerging technologies, including LLMs and online platforms, are closing these gaps. This necessitates a reassessment of global security measures to address the evolving threats posed by terrorists' use of emerging technologies in CBRN terrorism.

Cyberattacks targeting these systems could result in the accidental release of CBRN agents or sabotage key safety protocols, as seen in the Stuxnet cyberattack, which targeted Iranian nuclear facilities in 2010.[47] The attack caused disruptions by damaging centrifuges and delaying progress. It also exposed vulnerabilities in industrial control systems in Iran and other countries including India, spurring global investments in cybersecurity for critical infrastructure.[48] While the cyberweapon was attributed to a state-sponsored attack due to its complexity, it demonstrated the possibility of the cyber-sabotage of critical systems.[49] Similar tactics could be adopted by terrorist groups aiming to release or weaponise CBRN materials. Current cybersecurity measures in many CBRN-related facilities often need to be updated or improved to protect against sophisticated cyber threats.

In addition, cyberterrorists could hack into transportation systems or emergency response networks to delay or disrupt efforts to contain a CBRN incident. A coordinated cyberattack could amplify the impact of a physical CBRN attack, overwhelming response efforts and complicating efforts to mitigate the harm caused by the incident.[50]

Limited International Coordination and Information Sharing

CBRN preparedness requires coordinated international efforts, as the threats posed by these materials and emerging technologies are global. The lack of international coordination, information sharing, and cooperation among nations remains a severe barrier to effective CBRN defence. Many countries lack standardised protocols for sharing intelligence related to CBRN materials or emerging technology threats.[51,52] This is particularly problematic given the rapid global dissemination of new technologies such as drones, synthetic biology tools, and 3D printing. Terrorist groups could exploit these gaps to obtain technologies from one country and launch an attack on another.

Moreover, the distribution of open-source scientific knowledge and the global character of research provides hostile actors with quick access to specific fields such as synthetic biology and chemical engineering. Unless coordinated efforts are made to monitor and control these developments, security agencies may have little insight into terrorist groups' ability to launch CBRN attacks.

Given the gaps in CBRN preparedness, security frameworks need to evolve to ensure that they address increasing risks from emerging technologies. This entails the improved international regulation of dual-use technologies and detection systems as novel as synthetic biology, greater state integration of AI, and cybersecurity measures in national and global defence infrastructures. The cooperation and exchange of information between nations and the monitoring of technology defence should take precedence in shrinking the spectrum of CBRN terrorism.

Response Strategies and Policy Recomendations

The disruptive and dual-use nature of technology adds to CBRN threats at a global level. The first step to regulating and monitoring these would be to create technological safeguards, thereafter ensuring monitoring and regulation at a domestic level. The loop would then be closed through international accountability.

Technological Safeguards

- Advances in AI and cybersecurity are increasingly, and necessarily, at the centre of CBRN terror-risk mitigation. Technology can contribute to the enhanced ability to detect CBRN threats at early stages and to adopt practical response approaches to curb the attacks. AI-based systems can enhance the capacity to identify suspicious behaviours that would indicate a CBRN attack being planned, including unusual chemical synthesis and illegal trading of radioactive materials. AI can also be used to improve public health responses by rapidly analysing large amounts of data to monitor disease outbreaks or exposure to toxicants. Simultaneously, cybersecurity practices must be enhanced to stop the hacking of systems that deal with hazardous substances or biological agents. Beyond applying AI for detection, governments and intergovernmental organisations should prioritise the development of further technology-based countermeasures to prevent or reduce CBRN attacks. This includes the use of sophisticated diagnostic instruments to detect the availability of chemical or biological weapons in the event of a terrorist attack and the development and usage of decontamination technologies for civilians and first responders. This will also include protective equipment for CBRN response units that are enhanced with decontaminating materials and better detection systems.

Recommendation

It is important to invest in AI-based monitoring systems for early detection and real-time response to CBRN attacks. Such systems could also be applied to monitor chemical and biological research facilities, anomalous patterns of chemical production, and online activities to predict terrorist activities at an early stage. Governments also need to collaborate with cybersecurity companies to protect critical infrastructure from cyberattacks whose goal is CBRN materials theft or modification.

