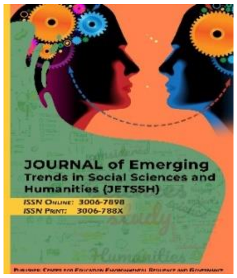

Journal of Emerging Trends in Social Sciences and Humanities

A Double-Blind, Peer-Reviewed, HEC recognized Y-category Research Journal

E-ISSN: 3006-7898 **P-ISSN:** 3006-788X

Volume 3 Issue 2, 2026, 243-252

Non-State Actors and Biological Threats: Revisiting Bioterrorism in the Twenty-First Century

Dr. Sultan Salah Ud Din[1]

[1] PhD in International Relations, Department of Politics and International Relations, International Islamic University, Islamabad, Pakistan.

Corresponding Author: Dr. Sultan Salah Ud Din, **Email:** sultan.phdir61@iiu.edu.pk

Article Information

Received:

2026-04-20

Revised:

2026-05-21

Accepted:

2026-06-22

Keywords

Bioterrorism; Non-state Actors; Synthetic Biology; Artificial Intelligence; Biological Weapons Convention; Biosecurity Governance; Global Health Security.

ABSTRACT

Bioterrorism remains a significant but contested dimension of international security, particularly as advances in synthetic biology, genome editing, artificial intelligence, and biological design are changing the technological environment in which biological threats emerge. This study re-examines the capacity of non-state actors to pose biological threats and addresses a gap in conventional debates that often focus either on the severity of the threat or on the practical barriers to its realization. Drawing on securitization theory, the study examines how biological threats posed by non-state actors are constructed as security concerns and how technological change may affect the relationship between intent and capability. It uses a qualitative comparative analysis of the Rajneeshee cult, Aum Shinrikyo, and Islamic State, together with an assessment of contemporary international biosecurity governance. The analysis finds that historical cases were constrained by limitations in specialized knowledge, access, dissemination, and organizational capacity, indicating that intent alone was insufficient to produce sustained biological violence. Emerging technologies may reduce some of these barriers, but technological progress does not automatically translate into operational capability; access, expertise, organizational capacity, and other institutional constraints remain important. The study further finds that existing frameworks, including the Biological Weapons Convention, dual-use research governance, and the Global Health Security Agenda, provide important foundations but remain fragmented in addressing emerging risks. The paper concludes that effective prevention requires stronger biosecurity governance, improved screening and verification mechanisms, preparedness, and sustained coordination among governments, scientific institutions, industry, and international organizations.

Publisher: Institute for Educating Environmental Resilience and Governance

1. Introduction

For more than two decades, the spectre of bioterrorism has occupied an uneasy place in security studies: simultaneously described as one of the gravest threats facing humanity and as a hazard whose real-world incidence has remained remarkably low. Bioterrorism has reportedly killed very few American citizens since the turn of the century, yet the United States spent a dramatic amount of money on biodefense starting with the anthrax letters of 2001 which killed five and sickened seventeen (The Bioterrorism Threat by Non-State Actors, 2018). This disproportionality between the amount of money spent and the amount of harm has been at the core of a scholarly debate regarding the exaggerated nature of the non-state bioterrorism threat or the nature of low incidence in the past as a reflection of the calm before a technologically enabled storm.

This article suggests that both sides have elements of truth to them but the proportion of each side is changing. Technical, organizational and dissemination obstacles have repeatedly hindered, and continue to hinder, historical non-state efforts to acquire and employ biological weapons, as evidenced by studies of the failed anthrax and botulinum programme of Aum Shinrikyo (Rosenau, 2001). However, the recent advancements in synthetic biology, genome editing, and artificial intelligence are transforming the landscape of capabilities that historically have been a challenge for non-state actors, leading to a renewed focus on the policies, science, and intelligence community (Sandbrink, 2023; Soice et al., 2023). This article seeks to re-examine the empirical history of non-state actor involvement in biological weapons; to analyze how new biotechnology tools and processes are changing the opportunity landscape for bioterrorism; and to evaluate the effectiveness of existing international governance arrangements – in particular the Biological Weapons Convention (BWC), dual-use research oversight, and the Global Health Security Agenda (GHSA) – to deliver on the management of this emerging threat. The article continues with the theoretical mapping of the securitization framework, a literature review of the hype/horror debate in the bioterrorism literature, an empirical examination of three cases, an examination of the technological change in the threat environment, an examination of the governance adequacy of the three cases, and some policy recommendations.

