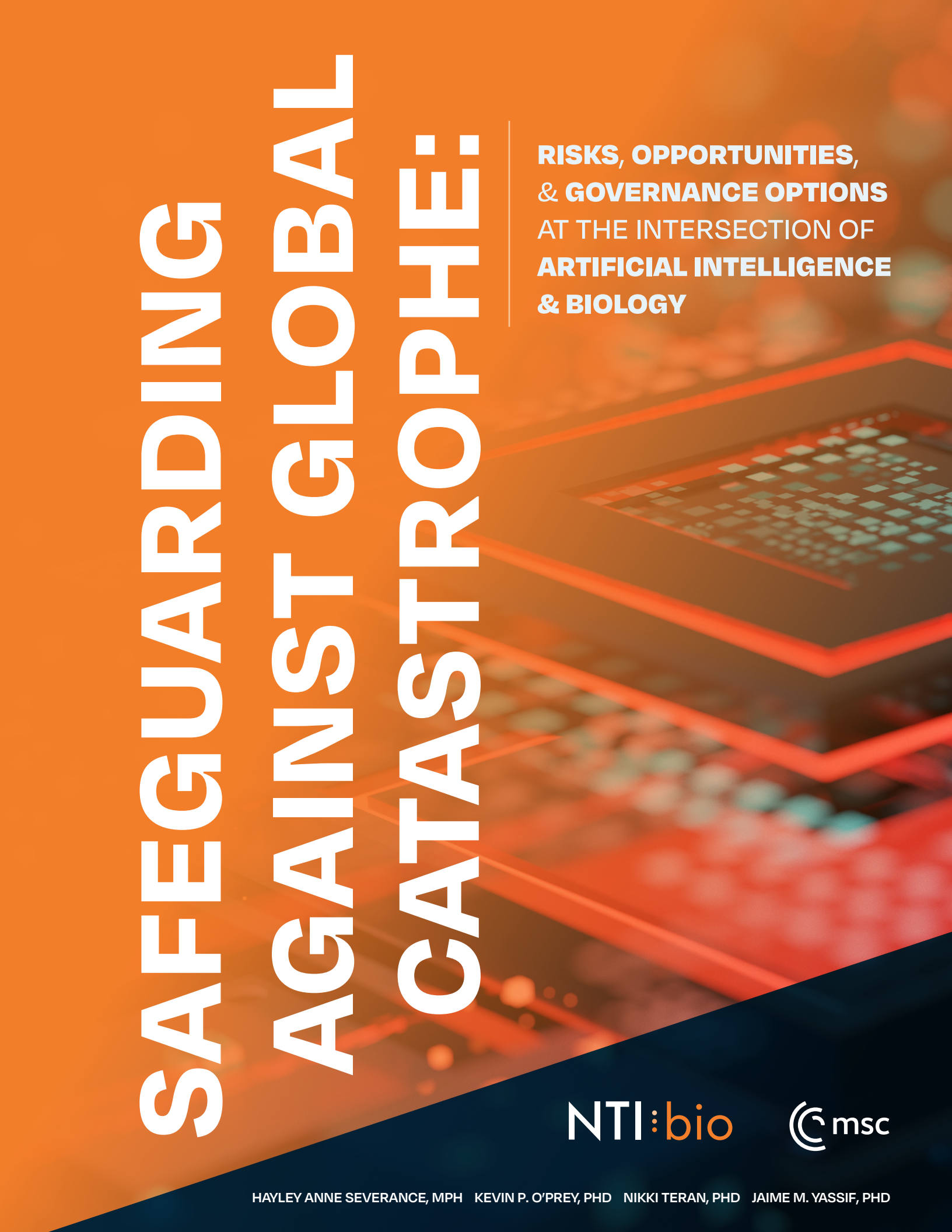
SAFEGUARDING AGAINST GLOBAL CATASTROPHE:

RISKS, OPPORTUNITIES, & GOVERNANCE OPTIONS AT THE INTERSECTION OF ARTIFICIAL INTELLIGENCE & BIOLOGY



NTI:bio

msc

HAYLEY ANNE SEVERANCE, MPH KEVIN P. O'PREY, PHD NIKKI TERAN, PHD JAIME M. YASSIF, PHD

We are grateful to Open Philanthropy for its support of our work to reduce global catastrophic biological risks. This exercise and report would not have been possible without its generous support.

The views expressed in this publication do not necessarily reflect those of the NTI Board of Directors or the institutions with which they are associated.

ABOUT THE REPORT

This report is based on insights from a tabletop exercise hosted by the Nuclear Threat Initiative (NTI) in collaboration with the Munich Security Conference (MSC) at the 2025 conference. The exercise focused on mitigating risks at the intersection of artificial intelligence and the life sciences. This effort marks the fifth in a series of joint NTI–MSC exercises designed to bring together senior leaders from government, industry, and civil society to examine global security threats stemming from shared vulnerabilities to high-consequence biological events and to identify concrete actions the international community can take to reduce these risks.

ABOUT NTI

NTI is a nonprofit, nonpartisan, global security organization focused on reducing nuclear, biological, and emerging technology threats imperiling humanity. Based in Washington, DC, NTI collaborates with governments and organizations to raise awareness, advocate, and implement creative solutions. As an independent and trusted partner, NTI transcends traditional thinking and stimulates new ways to address urgent threats. NTI | bio is the program that advances NTI's biosecurity and global health security mission.

ABOUT THE MUNICH SECURITY CONFERENCE

The Munich Security Conference (MSC) is the world's leading forum for debating international security policy. It is a venue for diplomatic initiatives to address the world's most pressing security concerns.

ACKNOWLEDGMENTS

The authors acknowledge those instrumental in the development and execution of this senior-level tabletop exercise. First, we thank our partners at the MSC, including Ambassador Wolfgang Ischinger, who co-chaired the exercise, and commend them for their efforts to raise biosecurity as an essential pillar of international security. We are grateful to the exercise participants whose valuable insights, expertise, and engagement were crucial to the success of the project. We thank Long Story Short for producing engaging exercise videos and for helping to shape our fictional narrative.

At NTI, we thank the members of NTI | bio who provided support for the project. Christopher R. Isaac and Sara Kaufman contributed valuable research and planning assistance. From NTI's Communications team, Scott Nolan Smith led the development of video production for this exercise, provided valuable comments on this manuscript, and led the report-publication process. We thank Secretary Ernest J. Moniz for co-chairing the exercise and Joan Rohlfing for her active participation.

We also thank Ryan Ritterson and Audrey Cerles at Deloitte, who developed the epidemiological model underpinning this exercise and informed development of the exercise.

Hayley Anne Severance, MPH
Deputy Vice President, Global Biological Policy and Programs, NTI

Kevin P. O'Prey, PhD
Managing Partner, The Palisades Group, LLC

Nikki Teran, PhD
Managing Member, Emerging Technology Solutions, LLC

Jaime M. Yassif, PhD
Vice President, Global Biological Policy and Programs, NTI

Contents

We cannot allow the pursuit of AI superiority to become a race to the bottom on safety and security

---

As global security hangs in the balance, the time for action is now.

Foreword

Remarkable advances in artificial intelligence (AI), biotechnology, robotics and automation, quantum computing, and other emerging technologies are transforming the technological foundation of human civilization. As these powerful technologies and their practical applications become more widely accessible, they promise breakthrough benefits for all of us. Yet, like all radical transformations, there are risks—many of which cannot be easily predicted.