- Restricting the development of technologies that have beneficial uses, such as gene editing or AI for healthcare, while preventing their potential misuse in CBRN weapons, creates an ethical dilemma: Limiting access to these technologies will stifle innovation in fields with life-saving potential. This moral quandary for policymakers requires a more creative approach to regulating innovation.

Recommendation

To address the ethical dilemma, an ethics committee must be instated to oversee technologies relevant to CBRN materials and threats and the explosives that may accompany them. Such an ethics committee must be established under the mandate of a National Security Strategy or a similar document. The committee should include national security officials and legal experts to ensure compliance with laws and regulations. Scientific and technical experts, including chemists, biologists, and cybersecurity specialists, are essential to assess the risks and potential misuse of CBRN technologies. Additionally, human rights advocates and civil society members should be included to ensure that decisions respect fundamental rights and societal well-being. These bodies should assess the risks and benefits of new advancements in technology development, such as the limits of synthetic biology, AI, and nuclear technology, ensuring that safeguards are in place without stifling progress. Including private-sector partners in some of these boards will help address how technology can continue to prosper without pushing the limits of innovation to impact humanity negatively.

Regulatory Challenges

- The regulation of dual-use technologies is challenging because it entails balancing tensions between two competing ends: facilitating the creation and proliferation of an enabling technology and limiting or stopping its proliferation for detrimental reasons. While countries might be under pressure to develop new technologies, these same technologies raise ethical and regulatory concerns when diverted for harmful purposes.

Recommendation

As technology applications themselves are difficult to monitor, governments must ensure that the materials required to create CBRN threats and the technology components accompanied are well monitored. India, for example, must employ stricter export control laws to monitor dual-use technologies. India already has the SCOMET (Special Chemicals, Organisms, Materials, Equipment, and Technologies) declaration, which covers a list of materials and delivery systems that are highly monitored due to high risks, including drones, bacillus bacteria, and ricin.[53] However, materials that are trafficked or 3D printed or chemicals that can be freely traded and used to develop dangerous explosives such as chlorine are still concerning. Ideally, imposing such laws must be done by using a two-faceted approach. The first would be to include accountability for all critical technologies and their supply chains, as mandated by a national security document or the Ministry of Defence. The second would be incorporating supplier accountability in industry-specific regulations, focusing on operations and outcomes and the supply chain that precedes operations. To this end, technology components must be registered under the supplier. Suppliers for these critical technologies must also be regularly audited by a third-party auditor and held accountable for their products and parts. For example, an organisation that makes drones should have their products registered to prevent drone attacks and have a clear trail if their products are misused or components are adapted into weaponised versions of their product. The same holds for parts of the nuclear, chip, biotechnology, and chemical development supply chains.

- Response norms and tactics need to be reassessed. The threat of CBRN materials is both underestimated and overdramatised. Efforts to ensure public awareness are minimal and mostly voluntary, and reporting methods are few. Further, information and misinformation control is dispersed, making India vulnerable to the spread of misinformation and resulting in mass panic, even if there is no attack.

Recommendation

Few institutions, such as hospitals, have response mechanisms for chemical or nuclear exposure. Stakeholders such as doctors need to be trained in exposure treatments and waste disposal. Further, for doctors to be able to assess individuals, patients would need to report on symptoms. Therefore, public awareness is critical. The National Disaster Response Force (NDRF) has already created public awareness campaigns; however, these must also be disseminated in schools to ensure that everyone can access this knowledge.[54] Further, the national security strategy of India, or any other similar document, must highlight a minimum level of threat that requires sharing information of a possible attack with the public or with an international organisation. Both mechanisms would encourage accountability and ensure that a panic response is controlled if the threat turns out to be negligible.

Global Partnerships and Intelligence Sharing

- Knowledge-sharing and coordinated actions are essential for countermeasures against CBRN terrorism. Terrorist networks are transnational in nature, and thus, it would be challenging for any one state to tackle a threat by itself. International cooperation enables the convergence of resources, competence, and information, which improves the prospects of detection and prevention of CBRN attacks.

Recommendation

Strengthen multilateral intelligence-sharing initiatives through international organisations, including INTERPOL, the United Nations Office on Drugs and Crime (UNODC), and regional security arrangements. This would require each government to establish a nodal committee under the Border Security Forces that will determine threat levels and share the information with international intelligence agencies, thus enhancing their role in developing secure, end-to-end communication networks for the sharing of intelligence information regarding CBRN threats.