2. Theoretical Framework

This study primarily draws on the Copenhagen School's theory of securitization, developed by Buzan, Wæver, and de Wilde (1998), to examine how bioterrorism has been constructed as a major security threat. Securitization theory views security as a social and political process in which an actor presents an issue as an existential threat to a valued referent object and uses this framing to justify measures beyond normal political processes (Buzan, Wæver, & de Wilde, 1998). This perspective is particularly useful for understanding why bioterrorism has received significant political and institutional attention despite the relatively limited number of successful biological attacks by non-state actors.

The securitization of health and biological risks since the late 1990s has expanded the traditional boundaries of national security. Bioterrorism has increasingly been framed as a potential mass-casualty threat because the deliberate use of biological agents could, under certain conditions, produce serious public-health, economic, and political consequences. Consequently, biological threats have been incorporated into broader national and international security agendas alongside other high-impact threats (Gostin & Phelan, 2014). While this framing has encouraged greater preparedness and investment in biosecurity, it also raises questions about whether perceptions of biological threats have sometimes exceeded the demonstrated capabilities of non-state actors.

The study therefore combines the securitization theory with a capability approach in order to overcome this problem. This is not a purely political evaluation of the threat but an assessment of the necessary circumstances for a non-state actor to conduct a biological attack. They involve purpose, access to relevant biological materials and knowledge, organizational capacity and the ability to surmount technical and institutional barriers. There have been historical precedents of hostile intent without operational capability. A number of challenges have arisen for non-state actors, including technical capacity, access, organizational capacity, and the challenges of creating intended impacts.

The combination of securitization theory and the capability-based approach therefore provides a balanced analytical framework. Securitization theory explains why bioterrorism has been elevated on the security agenda, while the capability-based approach evaluates the extent to which non-state actors have the practical capacity to translate intent into action. This distinction allows the study to avoid both exaggerated assessments of the threat and excessive dismissal of emerging risks, particularly as technological developments continue to change the biological security environment.

3. The Hype-Versus-Horror Debate in Bioterrorism Scholarship

To provide some context for the findings, bioterrorism research and writings related to the subject can be divided into approximately two opposing categories: alarmist and skeptic. The former concentrates on the fact that biological weapons can be relatively easy to acquire, particularly for those with the necessary scientific background. According to experts, such a prospect is supported by trends such as democratization of science, decreasing costs of equipment, and the availability of pathogens in nature and on the black market. According to research conducted as recently as 2017, the majority of respondents who acknowledged the possibility of bioterrorism attributed it to fast scientific progress, decreasing complexity of obtaining pathogens, and the example of the 2014 West African Ebola outbreak (Bioterrorism in the 21st Century, n.d.).

Alarmist literature and reports also highlight the potential threat posed by various pathogens becoming available due to advancements in gene-editing and genetic engineering, although the latter does not appear to be an imminent concern (Bioterrorism in the 21st Century, n.d.). Meanwhile, the skeptics cite failures of bioterrorism to take advantage of the opportunities available to them. The most frequent argument provided by skeptic literature is based on the example of the Japanese millenarian cult Aum Shinrikyo, which unsuccessfully attempted to weaponize numerous pathogens, including anthrax, botulinum, and plague, despite having significant resources at its disposal (Rosenau, 2001). According to research on the cult, the primary reason for failure was the inability to acquire the required level of virulence and aerosolize a pathogen for distribution, which failed several times (Aum Shinrikyo's Biological Weapons Program, n.d.).

A different approach to the bioterrorism threat highlights the discrepancies between what alarmist literature states about non-state actors' capabilities and real-life examples. The proponents of this view list multiple pieces of evidence demonstrating that non-state actors have showcased more capabilities than skeptics assume while lacking critical opportunities to enact bioterrorism (The Bioterrorism Threat by Non-State Actors, n.d.).

As this paper will argue, both sides' assumptions appear to stem from valid premises. It is common knowledge that to date, bioterrorism has rarely produced results, which illustrates the presence of limitations. Nevertheless, the alarmist perspective is also reasonable due to the possibility that these opportunities may disappear in the future, which would be a concern for bioterrorism research.