We consider the convergence of AI with the life sciences (AIxBio, for short) to be a case in point. AIxBio innovations are revolutionizing the life sciences as you read this. The Royal Swedish Academy of Sciences awarded the 2024 Nobel Prize in Chemistry to the team behind AlphaFold, the AI protein-structure prediction tool that is transforming the field of structural biology. Other AIxBio innovations promise radical improvements to our capacity to detect outbreaks, rapidly develop a range of medical countermeasures, and deliver better health outcomes on a daily basis.

Yet, the history of technological revolutions offers important reasons for caution: technological innovations can create risks of deliberate misuse or accidents, and managing or controlling the use of a technology after it has been widely adopted is very difficult. Knowledge of the atomic nucleus as the basis for a revolution in physics, a source of sustainable energy, or as the basis for devastating weapons, is a particularly compelling example that reinforces these lessons. While atomic energy and nuclear weapons programs were essentially "owned" by technologically advanced national governments, emerging technologies empower individuals and private organizations across the globe to create and innovate in ways that were not previously possible. For instance, one of the leading AI firms, Anthropic, found that its latest large language model could be used by an individual with a basic technical background to help develop a chemical, biological, or nuclear weapon. While Anthropic deserves praise for recognizing and actively working to mitigate these risks, not all private companies may be as responsible. Moreover, existing arms control institutions like the Biological Weapons Convention do not have the necessary capabilities and are not agile enough to manage this dynamic challenge.

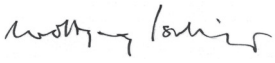
Current popular debates on this subject present a false dichotomy: AI evangelists depict AI's innovations as inevitable and fundamentally beneficial, while AI pessimists warn of catastrophic threats. In pursuit of a more balanced and nuanced discussion, we convened a group of senior international leaders from government, industry, academia, and think tanks for a tabletop exercise at this year's Munich Security Conference. We challenged the participants with a scenario that exposed the devastating consequences that can result from the misuse of AIxBio capabilities. As AI-enabled tools—especially biodesign tools-—become more accessible and sophisticated, we anticipate that the barriers to entry for malicious actors will decline, at the same time as the potential for harm grows.

Our discussions led us to the conclusion that there are pragmatic solutions that balance fostering innovation, while protecting against the misuse of powerful AIxBio capabilities. Establishing guardrails that safeguard AIxBio capabilities is the answer, requiring bold, collaborative efforts between government policymakers and leading innovators in the private sector and academia.

We cannot allow the pursuit of AI superiority to become a race to the bottom on safety and security. The stakes are too high. We must come together to define the risks we are unwilling to accept and take the necessary steps to safeguard the positive potential of these emerging technologies in the pursuit of a safer, more secure, healthier, and more prosperous world.

The pace of innovation is well ahead of our ability to govern the associated risks. As global security hangs in the balance, the time for action is now, before the proverbial horse is out of the barn.

Ernest J. Moniz
Co-Chair and CEO
NTI



Ambassador (ret.)
Wolfgang Ischinger
President Foundation
Council of the
MSC Foundation

Executive Summary

Imagine this: A global pandemic that eventually results in more than 850 million cases and 60 million deaths begins, sparked by a novel enterovirus strain that was intentionally engineered by an extremist group using artificial intelligence–enabled capabilities to engineer living systems (referred to as AIxBio capabilities). This was the fictional scenario featured in a tabletop exercise on safeguarding against risks at the convergence of AI and the life sciences that NTI conducted in partnership with the Munich Security Conference (MSC) in February 2025.

The exercise explored the opportunities and risks associated with advances in AIxBio capabilities, considered challenges and opportunities for safeguarding those capabilities, and explored innovative approaches for preventing their misuse. Exercise participants included 14 senior leaders and experts from around the world, with decades of combined experience in AI, biotechnology, international security, and public health.

The fictional scenario depicted a rapidly spreading pandemic. Early research into the causative agent, named the neo-enterovirus, revealed signs of genetic engineering that enabled the virus to invade an individual's central nervous system and cause paralysis, respiratory failure, and death. Ultimately, the exercise revealed that the outbreak was triggered by an intentional release of the engineered pathogen by a well-resourced extremist group that posed as a synthetic biology startup to use AIxBio capabilities to engineer a virus capable of causing a global catastrophe.

As the hypothetical scenario unfolded, discussion among exercise participants led to the following key findings:

✓ FINDING 1

The fictional pandemic facilitated by the exploitation of AIxBio capabilities is a plausible, high-consequence bioterror scenario that technical experts and counter-terrorism professionals find deeply concerning and worthy of near-term action to prevent.

✓ FINDING 2

Rapidly advancing AIxBio capabilities are eroding barriers to bioweapons development by malicious actors, while also raising the ceiling of possible harms.

✓ FINDING 3

Existing security regimes are not equipped to address AI-enabled biological threats, but multiple intervention opportunities exist to reduce the risk that these capabilities could be exploited for biological weapons development.

✓ FINDING 4

AIxBio model developers can lead in developing best practices and technical solutions to reduce risks throughout the AI-model development life cycle.

✓ FINDING 5

There is a need for an official forum at the international level for communication and coordination to assess and address AIxBio risks.

✓ FINDING 6

Efforts to manage AI risks must take into account the benefits of AIxBio capabilities and avoid placing undue constraints on scientific benefits.

To address these findings, the authors developed the following recommendations:

Recommendation 1

National governments, industry, and philanthropic organizations should politically support and fund a comprehensive research and development agenda to establish effective guardrails for AIxBio technologies and applications.

Recommendation 2

National governments should establish institutes focused on AI safety and security, whose missions include safeguarding AIxBio capabilities.

Recommendation 3

International partners should collaborate via a global platform to develop and disseminate best practices for AIxBio safeguards.

Recommendation 4

Global scientific and national security communities should actively leverage AI's beneficial applications in biosecurity and pandemic preparedness.

About the Exercise

The world is experiencing a revolution in bioscience and biotechnology, which is accelerating due to the convergence of artificial intelligence with the life sciences (AIxBio). These advances offer tremendous potential societal benefits, including for human health and economic development, but they also pose significant dual-use risks. The availability of increasingly sophisticated and widely distributed tools for engineering living systems, which continue to evolve with rapid advances in AI, makes the world increasingly vulnerable to accidental or deliberate misuse of AIxBio capabilities *(see Box 1)*.

To explore these risks and the opportunities to reduce them, NTI partnered with the Munich Security Conference (MSC) to conduct a tabletop exercise on safeguarding the convergence of AI and biology. For the exercise, senior international leaders along with experts in artificial intelligence, biotechnology, international security, and public health assembled to

EXPLORE the opportunities and risks associated with rapid advances in AI-enabled capabilities for engineering living systems (AIxBio capabilities)

DISCUSS challenges and opportunities for safeguarding AIxBio capabilities

EXAMINE the challenges associated with governing dual-use technologies

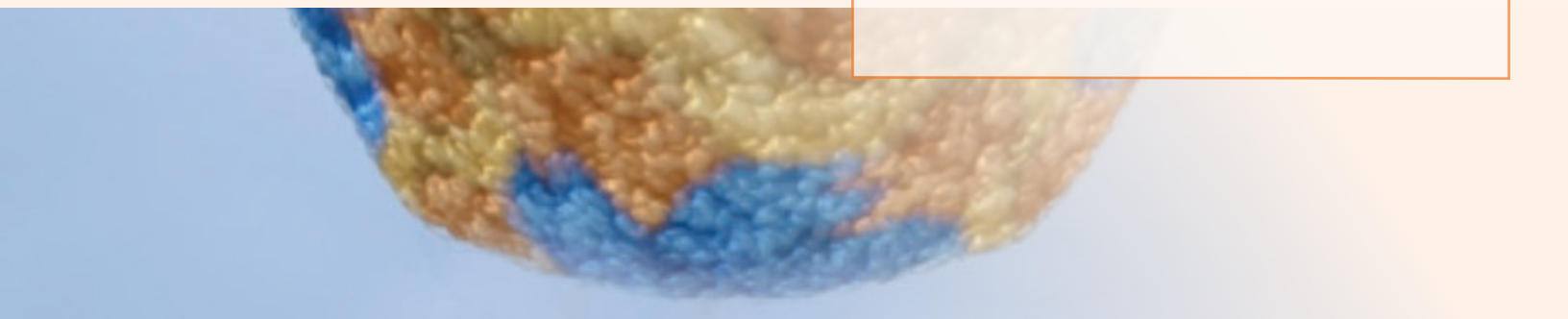
EXPLORE innovative approaches for securing AIxBio capabilities and preventing their misuse

BOX 1.