- International agreements such as the Biological Weapons Convention (BWC), the Chemical Weapons Convention (CWC), and the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) have been critical instruments in efforts to contain the diffusion of CBRN agents.[55,56,57] However, there is no treaty or international document in the area of radiological weapons and explosives.[58] This increases the risk of using radiological devices, more commonly called "dirty bombs", with other CBRN materials, such as exploding a dirty bomb in an industry laundry machine and exposing the area to aerosolised chlorine.[j] These agreements will need to adapt in order to remain meaningful in the face of new threats posed by non-state actors and terrorist groups. While most stakeholders are of the view that having specific technology bylines in these conventions may not have the desired impact, it is still essential to ensure that the technology does not go unmentioned.[k]

Recommendation

A convention must be established to monitor the use of radiological weapons, especially with other CBRN materials, that pose higher risks as a weapon of mass destruction. Further, stakeholders, including India, must revitalise and enhance the BWC and the CWC to handle new threats such as genetically engineered agents and the illegal production of chemical weapons. Specifically, while the norms themselves do not need to be adjusted, regular meetings should be held under them that highlight relevant technologies and encourage cooperation between countries and international organisations such as INTERPOL. These measures can help address challenges, including the trade of non-authorised devices, components, and materials that can be weaponised. These discussions must also include private actors to enable the design of a monitoring framework that can prevent CBRN terrorism. This may include an enabling conversation about regulating dual-use technologies and exchanging effective biosecurity and chemical security practices.

[j] The example was shared with the author in an interview by Col (Dr) Ram Athavale (Retd).

[k] This opinion was shared with the author in interviews with Amb. Rakesh Sood, Distinguished Fellow, Observer Research Foundation, Lakshmy Ramakrishnan, Associate Fellow, Observer Research Foundation, Col (Dr) Ram Athavale (Retd), Meghna Bal, Director, Esya Centre, and Lt Col Akshat Upadhya, Manohar Parrikar Indian Defence Studies and Analyses.

Conclusion

The multi-faceted nature and changing landscape of CBRN threats necessitate a comprehensive strategy incorporating enhanced collaboration between nations, regulating dual-use products, and leveraging the power of emerging technologies in areas such as AI and cybersecurity to identify and respond to CBRN threats.

India occupies a critical geographic location and geopolitical position. Therefore, while these threats impact the entire world, India must not wait for action from other states and should instead use its learnings from recorded incidents to enhance domestic law and international collaborations and secure the future of technological development without high risks.

Adopting existing frameworks, advancing technology-based countermeasures, and building international collaborations will allow governments to prepare for and try to prevent CBRN terrorism more effectively. Tackling these challenges through sound policy actions can protect the civilian population, national security, and the environment from the destructive consequences of CBRN weapons development and use.

Shravishtha Ajaykumar *is Associate Fellow, Centre for Security, Strategy and Technology, ORF.*

Endnotes

1 BBC News, "Aum Shinrikyo: The Japanese Cult Behind the Tokyo Sarin Attack," *BBC News,* July 6, 2018, https://www.bbc.com/news/world-asia-35975069.

2 BBC News, "Aum Shinrikyo: The Japanese Cult Behind the Tokyo Sarin Attack."

3 "History | Federal Select Agent Program," Government of the United States of America, https://www.selectagents.gov/overview/history.htm.

4 Mark S. Bell, "The Russia-Ukraine War and Nuclear Weapons: Evaluating Familiar Insights," *Journal for Peace and Nuclear Disarmament*, November 11, 2024, https://doi.org/10.1080/25751654.2024.2425379.

5 Sammy Salama and Lydia Hansell, "Does Intent Equal Capability? Al-Qaeda and Weapons Of Mass Destruction," *Nonproliferation Review*, November 2005, https://doi.org/10.1080/10736700600601236.

6 "Country Reports on Terrorism 2019 - United States Department of State," *United States Department of State*, May 10, 2021, https://www.state.gov/reports/country-reports-on-terrorism-2019/.

7 "Syria's Renewed Cooperation on Chemical Weapons File Bearing Positive Results, More Efforts Key to Close Outstanding Issues, Disarmament Chief Tells Security Council," United Nations, Meetings Coverage and Press Releases, June 11, 2024, https://press.un.org/en/2024/sc15725.doc.htm.

