



NOVEMBER 2025

Redefining Biological Weapons: Expanding the BWC to Incorporate Infrastructure Harm and Cyber-Biothreats

Shreyash Borkar

University of Tübingen
Germany

HOME COUNTRY

India

Sriram Kumar

University of Münster
Germany

HOME COUNTRY

India

Kaitlyn Connors

Georgetown University
United States

HOME COUNTRY

United States

Acknowledgments

We are grateful to Tessa Alexanian, technical lead for the Common Mechanism at the International Biosecurity and Biosafety Initiative for Science (IBBIS); Matt Sharkey, PhD, senior biosecurity resident at the RAND Corporation; and Gigi Kwik Gronvall, PhD, senior scholar and professor at the Johns Hopkins Center for Health Security, Bloomberg School of Public Health, for generously sharing their expertise and perspectives throughout the development of this work. We also acknowledge Yorgo El Moubayed and Alonso Flores for their valuable input and thoughtful contributions.

This paper was produced for the 2025 Next Generation for Biosecurity Competition.

Visit nti.org/nextgenbio for more information.

The 2025 Next Generation for Biosecurity Competition was sponsored by the Nuclear Threat Initiative, in partnership with 80,000 Hours, CBWNet, the iGEM Foundation, the InterAcademy Partnership (IAP), the International Biosecurity and Biosafety Initiative for Science (IBBIS), the United Nations Office of Disarmament Affairs (UNODA), and Women of Color Advancing Peace, Security, and Conflict Transformation.



© 2025 Nuclear Threat Initiative



This work is licensed under a Creative Commons AttributionNonCommercial-NoDerivatives 4.0 International License.

The views expressed in this publication are those of the authors alone, and do not necessarily reflect those of the sponsoring organizations, members of their Board of Directors or institutions with which they are associated, or any external experts involved with judging the competition.

Executive Summary

The definition of biological weapons in the 1972 Biological Weapons Convention (BWC) is being outpaced by emerging technologies, creating an “accountability vacuum” for evolving threats.¹ Innovations in synthetic biology and biotechnology powered by artificial intelligence (AI) and large language models (LLMs) may enable the creation of highly targeted or controllable agents attractive to malicious actors. While the BWC’s strength lies in its broad, forward-thinking definition and general purpose criterion (GPC), its implicit focus on human, animal, and plant diseases is a potential vulnerability. This paper proposes that the current pathogen-centric definition of bioweapons should be expanded to address two overlooked threats: metabolic sabotage, in which engineered microbes degrade material infrastructure, and cyber-biothreats, in which digital attacks corrupt biological workflows, such as hacking DNA synthesizers or bioreactors to produce altered sequences and harmful agents. These novel threats weaken the BWC and United Nations (UN) Security Council Resolution 1540 by creating an oversight gray area.²

To address metabolic sabotage, the definition of a *biological agent* should encompass harm to inanimate materials essential for sustaining life and the economy. To counter cyber-biothreats, the definition of a *biological and toxin weapon* should include digital systems and codes designed to produce or activate such agents for hostile purposes. These clarifications necessitate that states-parties agree not to develop, produce, stockpile, acquire, or retain microbial/biological agents/toxins that harm living and/or inanimate entities, unless justified for prophylactic, protective, or other peaceful purposes. To support this paradigm shift, a proactive oversight framework is essential. Key recommendations include adopting a “functional harm” principle, mandating “Biosecurity-by-Design,” establishing threat forecasting panels, fortifying cyber-bio infrastructure, integrating biosurveillance into infrastructure maintenance, and regulating access to high-risk microbes. These approaches help build a resilient biosecurity posture that effectively addresses 21st-century threats, safeguarding public health, infrastructure, and national security.

Background: An Evolving Definition for Evolving Threats

The definition of a biological weapon has always been a moving target, shaped by scientific progress and historical events, as illustrated in Figure 1. Early uses of biological warfare, like catapulting plague cadavers in 1346, were based on rudimentary observations of contagion.³ The Scientific Revolution, including the rise of germ theory, finally gave negotiators of the 1925 Geneva Protocol the language to prohibit “bacteriological methods of warfare.”⁴ However, its scope was critically limited; it did not prohibit development or stockpiling, which allowed many nations to retain offensive programs. This deterrence rationale fostered a “no-first-use” policy that failed to prevent a biological arms race. This crucial loophole was a factor that led to the landmark 1972 BWC and its GPC, an intentionally broad definition focused on hostile intent, designed to be future-proof against the dual-use nature of biology, already evident in early recombinant DNA research.⁵

For decades, the primary deterrent to the use of bioweapons, beyond morality and treaties, was their inherent uncontrollability; a released pathogen could simply rebound on its user. Today, that calculus has changed. The emergence of biological AI tools, parallel with rapid innovations in synthetic biology, enables more precise biological engineering, which in turn allows for novel pathogen development

with increased lethality and rapid transmission.⁶ This potential for control, including engineering organisms to interact with specific genotypes, activate only under certain conditions, or use time-limited lifespans, makes biological weapons a more usable and therefore a more attractive option for malicious actors.⁷ This technological leap complicates the BWC’s allowance for “prophylactic” research, as the tools needed to defend against a theoretical AI-designed pathogen are the very same tools that could create it, creating a perilous feedback loop.⁸

While the global community grapples with these advancements, the very concept of a biological target is also expanding. The destruction or degradation of infrastructure has always been a cornerstone of warfare; destroying bridges, poisoning wells, and blocking supply lines are classic tactics.⁹ The world now faces a future in which these age-old strategies can be executed with novel biological tools. The authors propose that the definition of a bioweapon and a biological agent must encompass less recognized yet dangerously plausible forms of biological harm: the metabolic sabotage of critical infrastructure materials and the corruption of cyber-biological systems. These are threats not just to living beings but to the inanimate skeleton of modern civilization.