4. Evidence: Case Studies of Non-State Actor Biological Threats

4.1. The Rajneeshee Salmonella Attack, 1984

To provide evidence for these arguments, the first bioterrorism attack in the United States history known as the Rajneeshee salmonella attack of 1984 will be used as an example. The members of the Rajneeshee cult intentionally contaminated ten salad bars in The Dalles, Oregon, with Salmonella so that ill people would not be able to vote in the upcoming election. As a result, more than 750 people were sick, although no deaths were reported (Turner, Marinconz, & Shimp, 2025).

The attack was notable in the context of bioterrorism because it did not involve any sophisticated technology or pathogens; it only utilized a bacterial infection that could be purchased in any reputable supplier (Turner, Marinconz, & Shimp, 2025). According to the literature, this case is typical of bioterrorism in general, as a successful attack can be made with relatively simple and widely available means (Turner, Marinconz, & Shimp, 2025).

4.2. Aum Shinrikyo: The Limits of Resourced Ambition

The second example is provided by the Japanese cult Aum Shinrikyo, which is considered to be one of the most dangerous terrorist organizations of recent times. Aum Shinrikyo not only had the intentions but also the opportunity to cause a bioterrorism attack of global impact. According to the research, the cult had a budget ranging between 500 and 1000 million USD, a significant number of facilities at its disposal, and a team of experienced scientists (Aum Shinrikyo's Biological Weapons Program, n.d.). Nevertheless, researchers argue that the organization faced challenges in terms of acquiring pathogens and manufacturing a reliable biological weapon (Rosenau, 2001).

The cult's biological weapons program was reportedly shut down in 1998, while its chemical weapons program produced the nerve agent sarin that was later used in the Tokyo subway attack of 1995 (Rosenau, 2001). According to one report, the cult's biosecurity expert Salikh Bugayev stated that the task was extremely challenging because the available pathogens lacked the necessary level of virulence (Aum Shinrikyo's Biological Weapons Program, n.d.).

A more recent report by the former U.S Navy Secretary Richard Danzig, based on interviews with ex-cult members, concluded that cult members' attempts to produce biological weapons failed because of their insufficient practical experience: making such weapons requires trial and error that cannot be learned from theoretical knowledge (Revisiting Aum Shinrikyo, 2025).

4.3 The Islamic State: Territorial Sanctuary and Chemical-Biological Ambition

The third example is provided by the Islamic State (IS), whose chemical weapons program is believed to be the closest to the bioterrorism capabilities of Aum Shinrikyo. When IS seized Mosul in 2014, it employed a former chemical weapons specialist from Saddam Hussein's chemical program, Salih Sabawi. Within six months, Sabawi was able to manufacture mustard gas and chlorine bombs with the assistance of local networks (Peshmerga helped foil ISIS chemical attack in Europe, 2022). According to intelligence reports published in Western newspapers, IS was reportedly interested in developing botulinum, ricin, and anthrax and capable of launching an attack in Europe (Peshmerga helped foil ISIS chemical attack in Europe, 2022). UN investigators later found that IS was using the University of Mosul as the organization's research base to experiment with chemical and possibly biological toxins on prisoners, who often died as a result of these experiments (Mosul university deemed hub for ISIS chemical weapons programme, 2021).

IS launched the first confirmed sulfur mustard attack against Kurdish and Iraqi forces in Taza Khurmatu, killing hundreds and injuring between six hundred and one thousand people (ISIS 'manufacturing leader,' accomplice in chemical attacks, pursued by US government, 2023). However, the IS's chemical weapons program was short-lived, as the militants lost Mosul in 2017 and, consequently, the materials and equipment needed to manufacture such weapons (The Evolution of the Islamic State's Chemical Weapons Efforts, 2018).

4.4 Comparative Synthesis

When comparing the three examples, it becomes evident that none of the perpetrators were entirely successful in achieving their goals. Although the Rajneeshee cult did manage to poison hundreds of people, it did not reach the goal of causing a large-scale health crisis. Similarly, Aum Shinrikyo and IS were both stopped before they could launch devastating bioterrorism attacks. Aum Shinrikyo failed to weaponize any pathogens, while IS was unable to mass-produce toxins. It is notable that the only successful attack committed by the listed perpetrators was relatively harmless in terms of health damage: the cult used Salmonella, a bacterial infection, rather than a deadly virus like Ebola.