8 Nicolò Miotto, "The Potential Terrorist Use Of Large Language Models For Chemical and Biological Terrorism," European Leadership Network, April 5, 2024, https://europeanleadershipnetwork.org/commentary/the-potential-terrorist-use-of-large-language-models-for-chemical-and-biological-terrorism/.

9 Janet Egan and Erin Rosenbach, "Biosecurity In the Age Of AI: What's the Risk?," The Belfer Center for Science and International Affairs, November 6, 2023, https://www.belfercenter.org/publication/biosecurity-age-ai-whats-risk.

10 Francesca Grisoni, "Chemical Language Models For De Novo Drug Design: Challenges and Opportunities," *Current Opinion in Structural Biology,* February 2, 2023, https://doi.org/10.1016/j.sbi.2023.102527.

11 Hyukhun Koh et al., "Can LLMs Recognize Toxicity? Definition-Based Toxicity Metric," *Arxiv,* https://arxiv.org/html/2402.06900v3.

12 Emily H. Soice et al., "Can Large Language Models Democratize Access To Dual-use Biotechnology?," *Arxiv*, June 6, 2023, https://arxiv.org/abs/2306.03809.

13 Noelia Ferruz et al., "ProtGPT2 Is a Deep Unsupervised Language Model for Protein Design," *Nature Communications*, July 27, 2022, https://doi.org/10.1038/s41467-022-32007-7.

Endnotes

14 Marco Fey, "3D Printing and International Security: Risks and Challenges Of an Emerging Technology," Peace Research Institute Frankfurt, May 22, 2017, https://www.researchgate.net/publication/317175090_3D_Printing_and_International_Security_Risks_and_Challenges_of_an_Emerging_Technology.

15 Nicolo Miotto, "3D Printing and WMD Terrorism: A Threat In the Making?," *European Leadership Network, January 10, 2024* https://europeanleadershipnetwork.org/commentary/3d-printing-and-wmd-terrorism-a-threat-in-the-making/.

16 United Nations, "Letter Dated 19 July 2024 From the Chair Of the Security Council Committee Pursuant to Resolutions 1267 (1999), 1989 (2011) and 2253 (2015) Concerning Islamic State In Iraq and the Levant (Da'esh), Al-Qaida and Associated Individuals, Groups, Undertakings and Entities Addressed To the President of the Security Council," Security Council, July 22, 2024, https://documents.un.org/doc/undoc/gen/n24/191/91/pdf/n2419191.pdf.

17 Miotto, "3D Printing and WMD Terrorism: A Threat In the Making?"

18 Daniel C. Tirone and James Gilley, "Printing Power: 3-D Printing and Threats to State Security," *Journal of Policing Intelligence and Counter Terrorism*, July 3, 2015, https://doi.org/10.1080/18335330.2015.1089636.

19 Shuan Tao et al., "The Application of the CRISPR-Cas System in Antibiotic Resistance," *Infection and Drug Resistance*, August 1, 2022, https://doi.org/10.2147/idr.s370869.

20 Chase Winter, "Tunisian Planned Ricin Attack On German 'Unbelievers,'" *Deutsche Welle*, August 4, 2018, https://www.dw.com/en/german-prosecutors-tunisian-planned-ricin-terror-bombing-against-unbelievers/a-44949132.

21 Kristina Hummel, "The June 2018 Cologne Ricin Plot: A New Threshold In Jihadi Bio Terror - Combating Terrorism Center St West Point," Combating Terrorism Center at West Point, March 21, 2022, https://ctc.westpoint.edu/june-2018-cologne-ricin-plot-new-threshold-jihadi-bio-terror/.

22 Kerry Chávez and Ori Swed, "Off the Shelf: The Violent Nonstate Actor Drone Threat," *Air & Space Power Journal* (2020), https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-3/F-Chavez_Swed.pdf.

23 Ulzhalgas Seidaliyeva et al., "Advances and Challenges In Drone Detection and Classification Techniques: A State-of-the-Art Review," *Sensors*, December 26, 2023, https://doi.org/10.3390/s24010125.