Figure 1: Evolving Definition of Biological Weapons: Influencing Factors and Actors Involved

EARLY DISEASE TRANSMISSION	1346	Plague-infected cadavers catapulted over walls to enemies	MONGOL FORCES ^a
Pathogens are recognized as warfare agents	1900	GERM THEORY	GLOBAL SCIENTISTS ^b
GENEVA PROTOCOL	1925	Prohibited use of “bacteriological methods” of warfare	SCIENTISTS & POLICYMAKERS ^c
United States terminated offensive BW development as WMD concerns grew	1969	UNITED STATES BANS BW DEVELOPMENT	UNITED STATES ^d
BWC OPENS FOR SIGNATURE	1972	States parties agreed to nondevelopment, acquisition, and possession of BW and agents	38 STATES ^e
Treaty is ratified and entered into force	1975	BWC RATIFIED	22 STATES ^f
BWC REVIEW CONFERENCE	1991	Ad Hoc Group for verification is established to address gene editing concerns	115 STATES ^g
GPC expanded to “any applications ... from genome studies” and genetic engineering	1996	BWC REVIEW CONFERENCE	140 STATES ^h
BIOTERRORISM ATTACKS	2001	U.S. anthrax attacks and Aum Shinrikyo attempts of the late 1990s	UNITED STATES & JAPAN ^a
De novo synthesis of poliovirus, BWC RevCon; calls for annual S&T review	2002	SYNTHETIC BIO CONCERNS	144 STATES ^{i, j}
SYNTHETIC BIO ADVANCEMENTS	2020s	“Dual-use research of concern”; codes of conduct	GLOBAL SCIENCE COMMUNITY ^{l, m}
Precise, simple, and low-cost gene editing in human cells	2012	CRISPR CONCERN	GLOBAL SCIENCE COMMUNITY ⁿ
CRISPR AS A BIOWEAPON	2016	U.S. intelligence community categorized gene editing as a potential WMD	GLOBAL SCIENCE COMMUNITY ^o
AI and biotechnology integration was posed to accelerate BW design and creation	2016	ARTIFICIAL INTELLIGENCE	U.S. INTELLIGENCE COMMUNITY ^{p, q}
CHINA'S BIOWEAPON LAW	2021	The law prohibited development, manufacture, acquisition, storage, possession, and use of BW	CHINA ^r
The pandemic, political, and economic tensions lead to interest in systematic S&T review	2022	9TH BWC REVIEW CONFERENCE	189 STATES ^s
REDEFINING BIOWEAPONS IN PRESENT DAY	2025	Creation of pathogens that pose a critical infrastructure risk	FUTURE BWC ARCHITECTS
		DNA data storage capabilities pose novel cyber-biosecurity risk	FUTURE BWC ARCHITECTS

Notes: RevCon = Review Conference; S&T = science and technology; WMD = weapon of mass destruction

Discussion: New Paradigms of Harm and the Oversight Accountability Vacuum

The traditional pathogen-centric security paradigm creates an “oversight accountability vacuum,” in which essential structures of the society are vulnerable to novel biological attack. The loopholes are not theoretical; they exist today, born from a failure to imagine biology as a weapon against the inanimate.

Metabolic Sabotage

One gap is the threat of metabolic sabotage to critical infrastructure.¹⁰ Research throughout the 20th century has confirmed that microbiologically influenced corrosion (MIC), in which bacterial communities, or “biofilms,” create corrosive microenvironments, causes billions of dollars in damage annually.¹¹ The steel pipes of oil pipelines, water mains, and naval vessels can be degraded within one to nine months.¹² Similarly, “concrete-eating” bacteria are a documented problem in sewers and tunnels, metabolizing compounds into sulfuric acid that pulverizes concrete structures.¹³ These naturally occurring organisms act like *infrastructural pathogens*, silently threatening national security assets without ever causing disease. Crucially, because they do not directly affect humans or agriculture, these microbes fall outside traditional biosecurity oversight, including select agent lists, allowing their study and use to proceed largely without regulation.

Yet the danger does not end with nature’s offerings. With the rise of synthetic biology, it is increasingly feasible to engineer known corrosive microbes to act faster, last longer, or evade detection.¹⁴ These pathogens could effectively compress months-long degradation timelines into mere weeks.¹⁵ Even more concerning is the potential to design entirely novel organisms with material-degrading capabilities, tailored to attack specific infrastructure, from bridges and tunnels to electronics. A cautionary example of this dual-use potential comes from the 2018 International Genetically Engineered Machine (iGEM) competition team at Bielefeld-CeBiTec.¹⁶ The team’s project aimed to engineer *Escherichia coli* to recover copper from electronic waste. The team acknowledged that such microbes could also be misused to degrade functioning electronic systems. iGEM’s robust biosafety framework and strong emphasis on dual-use awareness prompted early identification of theoretical risks and embedded safeguards at every step.¹⁷ This example highlights that fostering a community grounded in biosafety, dual-use literacy, and responsible innovation can create some of the most effective defenses against inadvertent misuse or accidents. A challenge in responding to engineered pathogens for material degradation will be assessing the potential for dual-use research of concern (DURC) and transparency among developers of the target material. Both natural and engineered biological agents pose a growing, overlooked threat to critical infrastructure.

This accountability vacuum signifies that states risk facing a strategic surprise—a crippling attack on infrastructure or the bioeconomy that causes WMD-level disruption, but for which no international framework has a clear attribution plan or accountability entity.

While naturally occurring microbes already offer templates for material degradation, synthetic biology allows for amplification or redesign of these capabilities for malicious ends.

Cyber-Biothreats

The stealthiest emerging risk lies in cyber-biothreats, which pose weaponization risks through two distinct pathways. The first is *weaponization by corruption*, in which a cyberattack serves as the direct cause for the creation of a harmful biological agent. Here, the cyber vector is a novel “method of production.” For example, a malicious actor could hack a DNA synthesis company and alter a digital sequence for a benign protein, causing the synthesizer to print the DNA for a harmful toxin.¹⁸ Similarly, an attack that disrupts the pasteurization process in a dairy plant could weaponize otherwise harmless microbes, turning milk into a vector for foodborne illness.¹⁹ In these cases, the end product is a biological weapon; the novelty lies in its digital origin, which is not covered by the current oversight framework focused on natural and anthropogenic origins, whether accidental or deliberate.