AIXBIO CAPABILITIES AND BIOLOGICAL DESIGN TOOLS

AIxBio capabilities refer to functionalities at the intersection of artificial intelligence and the life sciences. These functions employ a wide variety of tools such as large language models (LLMs), biological design tools (BDTs), and AI-enabled automation of the life sciences. These AIxBio capabilities are likely to accelerate advances in the life sciences in a wide range of ways, from helping scientists design new biological systems to creating new methodologies for conducting bioscience experiments at scale.

Biological design tools are trained on biological data and are developed to provide insights, predictions, and designs related to biological systems. Protein design tools are a classic example of BDTs—such tools can be used to design novel proteins for a wide range of therapeutic and other purposes. The capabilities of BDTs are evolving rapidly. Future models could enable the design of more complex biological systems—for example, groups of bio-molecules working together to perform more complex functions, such as cell signaling or enzymatic production of materials—or genome sequences that encode entire blueprints of viruses or bacteria. BDTs are also likely to be integrated with LLMs in the near future, which could significantly broaden access to a larger range of nonexpert users.



PARTICIPANTS

The exercise included 14 senior leaders and experts with decades of combined experience in artificial intelligence, biotechnology, international security, and public health from across the globe.

2025 NTI–Munich Security Conference Tabletop Exercise Participants

Co-Chairs

Ambassador Wolfgang Ischinger
President
Foundation Council of the MSC Foundation

Dr. Ernest J. Moniz
Co-Chair & CEO
NTI

Participants

Dr. Graham Allison
Douglas Dillon Professor of Government
Harvard University John F. Kennedy School of Government

Dr. Elizabeth Cameron
Professor of the Practice of Health Services, Senior Advisor to the Pandemic Center
Brown University School of Public Health

Dr. James Diggans
Distinguished Scientist, Bioinformatics and Biosecurity
Twist Bioscience

Dr. Gerald Epstein
Senior Scientist
RAND

Mr. Callam Fletcher
Founder
Asia Leader Series

Prof. Jane Halton
Chair
Coalition for Epidemic Preparedness Innovations (CEPI)

Dr. Emily LeProust
CEO & Co-Founder
Twist Bioscience

Mr. Daniel Poneman
Distinguished Fellow
Atlantic Council

Dr. Xiao Qian
Deputy Director
Tsinghua University, Center for International Security and Strategy

Mr. Bryan Rich
Senior Managing Director and Global AI Lead for Health, Public Sector, and Defense
Accenture

Ms. Joan Rohlfing
Former President and Chief Operating Officer
NTI

Mr. Brian Tse
Founder & CEO
Concordia AI

Col. Roman Woelfel
Director
Bundeswehr Institute of Microbiology

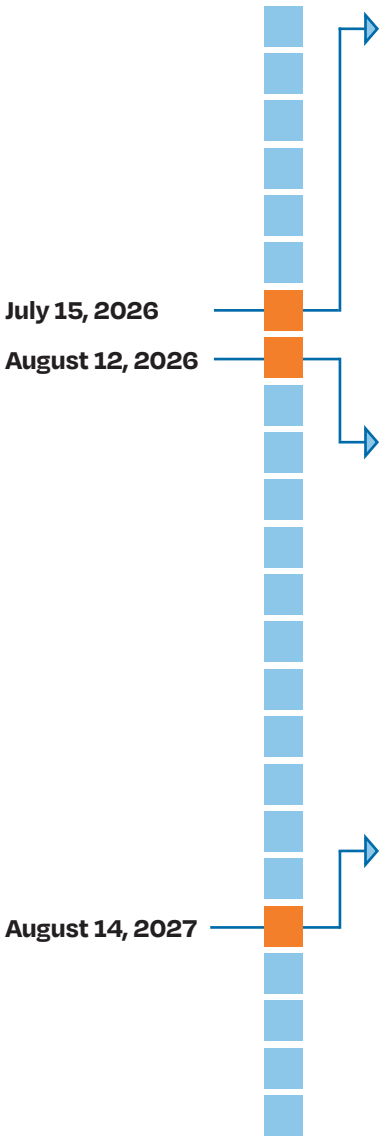
The Hon. Juan C. Zarate
Senior Adviser (Nonresident)
Warfare, Irregular Threats, and Terrorism Program and Human Rights Initiative, Center for Strategic & International Studies (CSIS)

Overview of Exercise

EXERCISE SCENARIO

The scenario developed for this tabletop exercise is set in the fictional country of Ankovia and depicts a pandemic sparked by a novel enterovirus strain that was intentionally engineered by an extremist group using AIxBio capabilities. The extremist group releases the resulting bioweapon, unleashing an outbreak that rapidly spreads globally, ultimately causing more than 850 million cases and 60 million deaths. The exercise was organized into three sequential "moves" that depict scenario developments, which are summarized in Table 1 and described in greater detail in the following paragraphs.

Table 1. Scenario Design and Exercise Moves



Move 1

Scenario

- 54,712 cases/821 deaths as a result of an ongoing outbreak detected in Ankovia
- 13 countries are affected (including Ankovia).
- Deliberate dispersal is suspected as the virus shows signs of genetic engineering; investigation is ongoing.
- No effective medical countermeasures (MCMs); ventilator shortages emerge.

Discussion Themes for Participants

- Characteristics of the modified neo-enterovirus.
- Characteristics of BDTs and the lack of existing guardrails.

Move 2

Scenario

- 363,333 cases/9,715 deaths
- World Health Organization declares a pandemic emergency.
- Ankovian extremist group KILL-9 is identified as the attack perpetrators with confirmation the group used BDTs.
- AI accelerates progress of MCM development.

Discussion Themes for Participants

- Unique risks and benefits of BDTs

Move 3

Scenario

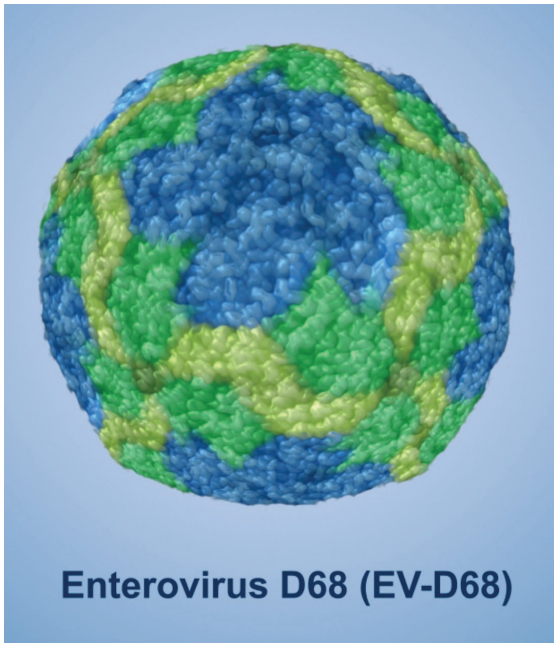
- 856,763,136 cases/60,206,021 deaths
- Distribution of an effective vaccine begins.
- An International Commission of Inquiry into the Origins of the Neo-enterovirus forms.