24 "'Reasonable Grounds to Believe' Syrian Government Used Chlorine Gas On Douma Residents In 2018, Head of Chemical Weapons Monitoring Organization Tells Security Council," United Nations, Meetings Coverage and Press Releases, February 7, 2023, https://press.un.org/en/2023/sc15194.doc.htm.

25 United Nations Office of Counter-Terrorism, Global Counter-Terrorism Programme On Autonomous and Remotely Operated Systems (AROS Programme) and Conflict Armament Research, "Global Report On the Acquisition, Weaponization and Deployment Of Unmanned Aircraft Systems By Non-State Armed Groups For Terrorism-related Purposes," United Nations Global Counter-Terrorism Strategy, 2023, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/unoct_car_global_report_web_en.pdf.

26 Adib Bin Rashid et al., "Artificial Intelligence In the Military: An Overview Of the Capabilities, Applications, and Challenges," *International Journal of Intelligent Systems*, November 6, 2023, https://doi.org/10.1155/2023/8676366.

27 E. Pauwels, "Cyber-biosecurity: How To Protect Biotechnology From Adversarial AI Attacks," *Biology, Computer Science, Environmental Science,* 2021, https://www.semanticscholar.org/paper/Cyber-biosecurity%3A-How-to-protect-biotechnology-AI-Pauwels/cbcfd538d71301bc30804183da009060010ce840.

28 U.S. Mission Italy, "Putin's Poisons: 2018 Attack On Sergei Skripal - U.S. Embassy & Consulates In Italy," U.S. Embassy & Consulates in Italy, April 12, 2022, https://it.usembassy.gov/putins-poisons-2018-attack-on-sergei-skripal/.

29 BBC News, "Alexander Litvinenko: Profile Of Murdered Russian Spy," January 21, 2016, https://www.bbc.com/news/uk-19647226.

30 BBC News, "Alexander Litvinenko: Profile Of Murdered Russian Spy"

31 Patrick D. Ellis, "Lone Wolf Terrorism and Weapons Of Mass Destruction: An Examination Of Capabilities and Countermeasures," *Terrorism and Political Violence*, December 20, 2013, https://doi.org/10.1080/09546553.2014.849935.

32 Alberto Asquer and Inna Krachkovskaya, "Uncertainty, Institutions and Regulatory Responses to Emerging Technologies: CRISPR Gene Editing In the US and the EU (2012–2019)," *Regulation & Governance*, June 26, 2020, https://doi.org/10.1111/rego.12335.

33 James A. Smith and J. Sandbrink, "Biosecurity In an Age of Open Science," *PLoS*, 2022, https://www.semanticscholar.org/paper/Biosecurity-in-an-age-of-open-science-Smith-Sandbrink/3d4f01c99f36cc8ffcdaddeed375965f737b51a2.

34 BBC News, "Kenya Police 'Foil Anthrax Attack' By 'IS-Linked Group,'" *BBC,* May 4, 2016, https://www.bbc.com/news/world-africa-36198561.

35 BBC News, "Kenya Police 'Foil Anthrax Attack' By 'IS-Linked Group.'"

36 Arthur P. Cracknell, "UAVs: Regulations and Law Enforcement," *International Journal of Remote Sensing*, March 22, 2017, https://doi.org/10.1080/01431161.2017.1302115.

37 International Committee of the Red Cross, "Autonomous Weapon Systems:

Technical, Military, Legal and Humanitarian Aspects," *International Committee of the Red Cross*, March 2014, https://www.icrc.org/sites/default/files/document/file_list/4221-002-autonomous-weapons-systems-full-report.pdf

38 Zachary Kallenborn and Philipp C. Bleek, "Swarming Destruction: Drone Swarms and Chemical, Biological, Radiological, and Nuclear Weapons," *The Nonproliferation Review*, September 2, 2018, https://doi.org/10.1080/10736700.2018.1546902.

39 Shravishtha Ajaykumar, "Securing India's Critical Infrastructure: Prioritising Cybersecurity in Chemical Facilities," Observer Research Foundation, October 7, 2024, https://www.orfonline.org/expert-speak/securing-india-s-critical-infrastructure-prioritising-cybersecurity-in-chemical-facilities.

40 "Moving Forward: Conclusions and Recommendations," Chapter 9 in *Biodefense in the Age of Synthetic Biology*, June 19, 2018, https://www.ncbi.nlm.nih.gov/books/NBK535868/.