The second pathway is *weaponization by denial*, a more subtle but equally devastating strategy. This involves using a cyberattack to remove a critical biological commodity from the population, causing harm through its absence. The U.S. National

Security Commission on Emerging Biotechnology identified biomanufacturing and its supply chains as a critical national security concern.²⁰ The 2017 NotPetya ransomware attack on Merck, which halted production of critical vaccines for months and caused over \$1.3 billion in damages, is a prime example.²¹ While no malicious agent was created, the denial of life-saving biological products indirectly led to preventable suffering and death. Here, the “weapon” is the disruption of the bioeconomy itself, a strategic attack that causes mass harm by allowing a pathogen to spread unabated.

These shifting concerns render existing international oversight mechanisms inadequate. How can the BWC gauge the intentions of a bioremediation lab secretly weaponizing a plastic-eating fungus? Would an attack using a material-degrading agent even be considered a “weapon” in the traditional sense, or would it be dismissed as sophisticated sabotage and fall outside the BWC’s scope? How can UN Security Council Resolution 1540, which prevents nonstate actors from acquiring weapons of mass destruction (WMDs), be enforced against an unattributable threat that originates as malicious code sent from halfway around the world? This accountability vacuum signifies that states risk facing a strategic surprise—a crippling attack on infrastructure or the bioeconomy that causes WMD-level disruption, but for which no international framework has a clear attribution plan or accountability entity.

Recommendations: Building a Resilient, Forward-Looking Biosecurity Framework

To address the multifaceted biological threats of the 21st century, a static, reactive posture is insufficient. States-parties must build an adaptive, proactive, and interdisciplinary biosecurity framework. Present concerns require moving beyond traditional arms control to a more holistic concept of biological risk regulation and management, involving multiple stakeholders with diverse technical expertise. Essential considerations are illustrated in Figure 2.

1. Formally Expanding the Definitions of *Biological Agent* and *Biological and Toxin Weapons*

The BWC's power lies in the GPC, but its implicit focus on human, animal, and plant disease is a vulnerability. The authors propose that states-parties, through a review conference or a special meeting of the working groups, formally affirm an expanded understanding of a biological agent, inspired by forward-looking and multistakeholder-driven national policies, such as the U.S. DURC framework.²² The definition of biological agent in the context of the BWC should be clarified to read:

Biological agent: Any microbial or other biological agent, naturally occurring or artificially created or altered, as well as its components,

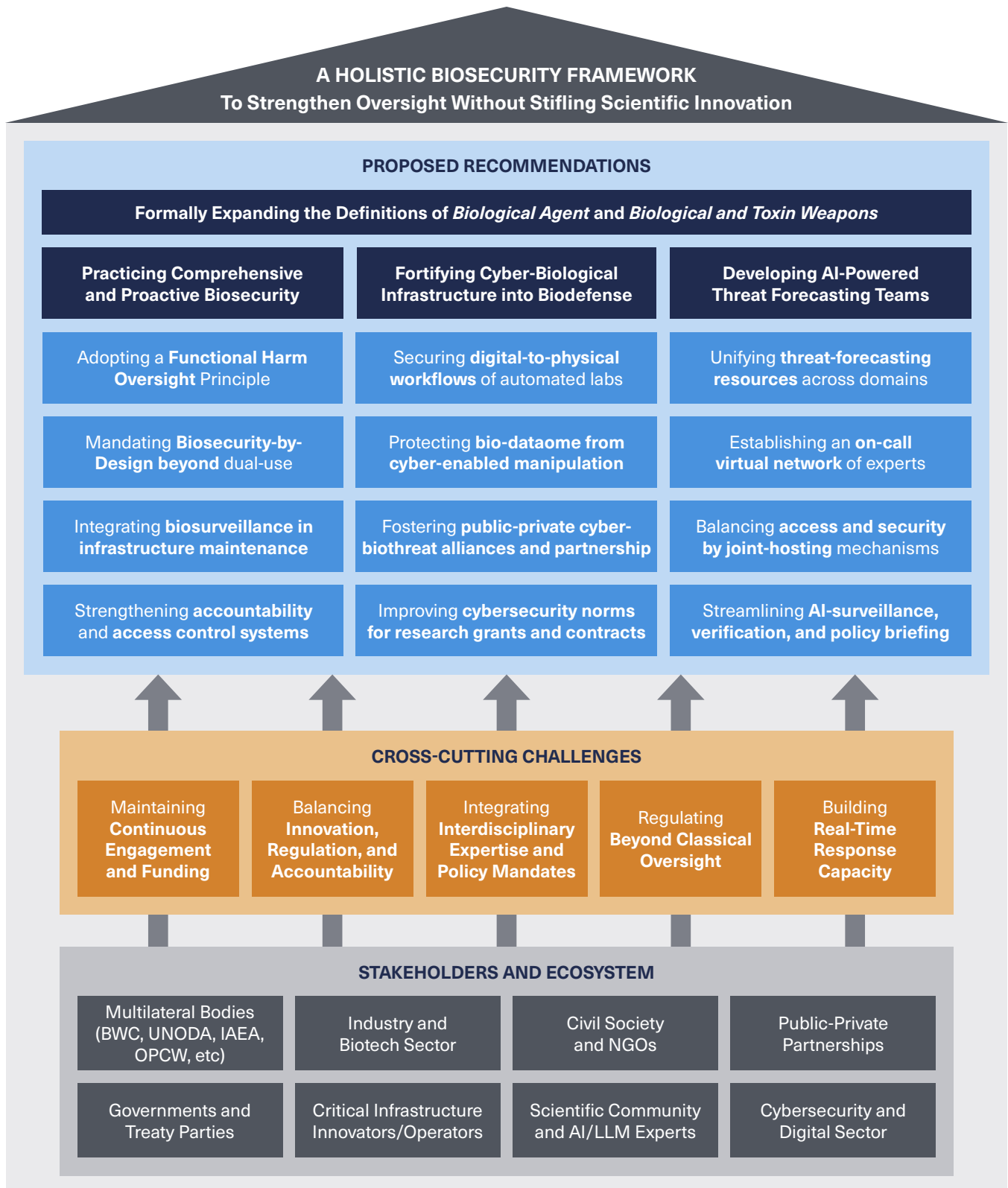
whatever its origin or method of production, that may cause harm to humans, animals, plants, ***or inanimate entities, including physical materials and information infrastructure, essential for maintaining the “living” society and economy.***

This simple addition would explicitly bring material-degrading agents under the BWC's purview, closing a major loophole. To address cyber-biothreats, the definition of biological and toxin weapons should be expanded to read:

Biological and toxin weapons: (1) Microbial or other biological agents, or toxins whatever their origin or method of production, of types and in quantities that have no justification for prophylactic, protective, or other peaceful purposes; (2) weapons, equipment, ***digital systems, computer code, or other*** means of delivery designed to ***activate or enable the production or use of*** such agents or toxins, ***or to disrupt the production or application of a critical biological commodity,*** for hostile purposes or in armed conflict.