Discussion Themes for Participants

- Courses of action to manage future risks

The exercise features a fictional news report of an emerging disease outbreak.

MOVE 1 (July 15, 2026) begins with the detection of an unusual enterovirus outbreak in the fictional country of Ankovia. The outbreak is immediately suspicious, as cases are detected simultaneously in several of Ankovia's urban centers. Early scientific investigations reveal hallmarks of genetic engineering of the virus, potentially facilitated by biological design tools. Although the virus is closely related to enterovirus D68—a common cause of mild respiratory illness in children—it appears to have been modified to enable invasion of the central nervous system. In 10 percent of cases with the modified strain, the infection progresses to acute flaccid myelitis, leading to respiratory failure and death. This is approximately 200–400 times greater than the rate of respiratory failure from untreated poliomyelitis (the disease caused by the polio virus, which is a closely related enterovirus). The neo-enterovirus seems to have been engineered to overcome preexisting immunity to enterovirus D68 in the population.



Shortly thereafter, neo-enterovirus disease cases are detected in 12 additional countries. In total, almost 55,000 cases and 821 deaths were reported globally in Move 1. There are no effective vaccines or therapeutics against the virus. As the outbreak rapidly expands, ventilator shortages emerge in some countries.

The discussion in Move 1 explored the definition and characteristics of BDTs, how they might have been used to engineer the neo-enterovirus, how the modified virus differs from natural enterovirus strains, and the lack of existing guardrails to prevent exploitation of BDTs.

MOVE 2 (August 12, 2026) continues with accelerating international spread of the virus and the declaration of a "pandemic emergency" by the World Health Organization (WHO). The worldwide case count stands at more than 360,000 cases with almost 10,000 deaths. Vaccine development begins and is accelerated by AI tools. Nevertheless, global healthcare systems reach their breaking points. Ventilator shortages become severe in low-resource settings.

During this period, authorities identify the Ankovian extremist group KILL-9 as the perpetrators of the attack. KILL-9 is a well-resourced group with scientific expertise, counting trained microbiologists and virologists among its members. Group members express apocalyptic goals provoked by extreme dissatisfaction with the status quo in Ankovia. The group's members are optimistic about surviving the pandemic while inflicting severe harm on the rest of the population because they live on a well-stocked and self-sustaining rural compound. To obtain the materials, equipment, and reagents (including synthetic DNA) needed to engineer the neo-enterovirus, the group had posed as a synthetic biology startup. Investigation of evidence collected from KILL–9's compound confirms that BDTs and related biological AI tools were used as part of the viral engineering process, including a protein-structure prediction tool, DNA fragment assembly tool, and a host-pathogen interaction tool (*see Box 2*). Additionally, the investigation finds that KILL–9 had drafted alternative plans, including one that involved resurrecting a strain of the 1918 H1N1 pandemic influenza virus and modifying it with the assistance of BDTs.

The discussion in Move 2 examined the unique risks posed by AI-enabled tools and how the dual-use nature of these capabilities creates heightened biosecurity challenges. Participants also considered how these technological advances shaped state and nonstate actors' capabilities and intentions.

BOX 2.

BIODESIGN TOOLS USED BY KILL–9

Protein structure prediction tool: Predicts three-dimensional protein structures from amino acid sequences and provides a computer-generated model of the structure.

Applications include the following:

- Understanding cellular processes and disease pathways
- Identification of potential drug targets and the design of small molecules
- Engineering of proteins with desired properties for industrial applications
- Development of novel biomaterials and biosensors

DNA fragment assembly tool: Generates short sequence fragments that can be assembled into a longer nucleic acid sequence.

Applications include the following:

- Accelerated research and development on emerging viruses
- Advanced vaccine development, prototyping, and manufacturing
- Improved viral vector design and approaches
- Optimized biomanufacturing

Host-pathogen interaction tool: Predicts interactions between pathogen and host proteins during infection or exposure.

Applications include the following:

- Accelerated and rational drug discovery
- Understanding infection and pathogenesis mechanisms
- Personalized medicine to prevent disease
- Early countermeasures and responses to emerging threats

The exercise scenario features accelerating international spread of the fictional neo-enterovirus.

MOVE 3 (August 14, 2027) takes place approximately one year after Move 2, as global distribution of a new vaccine begins. More than 850 million cases and more than 60 million deaths are recorded. However, the death toll continues to rise even as global distribution of the vaccine proceeds. In this move, the International Commission of Inquiry into the Origins of the Neo-enterovirus is formed to investigate the first pandemic caused by an AI-engineered pathogen. As commission members, exercise participants are tasked with developing recommendations to prevent misuse of BDTs and AIxBio capabilities more broadly.

- **TECHNICAL SOLUTIONS**, such as controls on AIxBio model training data, managed access approaches to powerful AIxBio models, and built-in screening mechanisms for BDTs
- **GOVERNANCE FRAMEWORKS**, including punitive approaches, incentive-based measures, and normative approaches (e.g., codes of conduct) at the national and international levels

Participants were asked to consider each of the proposed courses of action in terms of effectiveness, feasibility, and the likelihood of constraining beneficial scientific advances, and then make a recommendation on whether the measure should be adopted, rejected, or further explored.

Discussion and Key Findings

Exercise participants engaged in interactive discussions that examined technical feasibility as well as the security and policy implications of the scenario. The discussions generated a range of valuable insights and key findings, as described in the following paragraphs.

✓ FINDING 1

The fictional pandemic facilitated by the exploitation of AIxBio capabilities is a plausible, high-consequence bioterror scenario that technical experts and counterterrorism professionals find deeply concerning and worthy of near-term action to prevent.

From a technical perspective, participants affirmed that the scenario represented a realistic threat based on current and anticipated near-term AIxBio capabilities. They observed that the exercise demonstrated that existing and emerging BDTs and AI biological tools provide technically feasible pathways to engineer pandemic pathogens with novel properties.

From a security and counterterrorism perspective, participants assessed the scenario as particularly concerning because of the plausible convergence of gaps and weaknesses in biosecurity and public health systems, actors' apocalyptic intentions, and capabilities of sophisticated actors. Participants found that, taken together, these factors create risks that cannot be effectively managed by available security measures and current capabilities for containing infectious disease outbreaks. Several participants suggested that this scenario is a classic example of the type of high-consequence events that—despite their assumed low probability—counterterrorism and security professionals find realistic and deeply concerning.

Participants referenced historical examples of capable radical groups similar, in some ways, to the fictional KILL-9 group in the exercise scenario, specifically highlighting the bioweapons development attempts by the apocalyptic Japanese cult Aum Shinrikyo and al Qaeda's Tarnak Farms program. Both programs were relatively advanced efforts by highly motivated terrorist groups to acquire and use weapons of mass destruction. These and other groups failed primarily because they lacked sufficient scientific expertise or were intercepted by law enforcement or intelligence agencies before they could execute their plans. Participants noted that AI-enabled tools, especially LLMs, could lower the barriers to entry for nonexperts, potentially enabling future actors to succeed where previous attempts failed.