Furthermore, all three groups were limited by the same factor in terms of launching a bioterrorism attack, which was their incapacity to either acquire pathogens or weaponize them. While IS managed to produce chemical toxins and even had access to materials to produce biological ones, the organization failed to do so, reportedly due to a lack of qualified personnel. In contrast, Aum Shinrikyo had the necessary skills but lacked materials for bioterrorism.

This comparison provides valuable insights into how new technologies should be assessed in terms of their applicability to bioterrorism. Specifically, it is critical to consider not only whether certain advancements can be used by malicious non-state actors but also whether they address the specific opportunities gap outlined above. It is common knowledge now that such actors will inevitably seek to acquire biological weapons if given the opportunity. However, as the examples above demonstrate, bioterrorism has not been successful due to the lack of critical production capabilities. With that in mind, the alarmist literature's assumptions regarding democratization of science and gene-editing may be applied to the specific opportunities gap. If gene-editing advances allow malicious actors to bypass the current production limitations, bioterrorism may soon become much more dangerous than it is today.

5. The Transforming Landscape: Synthetic Biology, Genome Editing, and Artificial Intelligence

Advances in synthetic biology and genome-editing technologies such as CRISPR have dramatically reduced the cost and increased the accessibility of genetic engineering while simultaneously enabling unprecedented research advances in therapeutics, agri-tech, and environmental science (Biosecurity for Synthetic Biology and Emerging Biotechnologies, 2021). At the same time, these advances create the potential for both negligent and intentional abuse of these same tools, and policymakers have called for more flexible oversight frameworks to address the dual-use dilemma (Biosecurity for Synthetic Biology and Emerging Biotechnologies, 2021). However, none of these concerns compare to the revolutionary rise of artificial intelligence (AI) and especially large language models (LLMs) in synthetic biology and biological design. Sandbrink (2023) has drawn a useful distinction between LLMs that provide dual-use guidance that was previously scattered across the scientific literature and specialized biological design tools (BDTs) that directly assist in the design of novel biological agents. Esvelt and colleagues have argued that large language models could make pandemic-level agents accessible to non-experts if such agents had first been identified and described in the literature, an assertion which, if true, would have rendered the tacit knowledge barrier that stopped Aum Shinrikyo from weaponizing synthetic biology obsolete (Soice et al., 2023).

The evidence on the risk posed by AI to non-state bioweapons development is similarly mixed, which is why the capability-based approach proposed above is so useful. A 2024 RAND red-team exercise, in which teams of researchers played the role of non-state bioweapons developers, found no significant difference in the viability of the proposals generated with and without the assistance of LLMs (Mouton, Lucas, & Guest, 2024). Early 2024 safety evaluations of leading models by the firms that produced them found only marginal benefit overall over standard search tools in support of dual use research of concern (DURC). However, the situation changed drastically in just a few years: frontier model evaluations through 2025 found that models had improved by more than four times on challenging virology benchmarks on average, with one model outperforming human experts on a text-based diagnostic and troubleshooting task (Justen, 2025). Meanwhile, another 2025 red-team exercise found that modern foundation models could provide specific guidance on recovering a live polio virus from synthetic DNA, which has obvious implications for other pathogens (Contemporary Foundation AI Models Increase Biological Weapons Risk, 2025). Finally, leading AI developers have updated their risk assessments, with public statements from multiple firms in 2026 acknowledging that current models pose significantly higher risk to unsophisticated would-be bioweapon developers at specific stages of the acquisition pathway while providing only comparatively limited benefits to experts (AI as a Biosecurity Risk Amplifier, 2026). The tacit knowledge barrier, which had been believed to be an impenetrable hurdle to developing bioweapons by non-state actors, has proved to be ineffective against determined and well-motivated actors, as this evidence indicates, though it is far from dead and continues to be a point of contention and debate.