This specification recognizes the potential of cyberattacks to weaponize otherwise benign biological facilities and ensures the digital pathways capable of triggering physical biological effects are covered under the BWC.

Figure 2: Stakeholder Mapping with Proposed Recommendations and Cross-Cutting Challenges



Note: IAEA = International Atomic Energy Agency; NGOs = nongovernmental organizations; OPCW = Organisation for the Prohibition of Chemical Weapons; UNODA = United Nations Office for Disarmament Affairs

2. Practicing Comprehensive and Proactive Biosecurity

To effectively address emerging biosecurity threats, it is essential to move beyond the current pathogen-centric frameworks to adopt a broader *functional harm principle*. This approach assesses risks based on a technology or agent's potential to cause strategic disruption—not merely its pathogenicity. By doing so, oversight can encompass a wider range of potential threats, including non-pathogenic agents capable of destabilizing vital sectors such as energy, healthcare, communication, food supply, and defense logistics. Coupling this effort with a *Biosecurity-by-Design mandate*, a model that ensures high-risk research is paired with the development of appropriate countermeasures, would embed safety and innovator responsibility directly into the foundation of scientific progress.

2.1. Adopting a Functional Harm Oversight

Principle: Traditional biosecurity measures often focus on restricting research on known, high-risk pathogens. However, many agents with the ability to disrupt strategic infrastructure—such as material-degrading microbes or cyber-bio vectors—fall outside these classic definitions. The *Functional Harm Principle* redefines oversight criteria, requiring that any technology or agent with disruptive potential, regardless of its mechanism (infection, corrosion, or otherwise), be subject to biosecurity scrutiny. This option closes regulatory gaps and ensures all forms of biologically enabled strategic disruption are adequately managed.

2.2. Mandating Biosecurity-by-Design Beyond Dual-Use Research:

High-risk studies beyond classical DURC must proceed only with concurrent protocol development to mitigate potential misuse. Biosecurity-by-Design ties research funding and publication to the parallel development of countermeasures—such as neutralizing agents or targeted reversal technologies.²³ This creates a system in which innovator responsibility, proactive safety measures, and ethical research conduct are integral to scientific advancement.

2.3. Integrating Biosurveillance in Critical

Infrastructure Maintenance: Routine biosurveillance—using biological sampling

and advanced metagenomic analysis—should become a core component of critical infrastructure maintenance. By establishing microbial baselines in systems like water networks, tunnels, and energy grids, stakeholders can rapidly detect anomalies indicative of engineered threats. Early intervention becomes possible, reducing the risk of widespread disruption.

2.4. Strengthening Access Controls and Accountability Mechanisms:

To prevent the misuse of high-risk environmental microbes, robust access controls are essential. Adopting know-your-customer frameworks for commercial suppliers of such agents aids in monitoring their distribution and uses. These audits ensure legitimate research use while deterring and detecting malicious acquisition or deployment of bio-disruptive substances. These efforts thereby foster both innovation and security within the bioeconomy.

3. Fortifying Cyber-Biological Infrastructure into Biodefense Frameworks

The convergence of biology and cyberspace requires a dedicated, multilayered defense. This strategy must be a national priority, integrated into existing biodefense and cybersecurity frameworks.²⁴ The following recommendations are based on a September 2023 article published by the Council on Strategic Risks.²⁵

3.1. Securing the Digital-to-Physical Workflow:

This is the most critical attack vector. Action must be taken to harden the entire process from digital design to physical product. Such action includes:

- ◆ **For DNA Synthesis:** Mandating that all commercial synthesis providers adopt robust customer verification protocols and use state-of-the-art screening software to vet all ordered sequences against databases of concern. This software and its databases must also be secured against tampering.²⁶
- ◆ **For Automated Laboratories:** Classifying laboratory automation systems and bioreactors as critical operational technology (OT), which requires implementing OT-

specific security measures like network segmentation, anomaly detection, and access control to prevent corruption of experimental protocols or production recipes.

3.2. Protecting the “Bio-Dataome”: Biological data is a strategic national asset. A new data protection framework, analogous to HIPAA (the Health Insurance Portability and Accountability Act) and tailored for the bioeconomy, is needed.²⁷ This framework must ensure the confidentiality, integrity, and availability of genomic data, proprietary research, and other sensitive biological information stored in government, academic, and commercial databases against cyber-enabled theft and manipulation.²⁸

3.3. Fostering Public-Private Cyber-Biothreat Alliances: The authors recommend a partnership between governments and organizations like the Cyber-Biosecurity Information Sharing and Analysis Center to facilitate trusted, bidirectional sharing of threat intelligence and vulnerability data. This collaboration between government agencies and private biotechnology companies will enable a coordinated, real-time response to emerging threats.²⁹

3.4. Incentivizing Security Through Federal Leverage: Governments should use their purchasing power to drive market-wide security improvements. Federal contracts and research grants for life sciences should require recipients to meet stringent cyber-biosecurity standards. This would effectively make “secure-by-design” a prerequisite for national research and development participation; this requirement would be limited not just to bench science but to digital engagements.

4. Developing a Joint AI-Powered Threat Forecasting Platform

The authors propose a shared, AI-driven platform for continuous threat surveillance across the biological, chemical, and nuclear domains, operating under a Human-in-the-Loop (HITL) model. This collaborative approach pools resources to avoid redundant efforts across the BWC, the Organisation for the Prohibition of Chemical Weapons (OPCW), the International

Atomic Energy Agency, and the World Health Organization that share common technological needs, especially given the BWC’s challenge in expanding its Implementation Support Unit.³⁰

4.1. Operating Model: The workflow is a simple, three-stage process:

1. **AI Surveillance:** The platform scans open-source data to generate initial threat analysis reports.
2. **Expert Verification (HITL):** An on-call expert network, coordinated by the respective secretariat, validates and contextualizes AI’s findings over a virtual meeting.
3. **Policy Briefing:** Verified intelligence briefs on emerging technologies are presented at formal meetings (e.g., BWC meetings) to inform and guide discussions. If a possible biological attack is identified and validated by the experts, the UN Secretary-General’s Mechanism mandate is enforced.