Throughout the exercise, participants considered how AI, in particular, amplifies biosecurity risks. In addition to lowering barriers to entry, AI-enabled tools have the potential to ease the development of biological agents, creating conditions where less-skilled actors may be able to engineer enhanced pandemic pathogens that previously would have required extensive specialized expertise. The potential for AI tools to be exploited by malicious actors to develop biological weapons represents a force multiplier that traditional security frameworks are not prepared to prevent or effectively address.

✓ FINDING 2

Rapidly advancing AIxBio capabilities are eroding barriers to bioweapons development by malicious actors, while also raising the ceiling of possible harms.

Tabletop exercise participants agreed that the scientific barriers to developing biological weapons are dropping due to advances in AIxBio capabilities. Although participants broadly concurred that the ability to create or modify a pathogen like the neo-enterovirus with the assistance of BDTs is currently limited to technically sophisticated actors, they offered that less sophisticated actors could soon be enabled by rapid advances in both AI tools and related technologies (such as LLMs, automation, and closed-loop engineering in cloud and robotic laboratories). Furthermore, beyond lowering barriers to entry, BDTs could simultaneously raise the ceiling of possible harms by enabling the design of enhanced or entirely novel biological agents. Box 3 describes automated science in this context.

BOX 3.

AUTOMATED SCIENCE

The term "automated science" refers to the use of AI to automate steps in scientific discovery or the transfer of the entire process to AI. A major challenge in scientific discovery is the vast number of possible experiments that could be conducted, making systematic exploration of all options by humans impracticable. AI has the potential to automate this exploration and intelligently choose scientific questions and design experiments that are likely to be the most informative and useful to explore.

The fictional scenario highlights the beneficial application of AI in support of vaccine development to bolster response efforts.

The fictional scenario reveals that scientists identified a new virus closely related to enterovirus D68 with evidence that it was engineered to be more dangerous to humans.

Exercise participants emphasized that the convergence of various AI technologies is driving these trends forward. Several participants described how LLMs can provide information and guidance, BDTs can facilitate the design of novel biological constructs, and automated laboratories can dramatically accelerate the design-build-test cycle for engineered biological systems. Participants envisioned a near-future scenario in which a human user could simply describe their ultimate goal to an LLM, which would then interpret the request and direct BDTs and robotic laboratories to carry out research with minimal human involvement or oversight.

Multiple participants noted other ways that AI is lowering key barriers. Use of AI may significantly reduce the level of microbiology and molecular biology expertise traditionally needed to plan and design sophisticated pathogen modifications. Nonetheless, some participants argued that certain obstacles remain, many of which are immune to AI-enabled disruption. These choke points include physical access to essential reagents and equipment, particularly for steps that require specialized materials or facilities. Similarly, several participants stressed that, while AI may guide actors through complex protocols, the practical challenges of obtaining physical resources and the tacit knowledge required to use them continue to pose barriers to successfully developing an effective weapon.

The discussion extended beyond nonstate actors to consider the implications for state-sponsored programs. Participants recognized that although the exercise scenario focused on a notional nonstate actor, the same AIxBio capabilities could bolster state actors' biological weapons development capabilities. One participant offered a different perspective, arguing that states typically do not face expertise barriers for developing biological weapons, suggesting that they have less need to use AI to achieve their objectives. Participants also emphasized that AI would be effective if states chose to incorporate it into their programs to enhance the effectiveness of their weapons. However, given the dual-use nature of the technology, there would be no feasible way to prevent them from doing so, apart from efforts to shape intent.

One participant highlighted an asymmetry in how AI technologies could differentially benefit state and nonstate actors. The participant suggested that AI may prove more beneficial for the *offensive* capabilities of nonstate actors while having a greater relative impact in strengthening the *defensive* capabilities of state actors. The argument is that, for nonstate actors (as noted previously), AI can dramatically lower traditional barriers to access, enabling them to design and potentially create dangerous pathogens with far less expertise than previously required. For state actors—who likely already have the technical sophistication to have an offensive capability, if desired—AI can provide a substantial defensive advantage. It can enhance biodefense through advanced biosurveillance systems, rapid pathogen characterization, accelerated vaccine development, and improved modeling of outbreak scenarios. These dynamics could create a situation in which AI disproportionately expands the pool of potential bioterrorism actors while simultaneously enhancing state-level defensive capabilities.

✓ FINDING 3

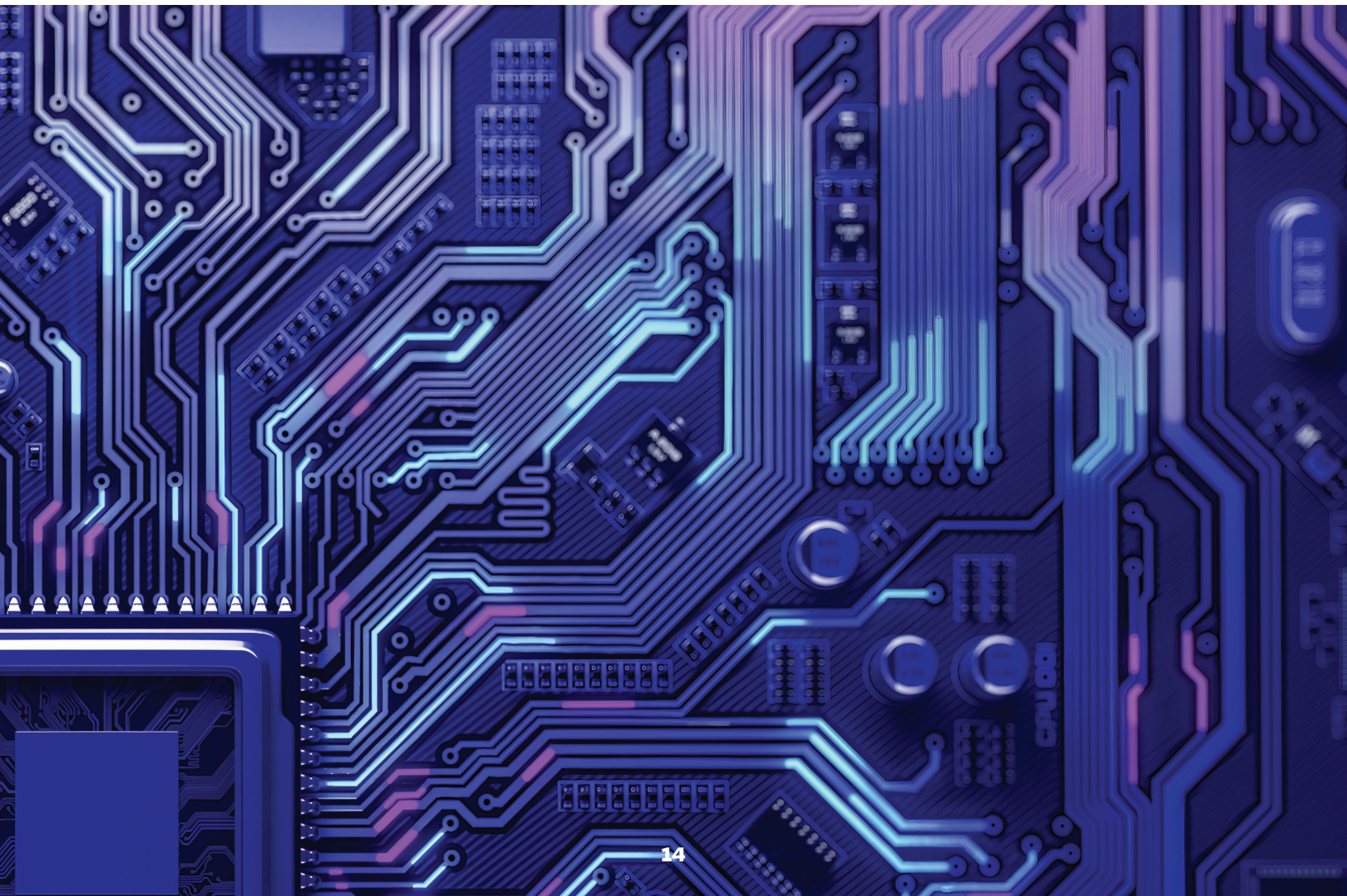
Existing security regimes are not equipped to address AI-enabled biological threats, but multiple intervention opportunities exist to reduce the risk that these capabilities could be exploited for biological weapons development.