6. Governance Adequacy: Gaps in the International Biosecurity Architecture

6.1 The Biological Weapons Convention

The 1972 Biological and Toxin Weapons Convention (BTWC) is the central pillar of the international law framework banning biological weapons, although it is generally recognized as the weakest of the weapons-of-mass-destruction treaties. Unlike the Chemical Weapons Convention, the BTWC lacks any verification measures, inspection regime, or formal implementing agency, only vague confidence-building measures that many signatories do not even follow (The Biological Weapons Convention and International Governance, 2026). Attempts to adopt a legally binding protocol that would have established a verification regime failed in 2001 when the U.S., citing the inability to devise inspection procedures that would not violate commercial and national security confidentiality, withdrew its support, and the issue has been deliberately taboo ever since (Strengthening the BWC, 1998; The Biological Weapons Convention Protocol Should Be Revisited, 2019). Meanwhile, recent review conferences have begun to focus more on the issues of verification and compliance, spurred by the 2001 anthrax attacks and the Syrian chemical weapons crisis (Strengthening the Biological Weapons Convention, 2024).

6.2 Dual-Use Research Governance and DNA Synthesis Screening

Governance of dual-use research of concern (DURC) is equally fragmented and inconsistent, both internationally and domestically. Millett (2017) has highlighted the inadequacy of the international regime, which has been exacerbated, rather than mitigated, by the rise of synthetic biology. He notes that the U.S. policy on gain-of-function and DURC has been particularly inconsistent, adopting a self-certification nucleic acid screening requirement for federally funded research in 2024, only for the 2025 executive order to effectively ban gain-of-function research and defund the 2024 directive, leaving the field in regulatory limbo just as the AI-fueled revolution in gene-editing technologies began (Biosecurity and Oversight Gaps in Dual-Use Biotechnology, 2026). In turn, no country has legislation that would require gene synthesis companies to screen customer requests and identify dangerous sequences, which is why this critical weakness in the international biosecurity architecture remains as an optional measure for industry self-regulation (Biosecurity and Oversight Gaps in Dual-Use Biotechnology, 2026). At the same time, national policies are also inconsistent: China's updated Biosecurity Law from 2020 now requires centralized oversight of all research involving pathogens, the EU's updated Dual-Use Regulation from 2024 effectively banned gene synthesis platforms using AI-driven design software, and other major regions have yet to adopt any significant legislation regarding AI-driven biosecurity challenges (Blurred Lines, 2025).

6.3 The Global Health Security Agenda and International Health Regulations

The Global Health Security Agenda (GHSA) and the World Health Organization's (WHO) International Health Regulations (IHR, 2005) represent another track of international health security governance that differs from the arms control paradigm of the BTWC, focusing instead on building national surveillance, laboratory, and biosafety capacities (Biosecurity & Biosafety, 2025). This approach is both necessary and effective, as it addresses the critical areas that the BTWC and its inadequacies in verification and oversight leave uncovered. However, international assessments of the IHR implementation in low- and middle-income countries (LMICs) have shown that just around 20% of WHO member states met the surveillance and response capacity requirements as of the early 2010s (Gostin & Phelan, 2014), and LMIC assessments continue to highlight serious resource, technical, and capacity limitations in implementing IHR (National Biosafety Management System, n.d.). Finally, since non-state bioweapons developers do not recognize jurisdiction, the inconsistencies in any single state's implementation of biological safety and security measures undermine the effectiveness of this entire system.

6.4. Regime Fragmentation as a Structural Vulnerability

BTWC, the international health security governance mechanisms, and national-level DURC oversight frameworks represent a deeply fragmented system that fails to account for the unique challenges posed by AI-fueled biotechnology advances while also being at odds with itself at the level of implementation and policy priorities. Even within the narrow realm of biosecurity, health inspectors, intelligence agencies, and defense departments all operate in isolation from one another, with limited coordination or information-sharing (Artificial Intelligence and Synthetic Biology, 2025). This is a serious vulnerability for the international system, as a determined and well-resourced non-state actor does not need to overcome the challenges imposed by all jurisdictions: The Islamic State was able to develop chemical and biological weapons in part due to the lack of restrictions in the territory under its control, and a similar opportunity exists for non-state bioweapons developers to take advantage of jurisdictional gaps.

7. Policy Recommendations

Based on the findings presented above, this paper offers five policy recommendations for further consideration by the international community in its efforts to respond to the non-state bioweapons security challenge.