4.2. Expert Network: To ensure the success of the HITL model, the authors recommend establishing a dynamic, on-call expert network rather than a static committee. This virtual network of vetted specialists, managed by relevant secretariats, would convene into ad hoc working groups via secure online platforms to analyze AI-generated alerts. Drawing on successful models like the OPCW’s Scientific Advisory Board, this panel would possess deliberately interdisciplinary expertise, including core sciences, convergent technologies, security and policy, and contextual fields, to effectively assess complex threats.

4.3. Hosting and Funding: The platform should be hosted by a neutral body like the United Nations Office for Disarmament Affairs to balance member state access with security. Development should be funded jointly by participating organizations via a pro rata contribution of their annual budgets.

4.4. Technical Precedents: Technical inspiration can be drawn from proven AI monitoring systems in public health (e.g., HealthMap, ProMED), open-source intelligence (e.g., Dataminr), cybersecurity (e.g., the User and Entity Behavior Analytics platforms), and graph-based data analytics.³¹

Conclusions

The 21st-century biological threat landscape is dynamic, interconnected, and increasingly complex, making reactive policies untenable. Therefore, a transition to proactive, holistic, adaptive, and interdisciplinary frameworks for biosecurity and emerging risks is imperative. The outlined recommendations, spanning expanded definitions, cyber-biological fortification, oversight innovation, and the cultivation of a responsible culture, offer a comprehensive strategy to close existing loopholes and meet both current and future challenges head-on.

By altering the definition of biological agents under the BWC to include material-degrading entities and broadening the definition of biological weapons to cover cyber-bio vectors, the authors anchor oversight in a “functional harm” principle to address biothreats, regardless of their pathogenic nature. Fortifying the cyber-biological infrastructure by securing the digital-to-physical workflow, protecting the national “bio-dataome,” and leveraging public-private alliances will diminish vulnerabilities at this critical interface. Equally vital is a strict Biosecurity-by-Design mandate that requires high-risk research to include parallel countermeasure development to ensure innovation does not outstrip safety. The creation of a joint, AI-powered threat forecasting platform, operating with a HITL model, equips policymakers with the foresight to navigate a shifting threat environment and drive robust, evidence-based decisions before crises materialize. Routine critical infrastructure biosurveillance, strengthened access controls, and AI-enhanced monitoring represent actionable, scalable tools to identify anomalies and intervene before harm escalates. This design ensures that automated, algorithmic insights are always balanced by human judgment and expertise.

Yet, the true foundation of a robust biosecurity posture lies in cultivating the right culture. Technology is wielded by people and culture remains the most powerful defense. The authors champion the development of a global biosecurity curriculum for universities, research institutions, and industry that moves beyond the adoption of preexisting materials for effective learning.³² Ideal biosafety training would use concrete case studies, such as material degradation, cyber-bio attacks, and AI-driven design, to move beyond abstract principles.³³ This would empower scientists and professionals at all levels to recognize and report dual-use concerns through clear, confidential channels, while fostering a shared sense of stewardship as our most fundamental line of defense.

Safe biological innovation is contingent on shared responsibility and concern for risks, coupled with a persistent commitment to reducing them. Biosecurity is no longer the exclusive domain of scientists or policymakers. It is an essential, collective undertaking spanning all disciplines, industries, and borders. As biology, digital information, and artificial intelligence converge, all actors involved, from governments to the private sector and individuals, must collaborate and anticipate risks to uphold a culture of responsible innovation. The outlook remains optimistic: With the right investments, strategic foresight, and cooperative spirit, stakeholders can responsibly harness biotechnological advances to benefit humanity while safeguarding against their misuse. The future of biosecurity depends on sustained commitment, adaptability, and readiness to address threats yet to be imagined.

Appendix

Abbreviations

AI	artificial intelligence
BW	biological weapons
BWC	Biological Weapons Convention
CRISPR	Clustered Regularly Interspaced Short Palindromic Repeats
DNA	deoxyribonucleic acid
DURC	dual-use research of concern
GPC	general purpose criterion
HIPAA	Health Insurance Portability and Accountability Act
HITL	Human-in-the-Loop
IAEA	International Atomic Energy Agency
iGEM	International Genetically Engineered Machine
LLM	large language model
MIC	microbiologically influenced corrosion
NGO	nongovernmental organization
OPCW	Organisation for the Prohibition of Chemical Weapons
OT	operational technology
RevCon	Review Conference
S&T	science and technology
UN	United Nations
UNODA	United Nations Office for Disarmament Affairs
U.S.	United States
WMD	weapon of mass destruction

Glossary

Accountability vacuum	A gap in global biosecurity efforts resulting from a reactionary approach to bioweapons due to a focus on historical agents.
Biosecurity	Policies and practices that protect against the deliberate misuse of biology to cause harm.
Critical biological commodity	Essential biological products, organisms, processes, or knowledge resources that are produced through, or dependent on, living systems and that are indispensable for sustaining public health, food and agriculture, medicine, industrial production, and environmental stability. These products include, but are not limited to, vaccines, therapeutics, diagnostic reagents, seed stocks, microbial strains, biological reference collections, and genetic databases.
Dual-use research of concern	Research that is intended to provide a clear benefit, but which could easily be misapplied to do harm. ³⁴
Functional harm	A proactive approach to pathogen risk assessment that identifies the inherent risks that novel and engineered pathogens may pose to humans, animals, plants, or inanimate entities, rather than a focus only on a defined set of pathogens of concern.
Metabolic sabotage	Pathogen-induced degradation of key functions for an entity's survival. This term encompasses a biological entity's cellular or immune function and inanimate material's chemical structure required to maintain integrity.