Exercise participants reached consensus that immediate action is needed to manage AIxBio risks. However, they also agreed that existing security regimes are not up to the task. Not one participant supported a "wait and see" approach in response to the emerging risks. Instead, multiple participants emphasized that effective intervention requires examining the entire life cycle of AI-enabled biological weapons development, from ideation, design, development, and testing to deployment.

Participants identified multiple intervention opportunities beyond technical controls on software, reagents, and the equipment needed to design and build a biological weapon. These interventions include monitoring life-science supply chains, digital communications, and financial transactions that might indicate malicious activity.

In addition, the transition from digital agent design to physical synthesis and acquisition represents a crucial point where security measures can be implemented. Participants emphasized that this transition involves not only DNA synthesis but also procurement of equipment, reagents, laboratory access, and even baseline biological agents for further modification. Participants further suggested interventions at the design and ideation stage, such as managing access to and screening the outputs of BDTs, which can effectively reduce weaponization risks (discussed further in Finding 4).

Participants also expressed concern that malicious actors could use AI to bypass biosecurity controls such as DNA-screening algorithms, observing that many legitimate companies in the biotechnology supply chain lack the resources to invest in capabilities to detect such attempts at misuse. If not proactively addressed, participants noted, the use of AI to circumvent biosecurity measures could become a growing vulnerability—one that could increasingly undermine the effectiveness of existing risk-mitigation strategies.

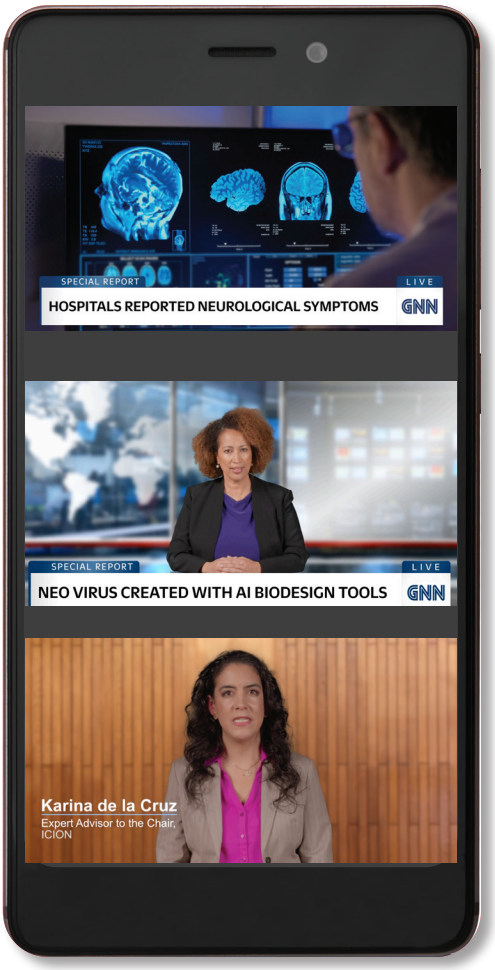


Exercise participants consistently emphasized that interventions must be targeted, rather than overly broad or hasty. Unfocused approaches, such as blanket restrictions or undifferentiated regulatory approaches, could fail to address critical risks while unnecessarily constraining beneficial scientific research. They also warned that hastily implemented measures might create a false sense of security without addressing core vulnerabilities. Participants advocated for a balanced approach that meaningfully reduces risks without hampering scientific progress. This approach centered on three principles:

- **FIRST**, participants stressed the importance of identifying the most critical steps in the biological weapons design, development, and deployment pathway for intervention. Rather than attempting to control every aspect of AIxBio development, risk-reduction measures should be implemented at critical chokepoints and should consider impacts of evolving technologies.
- **SECOND,** participants emphasized that interventions must be carefully designed to target relevant types of actors, recognizing that state actors, sophisticated nonstate groups, and less-capable actors each present different challenges, threats, and vulnerabilities.
- **THIRD**, while encouraging innovative thinking, participants also recognized the value of learning from established regulatory initiatives—both successful and failed. One participant specifically drew parallels to cryptocurrency regulation, suggesting that the financial sector's experience in tracking digital assets and preventing illicit transactions could provide valuable lessons for monitoring AIxBio capability development and detecting suspicious activities.

Notably, participants expressed a limited appetite for creating entirely new regimes, instead favoring targeted enhancements to existing ones or other innovative approaches. They recognized that existing frameworks and institutions—including arms-control regimes such as the Biological Weapons Convention (BWC) and international organizations such as WHO—lack the technical expertise and adaptive capacity needed to address rapidly evolving AI-enabled biological threats.

Given the fast-moving nature of AI development, participants emphasized that traditional regulatory processes would likely be too slow to respond effectively to emerging challenges. Instead, they recommended looking to other dynamic sectors—such as banking and cybersecurity—for examples of innovative governance approaches that can be quickly developed and adapted. Participants stressed the need for ongoing evaluation of oversight mechanisms, involving experts who can continuously assess evolving risks in real time, rather than relying on static regulatory frameworks. They emphasized that effective governance would require creative, responsive guardrails that can evolve alongside the technology, recognizing that the current understanding of these risks is still evolving and will require continuous refinement as AIxBio capabilities advance.



✓ FINDING 4

AIxBio model developers can lead in developing best practices and technical solutions to reduce risks throughout the AI-model development life cycle.

Exercise participants broadly agreed that the AIxBio community—especially BDT model developers from academia and industry—should take the lead in developing self-governance norms, best practices, and technical solutions that build in biosecurity by design. This approach recognizes that developers understand both the potential benefits and risks of their models much better than traditional regulators.

There was strong consensus among participants supporting the value of community-led norm-setting. However, they also acknowledged potential challenges—especially those related to the academic traditions of open-source sharing and the rapid pace of technological change. Several noted that academic research culture places a high value on transparency and open dissemination of tools and findings. This tradition could conflict with efforts to restrict or manage access to potentially dangerous AIxBio capabilities. Participants suggested that one way to potentially reconcile some of these tensions would be to recognize that the open dissemination of tools is valued in academia because it brings benefits such as ease of access, validation, and maintenance. Managed access approaches might be able to provide these same benefits, offering many of the advantages of open access while providing enhanced security. Additionally, participants expressed concern that the speed of AI advancement might outpace the scientific community's ability to internally establish and enforce effective norms, potentially leaving dangerous vulnerabilities.