First, BTWC parties should consider adopting incremental, confidence-building measures that would improve upon the current verification mechanisms while avoiding the pitfalls of the failed 2001 protocol, such as a standing scientific advisory group on dual-use research, mandatory rather than voluntary reporting measures, and a better-resourced implementation support unit, as has been proposed at recent review conferences (Strengthening the Biological Weapons Convention, 2024).

Second, the international research and commercial communities should adopt a binding, harmonized standard for DNA and RNA synthesis screening, which would close the current capability gap while also providing appropriate funding incentives for the industry (Biosecurity and Oversight Gaps in Dual-Use Biotechnology, 2026).

Further, AI governance and biosecurity governance should be brought into closer alignment, possibly through a tiered risk management framework that would impose specific restrictions based on the capabilities of a given AI model. A common, standardized evaluation framework for frontier AI models with a particular focus on biosecurity applications may help inform such restrictions, inspired in part by the growing body of research on the capabilities of different models (Justen, 2025; Mouton, Lucas, & Guest, 2024).

Fourth, persistent and predictable funding for GHSA capacity-building efforts in low- and middle-income countries should be prioritized to reduce the discrepancy between these countries and high-income counterparts in terms of surveillance and biosafety infrastructure, which represents a critical vulnerability in the current system (Gostin & Phelan, 2014).

Finally, security and intelligence agencies should build stronger relationships with public health and biosafety counterparts at the national level, as the evidence presented in this paper demonstrates that interdiction of key personnel and disruption of supply chains can be far more effective in curtailing illicit biotechnology research than any arms control measures, including inspections and treaties.

8. Conclusion

This article argues that the threat of non-state bioterrorism should not be viewed as fixed, but as a changing relationship between malicious intent and practical capability. The relatively low number of successful biological attacks in the past reflects not simply a lack of intent, but significant barriers related to access, technical knowledge, organizational capacity, and the ability to achieve the intended effects. The Rajneeshee cult, Aum Shinrikyo, and Islamic State examples show various examples of this connection: some success with readily available biological materials, some unsuccessful with a lot of resources, and some short-term gains due to territorial control. But the boundaries of knowledge and information are being eroded over time by the development of synthetic biology, genome editing and artificial intelligence, which will help limit the restrictions some non-state actors face. Meanwhile, global systems for controlling these risks are still weak and inconsistent, such as the Biological Weapons Convention, dual-use research control, DNA-synthesis screening, and the Global Health Security Agenda. Therefore, the analysis suggests a balanced approach toward biosecurity – that is, not underestimate the risk that may emerge in the future and not overestimate the capacity of non-state actors in the current context. Rather, more efforts must be made in enhancing the governance, screening, verification, preparedness, and cooperation between governments, scientific institutions, industry and international organisations on relevant issues. This can help meet evolving biological threats without stifling legitimate scientific research and international collaboration.

Conflict of Interest

The authors showed no conflict of interest.

Funding

The authors did not mention any funding for this research.

References

AI as a biosecurity risk amplifier. (2026). *The Biosecurity Handbook*. https://biosecurityhandbook.com/ai-biosecurity/ai-risk-amplifier.html

Artificial intelligence and synthetic biology: Biosecurity risks, dual-use concerns, and governance pathways. (2025). AI and Ethics. *Springer Nature Link*. https://link.springer.com/article/10.1007/s43681-025-00872-9

Aum Shinrikyo's biological weapons program: Why did it fail? (n.d.). *Office of Justice Programs*. https://www.ojp.gov/ncjrs/virtual-library/abstracts/aum-shinrikyos-biological-weapons-program-why-did-it-fail

Bioterrorism in the 21st century. (n.d.). *NYU Global Affairs Review*. https://gareviewnyu.com/2018/04/11/bioterrorism-in-the-21st-century/

Biosecurity and oversight gaps in dual-use biotechnology: A crisis of governance in the age of synthetic biology, Part V. (2026). *Foreign Affairs Forum*. https://www.faf.ae/home/2026/5/6/biosecurity-and-oversight-gaps-in-dual-use-biotechnology-a-crisis-of-governance-in-the-age-of-synthetic-biology-part-v

Biosecurity for synthetic biology and emerging biotechnologies: Critical challenges for governance. (2021). In Emerging threats of synthetic biology and biotechnology. *National Academies Press (NCBI Bookshelf)*. https://www.ncbi.nlm.nih.gov/books/NBK584259/

Biosecurity & biosafety. (2025). *Global Health Security Agenda*. https://globalhealthsecurityagenda.org/biosecurity-biosafety/

Blurred lines: Law, science, and the regulation of dual-use biological research. (2025). *International Bar Association*. https://www.ibanet.org/dual-use-biological-research-law

Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. *Lynne Rienner*.