References

1. UNIDIR (United Nations Institute for Disarmament Research), "Biological Weapons Convention National Implementation Measures Database: Glossary," 2024, <https://bwcimplementation.org/page/glossary>.
2. United Nations Security Council, Resolution 1540, S/RES/1540, April 28, 2004, [https://undocs.org/S/RES/1540\(2004\)](https://undocs.org/S/RES/1540(2004)).
3. Filippa Lentzos, *Biological Threats in the 21st Century* (London: Imperial College Press, 2016).
4. United Nations, Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, signed June 17, 1925, League of Nations Treaty Series 94, no. 2138 (1929): 65–74.
5. United Nations, Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, April 10, 1972, 1015 UNTS 163 (hereafter, BWC).
6. Nicole E. Wheeler, "Responsible AI in Biotechnology: Balancing Discovery, Innovation and Biosecurity Risks," *Frontiers in Bioengineering and Biotechnology* 13 (2025), <https://doi.org/10.3389/fbioe.2025.1537471>; National Academies of Sciences, Engineering, and Medicine; Policy and Global Affairs, Committee on International Security and Arms Control; Committee on Enhancing Global Health Security Through International Biosecurity and Health Engagement Programs, "The Changing Biothreat Landscape" in *A Strategic Vision for Biological Threat Reduction: The U.S. Department of Defense and Beyond* (National Academies Press, 2020), <https://www.ncbi.nlm.nih.gov/books/NBK557957/>; and Michael Jacob, "Advances in AI and Increased Biological Risks" (briefer, Council on Strategic Risks, Washington, DC, July 12, 2024), <https://councilonstrategicrisks.org/2024/07/12/advances-in-ai-and-increased-biological-risks/>.
7. Anders Bergström et al., "Insights into Human Genetic Variation and Population History from 929 Diverse Genomes," *Science* 367, no. 6484 (2020), <https://doi.org/10.1126/science.aay5012>; Sylvie Briquet, Mathieu Gissot, and Olivier Silvie, "A Toolbox for Conditional Control of Gene Expression in Apicomplexan Parasites," *Molecular Microbiology* 117, no. 3 (2021): 618–631, <https://doi.org/10.1111/mmi.14821>; and Tien-Hung Lan et al., "Optogenetics for Transcriptional Programming and Genetic Engineering," *Trends in Genetics* 38, no. 12 (December 2022), [https://www.cell.com/trends/genetics/fulltext/S0168-9525\(22\)00140-8](https://www.cell.com/trends/genetics/fulltext/S0168-9525(22)00140-8).
8. Jaspreet Pannu et al., "Dual-Use Capabilities of Concern of Biological AI Models," *PLOS Computational Biology* 21, no. 5 (2025): e1012975, <https://doi.org/10.1371/journal.pcbi.1012975>.
9. Chaveso Cook, "Beyond Bullets, Bombs, Raids, and Rockets: The Environmental Impact of War," *War Room*, U.S. Army War College, April 3, 2025, <https://warroom.armywarcollege.edu/articles/environmental-impact-of-war/>; and Jeannie L. Sowers, Erika Weinthal, and Neda Zawahri, "Targeting Environmental Infrastructures, International Law, and Civilians in the New Middle Eastern Wars," *Security Dialogue* 48, no. 5 (2017): 410–430, <https://www.jstor.org/stable/26294229>.
10. J Knisz et al., "Microbiologically Influenced Corrosion—More than Just Microorganisms," *FEMS Microbiology Reviews* 47, no. 5 (2023), <https://doi.org/10.1093/femsre/fuad041>; Judit Telegdi, Absul Shaban, and Laszlo Trif, "Microbiologically Influenced Corrosion (MIC)," chap. 8 in *Trends in Oil and Gas Corrosion Research and Technologies*, ed. A. M. El-sherik (Woodhead Publishing, 2017): 191–214, <https://doi.org/10.1016/B978-0-08-101105-8.00008-5>; Sheikh Idrees Ali and Sheikh Nazir Ahmad, "Microbiologically Influenced Corrosion in Uncoated and Coated Mild Steel," *Scientific Reports* 15, no. 12629 (2025); and Qianwei Li et al., "Dual Role of Microorganisms in Metal Corrosion," *Frontiers in Microbiology* 16 (2025).
11. J Knisz et al., "Microbiologically Influenced Corrosion"; Telegdi, Shaban, and Trif, "Microbiologically Influenced Corrosion (MIC)"; Ali and Ahmad, "Microbiologically Influenced Corrosion in Uncoated and Coated Mild Steel"; and Li et al., "Dual Role of Microorganisms in Metal Corrosion."
12. J Knisz et al., "Microbiologically Influenced Corrosion"; Telegdi, Shaban, and Trif, "Microbiologically Influenced Corrosion (MIC)"; Ali and Ahmad, "Microbiologically Influenced Corrosion in Uncoated and Coated Mild Steel"; Li et al., "Dual Role of Microorganisms in Metal Corrosion"; and G. Kobrin et al., "Microbiologically Influenced Corrosion of Stainless Steels by Water Used for Cooling and Hydrostatic Testing," Nickel Institute, No. 10085, presented at the 58th Annual International Water Conference, Pittsburgh, PA, November 3–5, 1997.