Several participants noted that the DNA synthesis industry provides a valuable model for how technical communities can shape effective norms and screening practices. They emphasized that motivations for this industry's forward-leaning security posture should extend beyond ethical considerations and include self-interest, particularly in reducing legal exposure and influencing future government regulation. Companies must recognize that if their products or services were used to develop a biological weapon, they could face significant legal liability, regulatory penalties, and reputational damage. Participants highlighted how DNA synthesis companies successfully established voluntary screening standards through organizations such as the International Gene Synthesis Consortium, which promotes guidance for customer and DNA sequence screening.

Participants also examined several potential courses of action to prevent intentional misuse of BDTs (*see Box 4*).

Following in-depth discussions, participants prioritized possible actions to prevent the misuse of BDTs. Key considerations included the potential effectiveness of each action, along with feasibility and how well such action balances security considerations with enabling scientific benefits.

MANAGED ACCESS approaches emerged as the most promising option with potential to control access to the most powerful AIxBio tools. Participants were particularly optimistic about this approach, rating it as moderately to highly effective, feasible to implement, and unlikely to constrain scientific progress, if properly implemented. Several participants emphasized that any managed access system must carefully balance security with equity concerns to ensure that researchers from all backgrounds and regions can access these technologies. Participants also stressed that transparency about the structure of the managed access framework and scientific community participation in its development would be essential, allowing the scientific community to inform, understand, and trust the decision-making process.

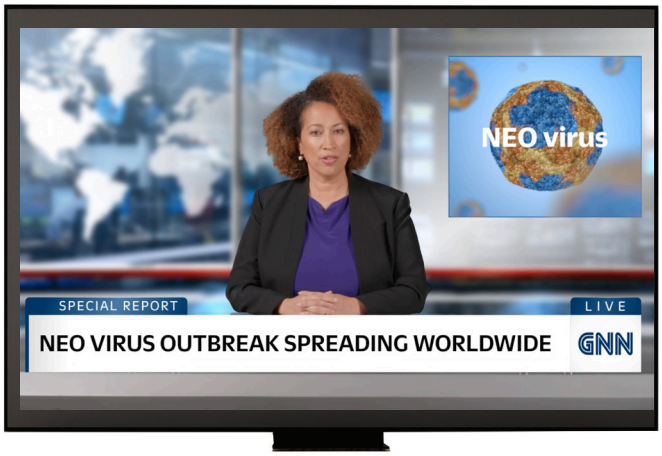
INCENTIVE-BASED APPROACHES also received support from participants. They were viewed as a way to promote responsible behavior without stifling innovation. Many participants noted that financial and regulatory incentives could be especially effective at the national level because governments have more direct leverage over research institutions and industry within their borders. Participants suggested that funding agencies could make compliance with biosecurity norms a prerequisite for grants, effectively aligning economic and professional interests with security goals.

BUILT-IN SCREENING MECHANISMS generated considerable discussion, with most participants seeing them as valuable but having significant limitations. Although participants rated their potential effectiveness as medium to high, they were more measured about the feasibility of their implementation. They assessed implementation as medium, noting the technical challenges involved in developing and deploying robust screening tools. Several participants suggested that current screening technologies remain immature and would need further development before implementation. Several participants were more optimistic; however, one bluntly stated that these tools currently "aren't very good."

BOX 4.

COURSES OF ACTION TO PREVENT MISUSE OF BDTS

- **CONTROLS ON DATA USED TO TRAIN AIXBIO MODELS:** Controlling access to pathogen-relevant biological datasets involves several safeguarding measures. These controls include access restrictions, licensing agreements, and technical safeguards to prevent sensitive data—such as genomic, protein, metabolic, or other biological information—from being used to train AI models that could be used to design dangerous biological agents. This control would apply to data currently not publicly available and/or data generated in the future. Such controls could include requiring researcher credentials, institutional review, and/or legitimate research justification before granting access to datasets that contain information about virulence factors, antibiotic resistance mechanisms, or pathogen transmission pathways. The goal is to balance scientific progress with biosecurity by ensuring that powerful BDTs cannot be clandestinely or accidentally trained on data that would enhance their capability to create harmful organisms or biological weapons.
- **BUILT-IN SCREENING MECHANISMS FOR BDTS:** These systems automatically evaluate the outputs of BDTs to determine if they match sequences, structures, or functions associated with dangerous pathogens or toxins. When potentially harmful designs are detected, the model can either refuse to provide the output or flag it for human review.
- **MANAGED ACCESS APPROACHES FOR BDTS:** This approach is a framework that controls who can use potentially dangerous biological design capabilities by requiring users to meet legitimacy criteria before gaining access, thereby reducing the potential for misuse while enabling beneficial scientific research. The approach uses tiered access levels based on the tool's risk profile—from simple registration for low-risk tools to extensive verification of institutional affiliation, scientific credentials, and project documentation for high-risk capabilities. This system balances biosecurity concerns with the need for equitable access, allowing verification that tools are used only for legitimate purposes while supporting the scientific community's ability to advance beneficial applications such as medical countermeasures.
- **PUNITIVE NATIONAL OR INTERNATIONAL MEASURES:** These measures are enforcement mechanisms that impose legal penalties, sanctions, or other consequences on individuals, organizations, or nations that develop or deploy AI-enabled biological weapons or misuse BDTs for harmful purposes. Such measures could include criminal prosecution, economic sanctions, export controls, or other punitive actions.
- **INCENTIVE-BASED NATIONAL OR INTERNATIONAL MEASURES:** These measures are positive inducements such as funding, tax incentives, research grants, or regulatory fast-tracking that reward individuals, organizations, or nations for implementing robust biosecurity measures, adhering to responsible development practices, or contributing to safety research. International assistance should be offered only to countries that demonstrate a commitment to peaceful research and development in adherence with international norms, standards, and best practices. Such measures aim to encourage voluntary compliance and proactive risk mitigation.
- **NORMATIVE APPROACHES:** These measures are voluntary standards and ethical guidelines (e.g., codes of conduct) developed by the AIxBio research community to establish shared expectations for responsible development and use of BDTs. These approaches rely on normative behaviors, professional reputation, and community self-governance rather than legal oversight and enforcement.



The exercise scenario features a rapidly expanding outbreak that spreads across borders.

NORMATIVE APPROACHES—such as codes of conduct—sparked debate about their real-world impact. Although participants acknowledged these measures would be relatively easy to implement, questions arose about whether they could meaningfully deter determined bad actors. Several participants warned that such approaches can become mere "security theater" (i.e., visible actions that create an illusion of security without addressing fundamental risks).

PUNITIVE MEASURES proved the most controversial, dividing participants sharply. Some argued for their deterrent value, while others questioned whether the international community could ever agree on enforcement mechanisms. The discussion revealed skepticism about the feasibility of coordinated punitive action, with some participants suggesting such measures might work only at the national level, where governments have clearer enforcement authority.

CONTROLS ON DATA required to train AIxBio models received the least support from participants. Overall, exercise participants debated the effectiveness of this course of action and viewed it as both difficult to implement and potentially damaging to scientific progress. Participants were divided on the effectiveness of data restrictions in constraining AI-enabled tools and systems from producing harmful outputs over the long term. Participants consistently rated its feasibility as low, pointing out that the vast amounts of biological data needed for training models are already widely available across countless public databases and research repositories. However, there was little discussion about privately held data or data that will be created in the future. Several participants emphasized that attempting to restrict access to fundamental scientific data would impede legitimate research that relies on large datasets to advance medical treatments and biotechnology. Consequently, most participants recommended rejecting this approach entirely or exploring it only in very limited contexts.