Contemporary foundation AI models increase biological weapons risk. (2025). *RAND Corporation*. https://www.rand.org/pubs/perspectives/PEA3853-1.html

Gostin, L. O., & Phelan, A. (2014). The Global Health Security Agenda in an age of biosecurity. *Georgetown Law Faculty Publications*. https://scholarship.law.georgetown.edu/facpub/1356/

ISIS 'manufacturing leader,' accomplice in chemical attacks, pursued by US government. (2023). https://alfasselnews.com/en_GB/articles/gc1/features/2023/12/19/feature-01

Justen, L. J. (2025). LLMs outperform experts on challenging biology benchmarks. arXiv. https://arxiv.org/pdf/2505.06108

Millett, P. D. (2017). Gaps in the international governance of dual-use research of concern. *National Academies Press*. https://nap.nationalacademies.org/resource/24761/Millett_Paper_011717.pdf

Mosul university deemed hub for ISIS chemical weapons programme. (2021). *Diyaruna*. https://diyaruna.com/en_GB/articles/cnmi_di/features/2021/05/19/feature-01

Mouton, C. A., Lucas, C., & Guest, E. (2024). The operational risks of AI in large-scale biological attacks: Results of a red-team study. *RAND Corporation*. https://www.rand.org/pubs/research_reports/RRA2977-2.html

National biosafety management system: A combined framework approach based on 15 key elements. (n.d.). PMC. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8342751/

Peshmerga helped thwart ISIS chemical attacks in Europe. (2022). *Kurdistan24*. https://www.kurdistan24.net/en/story/388933

Revisiting Aum Shinrikyo: New insights into the most extensive non-state biological weapons program to date. (2025). *Nuclear Threat Initiative*. https://www.nti.org/analysis/articles/revisiting-aum-shinrikyo-new-insights-most-extensive-non-state-biological-weapons-program-date-1/

Rosenau, W. (2001). Aum Shinrikyo's biological weapons program: *Why did it fail? Studies in Conflict and Terrorism*, *24*(2), 289–301. RAND Corporation. https://www.rand.org/pubs/external_publications/EP20010716.html

Sandbrink, J. B. (2023). Artificial intelligence and biological misuse: Differentiating risks of language models and biological design tools. *arXiv*. https://arxiv.org/pdf/2306.13952

Soice, E. H., Rocha, R., Cordova, K., Specter, M., & Esvelt, K. M. (2023). Can large language models democratize access to dual-use biotechnology? *arXiv*. https://arxiv.org/pdf/2306.03809

Strengthening the BWC: Moving toward a compliance protocol. (1998). *Arms Control Association*. https://www.armscontrol.org/act/1998-01/arms-control-today/strengthening-bwc-moving-toward-compliance-protocol

Strengthening the Biological Weapons Convention. (2024). *Arms Control Association*. https://www.armscontrol.org/act/2024-12/features/strengthening-biological-weapons-convention

The Biological Weapons Convention and international governance. (2026). *The Biosecurity Handbook*. https://biosecurityhandbook.com/frameworks/bwc-governance.html

The Biological Weapons Convention protocol should be revisited. (2019). *Bulletin of the Atomic Scientists*. https://thebulletin.org/2019/11/the-biological-weapons-convention-protocol-should-be-revisited/

The Bioterrorism Threat by Non-State Actors: Hype or horror? (n.d.). *Research Gate*. https://www.researchgate.net/publication/235133996_The_Bioterrorism_Threat_by_Non-State_Actors_Hype_or_Horror

The Evolution of the Islamic State's chemical weapons efforts. (2018). *Combating Terrorism Center at West Point*. https://ctc.westpoint.edu/the-evolution-of-the-islamic-states-chemical-weapons-efforts/

Turner, M. D., Marinconz, K., & Shimp, G. (2025). The 1984 Rajneeshee bioterrorism attack: An example of biological warfare by violent non-state actors. *Cureus*, *17*(7), e88514. https://doi.org/10.7759/cureus.88514