13. Sabina Karačić et al., “Microbial Acidification by N, S, Fe and Mn Oxidation as a Key Mechanism for Deterioration of Subsea Tunnel Sprayed Concrete,” *Scientific Reports* 14, no. 22742 (2024): 22742, <https://doi.org/10.1038/s41598-024-73911-w>.
14. Mahboubeh Soleimani Sasani, “The Importance of Biosecurity in Emerging Biotechnologies and Synthetic Biology,” *Avicenna Journal of Medical Biotechnology*, October 19, 2024, <https://doi.org/10.18502/ajmb.v16i4.16738>.
15. Mahboubeh Soleimani Sasani, “The Importance of Biosecurity in Emerging Biotechnologies and Synthetic Biology,” *Avicenna Journal of Medical Biotechnology*, October 19, 2024, <https://doi.org/10.18502/ajmb.v16i4.16738>.
16. iGEM, “Team: Bielefeld-CeBiTec/Team,” 2018, <https://2018.igem.org/Team:Bielefeld-CeBiTec/Team>.
17. iGEM, “iGEM Responsibility,” 2024, <https://responsibility.igem.org/>.
18. Jonathan Smith, “Biotech Startups Face a Growing Wave of Cyberattacks,” *Labiotech*, October 21, 2020, <https://www.labiotech.eu/in-depth/cyberattack-biotech-startups-covid/>; Abi Olvera, “The Cyber-Biosecurity Nexus: Key Risks and Recommendations for the United States,” Council on Strategic Risks, September 14, 2023, <https://councilonstrategicrisks.org/2023/09/14/the-cyber-biosecurity-nexus-key-risks-and-recommendations-for-the-united-states/>; and Laura Adam and George H. McArthur, IV, “Substitution Attacks: A Catalyst to Reframe the DNA Manufacturing Cyberbiosecurity Landscape in the Age of Benchtop Synthesizers,” *Applied Biosafety* 29, no. 3 (2024): 172–180, <https://doi.org/10.1089/apb.2023.0035>.
19. Jeffrey T. LeJeune and Päivi J. Rajala-Schultz, “Unpasteurized Milk: A Continued Public Health Threat,” *Clinical Infectious Diseases* 48, no. 1 (2009): 93–100, <https://doi.org/10.1086/595007>.
20. U.S. National Security Commission on Emerging Biotechnology, “Charting the Future of Biotechnology: An Action Plan for American Security and Prosperity,” May 2025, <https://www.biotech.senate.gov/final-report/chapters/>.
21. Andy Greenberg, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History,” *WIRED*, August 22, 2018, <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.
22. Administration for Strategic Preparedness and Response, “Dual Use Research of Concern Oversight Policy Framework,” U.S. Department of Health and Human Services, 2024, <https://aspr.hhs.gov/S3/Pages/Dual-Use-Research-of-Concern-Oversight-Policy-Framework.aspx>; and National Institute of Health, “Dual Use Research of Concern (DURC) Institutional Review Entity,” Office of Intramural Research, n.d., <https://oir.nih.gov/sourcebook/committees-advisory-ddir/dual-use-research-concern-durc-institutional-review-entity>.
23. Gurpreet Dhaliwal, Askar A. Kleefeldt, and Alexandra Klein, “Biosecurity-By-Design to Safeguard Emerging Bioeconomies: Integrating Biosecurity Considerations into the Complete Biotechnology Innovation and Development Pipeline,” November 2023, https://www.nti.org/wp-content/uploads/2023/11/Biosecurity-by-design_final_Nov2023.pdf.
24. Ramanpreet Kaur, Dušan Gabrijelčič, and Tomaž Klobučar, “Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions,” *Information Fusion* 97 (September 1, 2023): 101804, <https://doi.org/10.1016/j.inffus.2023.101804>.
25. Abi Olvera, “The Cyber-Biosecurity Nexus: Key Risks and Recommendations for the United States,” Council on Strategic Risks, September 14, 2023, <https://councilonstrategicrisks.org/2023/09/14/the-cyber-biosecurity-nexus-key-risks-and-recommendations-for-the-united-states/>.
26. Bruce J. Wittmann et al., “Toward AI-Resilient Screening of Nucleic Acid Synthesis Orders: Process, Results, and Recommendations,” *bioRxiv*, December 4, 2024, <https://doi.org/10.1101/2024.12.02.626439>.
27. U.S. Department of Health and Human Services, “Cyber Security Guidance Material: How the HIPAA Security Rule Can Help Defend Against Cyber-Attacks,” June 7, 2017, <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html>.
28. Elizabeth Crawford et al., “Cyberbiosecurity in High-Containment Laboratories,” *Frontiers in Bioengineering and Biotechnology* 11 (2023), <https://doi.org/10.3389/fbioe.2023.1240281>.
29. Bioeconomy Information Sharing and Analysis Center, “BIO-ISAC: Biotech 2025,” 2025, <https://www.isac.bio/>; and European Union, “EU Non-Proliferation and Disarmament eLearning Course,” 2025, <https://nonproliferation-elearning.eu/>.
30. Gabrielle Essix, David Stiefel, and Jamie M. Yassif, “The Next 50 Years: Strengthening the Biological Weapons Convention—Explained,” Nuclear Threat Initiative, March 26, 2025, <https://www.nti.org/risky-business/the-next-50-years-strengthening-the-biological-weapons-convention-explained/>.

31. HealthMap, "HealthMap," 2012, <https://www.healthmap.org/en/>; ProMED, "Protecting Global Health, One Alert at a Time," International Society for Infectious Diseases, 2025, <https://www.promedmail.org/>; Dataminr, "Real-Time Event and Risk Detection," 2019, <https://www.dataminr.com/>; and Venu Shastri, "What Is User and Entity Behavior Analytics (UEBA)?" CrowdStrike, January 8, 2025, <https://www.crowdstrike.com/en-us/cybersecurity-101/identity-protection/user-and-entity-behavior-analytics-ueba/>.
32. European Union, "EU Non-Proliferation and Disarmament eLearning Course."
33. Federation of American Scientists, "Biosecurity Education Portal," 2025, <https://programs.fas.org/bio/educationportal.html>; iGEM, "iGEM Responsibility"; World Health Organization, "Learn to Build a Healthier World," WHO Academy, 2025, https://whoacademy.org/coursewares/course-v1:WHOAcademy-Hosted+H0126EN+2025_Q2; and Tonex Training, "GenAI in Dual-Use Biosafety Risk Fundamentals," 2025, <https://www.tonex.com/training-courses/genai-in-dual-use-biosafety-risk-fundamentals/>.
34. World Health Organization, "What Is Dual-Use Research of Concern?," December 13, 2020, <https://www.who.int/news-room/questions-and-answers/item/what-is-dual-use-research-of-concern>.