41 Vijai Pal et al., "Biological Warfare Agents and Their Detection and Monitoring Techniques (Review Paper)," *Defence Science Journal*, September 30, 2016, https://doi.org/10.14429/dsj.66.10704.

42 Justin R. Robinson et al., "Design and Test of an Autonomous Drone SWARM for Chemical Agent Detection," *AIAA AVIATION 2022 Forum*, June 20, 2022, https://doi.org/10.2514/6.2022-3847.

43 James Risser and Mark Saxon, "Systems engineering approach to chemical biological and radiological detection system design," IEEE International Conference on Technologies for Homeland Security (HST) (2011), https://www.researchgate.net/publication/261500259_Systems_engineering_approach_to_chemical_biological_and_radiological_detection_system_design

44 Tamás Kegyes et al., "Machine Learning -based Decision Support Framework for CBRN Protection," *Heliyon*, February 1, 2024, https://doi.org/10.1016/j.heliyon.2024.e25946.

45 Shravishtha Ajaykumar, "Securing India's Critical Infrastructure: Prioritising Cybersecurity in Chemical Facilities."

46 Miotto, "The Potential Terrorist Use of Large Language Models for Chemical and Biological Terrorism."

47 Sean Collins and Stephen McCombie, "Stuxnet: The Emergence Of a New Cyber Weapon and Its Implications," *Journal of Policing Intelligence and Counter Terrorism*, March 23, 2012, https://doi.org/10.1080/18335330.2012.653198.

48 "Connect the Dots on State-Sponsored Cyber Incidents - Stuxnet," Council on Foreign Relations, https://www.cfr.org/cyber-operations/stuxnet.

Endnotes

49 Marie Baezner, Patrice Robin, “Hotspot Analysis: Stuxnet,” *Center for Security Studies (CSS), ETH Zürich*, 2017, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf.

50 G. Loukas et al., “A Taxonomy of Cyber Attack and Defence Mechanisms for Emergency Management Networks,” *IEEE International Conference on Pervasive Computing and Communications Workshops* (2013), https://www.semanticscholar.org/paper/A-taxonomy-of-cyber-attack-and-defence-mechanisms-Loukas-Gan/d6df41ef7e6e7a151f2c57c993af28f85b6bd727.

51 Elham Anbari et al., “From Investigation of Hospital Protocols and Guidelines to Designing a Generic Protocol for Responding to Chemical, Biological, Radiological, and Nuclear Incidents,” *International Journal of Health System and Disaster Management*, January 1, 2015, https://doi.org/10.4103/2347-9019.162553.

52 Julie A. Bentz et al., “It’s All About the Data: Responding To International Chemical, Biological, Radiological, and Nuclear Incidents,” *Bulletin of the Atomic Scientists*, June 18, 2014, https://doi.org/10.1177/0096340214539117.

53 “SCOMET | Department of Chemicals and Petrochemicals,” Directorate General of Foreign Trade (DGFT), Ministry of Commerce & Industry, https://chemicals.gov.in/scomet.

54 “Disaster Awareness.” *National Disaster Response Force*,” *Ministry of Home Affairs*, https://www.ndrf.gov.in/hi/%E0%A4%86%E0%A4%AA%E0%A4%A6%E0%A4%BE-%E0%A4%9C%E0%A4%BE%E0%A4%97%E0%A4%B0%E0%A5%82%E0%A4%95%E0%A4%A4%E0%A4%BE.

55 “Biological Weapons Convention,” *UNODA*, https://disarmament.unoda.org/biological-weapons/.

56 “Chemical Weapons Convention,” *OPCW*, https://www.opcw.org/chemical-weapons-convention.

57 “Treaty on the Non-Proliferation of Nuclear Weapons (NPT),” *IAEA*, https://www.iaea.org/publications/documents/treaties/npt.

58 “First Committee Chair, Concluding Session, Says World Without Bedrock Treaties Banning Weapons of Mass Destruction Would Be ‘A Gloomy Place’ ,” United Nations Meetings Coverage and Press Releases, November 3, 2023, https://press.un.org/en/2023/gadis3733.doc.htm.

Images used in this paper are from Getty Images/Busà Photography.

ORF OBSERVER RESEARCH FOUNDATION

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. Fax : +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org