Timeline References

- a. Filippa Lentzos, *Biological Threats in the 21st Century* (London: Imperial College Press, 2016).
- b. Fredric Carlsson and Lars Råberg, "The Germ Theory Revisited: A Noncentric View on Infection Outcome," *Proceedings of the National Academy of Sciences of the United States of America* 121, no. 17 (2024), <https://doi.org/10.1073/pnas.2319605121>.
- c. United Nations, "Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare," signed June 17, 1925, League of Nations Treaty Series 94, no. 2138 (1929): 65–74.
- d. U.S. Department of State, "Statement Issued by President Nixon, November 25, 1969," Office of Electronic Information, Bureau of Public Affairs, September 19, 2007, <https://2001-2009.state.gov/r/pa/ho/frus/nixon/e2/83597.htm>.
- e. United Nations Office of Disarmament Affairs, "Biological Weapons Convention," 2025, <https://disarmament.unoda.org/en/our-work/weapons-mass-destruction/biological-weapons/biological-weapons-convention>.
- f. U.S. Department of State, "Biological Weapons Convention," 2009, <https://2001-2009.state.gov/t/ac/trt/4718.htm>.
- g. United Nations, "The Third Review Conference of the States Parties to the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction," BWC/CONF.III/23, Geneva, September 9–27, 1991.
- h. United Nations, "Final Declaration of the Fourth Review Conference of the Parties to the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction," BWC/CONF.IV, Geneva, November 25–December 6, 1996.
- i. Jeronimo Cello, Aniko V. Paul, and Eckard Wimmer, "Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template," *Science* 297, no. 5583 (2002): 1016–1018, <https://doi.org/10.1126/science.1072266>.
- j. Jonathan Tucker, "The Fifth Review Conference of the Biological and Toxin Weapons Convention (BWC)," Nuclear Threat Initiative, January 31, 2002, <https://www.nti.org/analysis/articles/biological-and-toxin-weapons-bwc/>.
- k. Administration for Strategic Preparedness and Response, "History of Research Oversight Policies," 2025, <https://aspr.hhs.gov/S3/Pages/History-of-Research-Oversight-Policies.aspx>.
- l. National Research Council (U.S.) Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, *Biotechnology Research in an Age of Terrorism* (Washington, DC: National Academies Press, 2004).
- m. National Academies of Sciences, Engineering, and Medicine, "Introduction" in *Dual Use Research of Concern in the Life Sciences: Current Issues and Controversies* (Washington, DC: National Academies Press, 2017), <https://www.ncbi.nlm.nih.gov/books/NBK458495/>.
- n. Martin Jinek et al., "A Programmable Dual-RNA-Guided DNA Endonuclease in Adaptive Bacterial Immunity," *Science* 337, no. 6096 (2012): 816–821, <https://doi.org/10.1126/science.1225829>.
- o. Antonio Regalado, "Top U.S. Intelligence Official Calls Gene Editing a WMD Threat," *MIT Technology Review*, February 9, 2016, <https://www.technologyreview.com/2016/02/09/71575/top-us-intelligence-official-calls-gene-editing-a-wmd-threat/>.
- p. Peter Stone et al., "Artificial Intelligence and Life in 2030: One Hundred Year Study on Artificial Intelligence," Stanford University, September 2016, <http://ai100.stanford.edu/2016-report>.
- q. Darren N. Nesbeth et al., "Synthetic Biology Routes to Bio-Artificial Intelligence," *Essays in Biochemistry* 60, no. 4 (2016): 381–391, <https://doi.org/10.1042/EBC20160014>.
- r. Cong Cao, "China's Evolving Biosafety/Biosecurity Legislations," *Journal of Law and the Biosciences* 8, no. 1 (2021), <https://doi.org/10.1093/jlb/lsab020>.
- s. United Nations, "Final Document of the Ninth Review Conference of the States Parties to the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction," BWC/CONF.IX/9, Geneva, December 21, 2022, https://unodaweb-meetings.unoda.org/public/2022-12/2022-1221%20BWC_CONF_IX_9%20adv%20vers.pdf.

About the Authors



Mr. Shreyash Borkar (Home Country: India)
PhD Student, University of Tübingen, Germany

Shreyash Borkar is an industrial PhD student as part of EU-funded Marie Skłodowska-Curie Actions Doctoral Network MAGic MOLFU. He is driven by the incredible power of biotechnology to design, build, and reprogram life, viewing it as one of the most transformative tools humanity has ever created. His expertise spans multiple angles of this field, including PhD research exploring metagenomes, hands-on experience as an entrepreneur, and strategic thinking on global policies and markets. Recognizing that such a “superpower” requires careful handling, he is committed to ensuring innovation and biosecurity advance together to responsibly empower and uplift the future.



Dr. Sriram Kumar (Home Country: India)
Postdoctoral Scientist, Institute of Virology, Münster, Germany

Sriram (Sri) Kumar is a postdoctoral fellow specializing in highly pathogenic respiratory viruses at the Institute of Virology in Münster, Germany. He completed his bachelor's and master's studies in biotechnology in India and Singapore, gaining early experience with medically relevant viruses. Sri received his Ph.D. from the University of Münster in 2023, after which he undertook a short postdoctoral fellowship at UT Southwestern Medical Center in Dallas, focusing on viral genomics. He later returned to Münster to commence his postdoctoral research full-time. In addition to his scientific work, Sri is actively engaged in policy discussions, particularly in the oversight of dual-use research involving enhanced Potential Pandemic Pathogens (ePPPs). He co-initiated and coordinated a Dual-Use Forum within a Research Training Group in Münster, addressing policy gaps at the intersection of biology and medicine. Sri also serves on the iGEM Biosafety and Biosecurity Committee and has led dual-use research workshops for undergraduates.



Ms. Kaitlyn Connors (Home Country: United States)
Master's Student, Georgetown University, United States

Kaitlyn (Kait) Connors is a master's student of Biohazardous Threat Agents & Emerging Infectious Diseases at Georgetown University. Her recently published wet lab research examines transcriptional changes that occur during co-infections of Dengue Virus and avirulent Wolbachia bacteria. She is also a science diplomacy fellow with the National Science Policy Network, examining global governance strategies for AlxBio applications among member nations of the Global Health Security Agenda's working group for biosafety and biosecurity. Kait holds a BS in Biology and Public Health from George Washington University.




NTI:bio

1776 Eye Street, NW | Suite 1000 | Washington, DC 20006 | www.nti.org

 facebook.com/nti.org

 [@NTI_WMD](https://twitter.com/NTI_WMD)

 [NTI_WMD](https://www.instagram.com/NTI_WMD)

 [Nuclear Threat Initiative](https://www.linkedin.com/company/nuclear-threat-initiative)