✓ FINDING 5

There is a need for an official forum at the international level for communication and coordination to assess and address AIxBio risks.

Participants highlighted the need for a dedicated international forum to identify AIxBio risks and governance solutions as a critical component of the global biosecurity architecture. Although existing instruments such as the BWC and UN Security Council Resolution 1540 provide frameworks for preventing deliberate misuse of biology, participants broadly agreed that these structures are ill-suited to handle the rapidly evolving nature of AIxBio capabilities.

The group aligned on the need for an international platform to facilitate communication and coordination on AIxBio risks and opportunities. However, participants preferred approaches that avoided creating new formal regimes or overburdening existing ones that lack appropriate expertise and agility. Participants envisioned this forum as serving multiple functions critical to managing emerging risks. They suggested it could analyze specific threats, forecast scenarios of greatest concern, and establish a shared understanding of potential dangers before they materialize. Participants also emphasized that the forum could facilitate discussions on risk thresholds and red lines (i.e., predetermined capability levels that signal escalating AI biological risks that should trigger immediate intervention). Several participants noted that such conversations are essential for developing shared international norms and best practices for responsible AIxBio development.

FINDING 6

Efforts to manage AI risks must take into account the benefits of AIxBio capabilities and avoid placing undue constraints on scientific benefits.

Exercise participants strongly emphasized that while addressing AIxBio risks, the international community must preserve the tremendous beneficial potential of these technologies. Participants highlighted multiple ways that AI could contribute to biosecurity as well as broader pandemic preparedness and response, including by accelerating the development of medical countermeasures, enhancing disease surveillance capabilities, and strengthening DNA synthesis screening mechanisms for dangerous pathogens. Several participants specifically noted that AI's capacity to process vast amounts of biological data could enable early detection of emerging threats by identifying subtle patterns or signals that might otherwise go unnoticed (*see Box 5*).

Given the significant beneficial potential of AIxBio capabilities for biosecurity and pandemic preparedness, exercise participants emphasized that any regulatory or governance measures should not only incorporate considerations about efficacy and feasibility but also avoid constraining beneficial scientific advances and innovation. Participants also raised concerns about equity in access to these technologies, warning that overly restrictive measures could exacerbate global disparities in scientific capabilities and pandemic preparedness.

Ultimately, participants concluded that effective management of AIxBio risks requires approaches that can simultaneously minimize threats while maximizing the technology's potential to enhance global health security and scientific progress.

BOX 5.

AI FOR ADVANCING BIOSECURITY AND PANDEMIC PREPAREDNESS

- **BIOSURVEILLANCE:** AI tools can enhance the detection and monitoring of biological threats by analyzing outbreak data, genomic sequences, and environmental samples, such as wastewater, to identify emerging pathogens and high-risk variants before they spread widely.
- **MEDICAL COUNTERMEASURES:** AI can accelerate the design and development of vaccines, antibodies, and antimicrobial treatments, potentially reducing development timelines from months to days or weeks by enabling rapid analysis of pathogen genomes and optimizing experimental designs and interpretation of results.
- **OUTBREAK RESPONSE LOGISTICS:** AI can optimize pandemic response by forecasting disease spread to inform policy decisions and hospital preparedness, while also designing efficient delivery routes for medical supplies and infrastructure.
- **INTELLIGENCE:** AI can help analyze patterns across supply chains, financial transactions, equipment purchases, and communications data that may indicate state or nonstate biological weapons development activities.

Recommendations

The authors developed the following recommendations based on key findings from the exercise discussions, and they do not necessarily reflect the views of the exercise participants.

Although the exercise offered a specific example of misuse of AIxBio capabilities, it is representative of a much broader array of potential AI-enabled biological threats that could emerge, making the insights gleaned from the exercise and the resulting recommendations relevant to managing a wider range of risks.

As technology rapidly advances at the intersection of AI and biotechnology, the world faces both remarkable opportunities and unprecedented risks. Global competition to develop increasingly powerful AI capabilities has intensified. Without a proactive approach to managing risk, this competitive environment could become dangerous, and trigger a race to the bottom for AI safety and security—especially for AIxBio capabilities. To prevent this outcome, the global community must commit to responsible innovation by prioritizing security alongside scientific advancement and establishing guardrails to manage risks while tapping AI's tremendous potential to improve global health security.

The following practical recommendations help meet the goal of advancing responsible AIxBio innovation while guarding against the risks of misuse.

Recommendation 1

National governments, industry, and philanthropic organizations should politically support and fund a comprehensive research and development agenda to establish effective guardrails for AIxBio technologies and applications.

- The research agenda should explore a series of technical guardrails—such as built-in screening mechanisms and managed-access frameworks—as well as governance mechanisms, including incentive-based policy measures and accountability frameworks. Research should also examine how to implement guardrails while still supporting equitable access for researchers, recognizing that security and equity are not competing objectives.
- The research agenda should account for the rapid evolution of AI capabilities through systematic risk assessments and horizon scanning. Risk assessments should evaluate the potential for misuse of current and near-term AIxBio capabilities and regularly evaluate the effectiveness of existing safeguards against evolving threats. Horizon scanning should track emerging AI developments, and developments in adjacent fields, which are likely to dramatically change AIxBio capabilities in the next two to five years.
- Government research funding agencies and philanthropic organizations should support innovation in AIxBio safety and security, providing mechanisms for translating successful approaches into widely adopted practices. Government incentives could include grant programs, advance market commitments, tax credits for safety research investments, and preferential treatment in procurement processes.

Recommendation 2

National governments should establish institutes focused on AI safety and security, whose missions include safeguarding AIxBio capabilities.

- Governments with AI investments or a domestic AI industry should create institutes focused on AI safety and security—building on commitments initially made by 10 nations plus the European Union at the 2024 AI Seoul Summit—and their mission should include safeguarding AIxBio capabilities. Some countries have established AI safety or security institutes, but the structures can vary. Additional nations should establish these institutes, and they should integrate biosecurity expertise with AI safety competencies.
- Government organizations charged with AI safety and security should take the lead in organizing and stewarding the research agenda outlined in Recommendation 1. These bodies should function in a hub-and-spoke model, drawing on a range of technical experts within and outside the government. They should facilitate public-private cooperation, innovation in AIxBio safety, and agility in exploring and developing novel governance approaches. Guidance or recommendations for industry can be based on analysis by government AI safety organizations, which can also inform recommendations for government guidelines, incentives, and regulations.
- Institutes focused on AI safety and security also should serve as technical evaluation authorities for industry-proposed guardrails, conducting rigorous testing that is further informed by threat intelligence and threat modeling. Independent evaluation provides industry with credible validation of its safety measures while offering governments assurance that voluntary standards meet necessary security thresholds, potentially reducing the need for restrictive regulations.

Recommendation 3

International partners should collaborate via a global platform to develop and disseminate best practices for AIxBio safeguards.

- This global platform should facilitate international dialogue on AIxBio risks, responsible innovation, and application of AIxBio safeguards that balance security needs with equitable access to beneficial technologies. This collaborative approach among AI model developers, life science researchers, security experts, and policymakers can build trust in best practices and increase the likelihood that they will be adopted.
- National institutes charged with AI safety and security should actively participate in those platforms to ensure alignment between technical expertise and practical implementation of safeguards. Participation provides these institutes with valuable access to information and insights from the broader international expert community outside of government.
- Drawing inspiration from the DNA synthesis industry's self-governance efforts, the platform should engage an international group of experts from industry and the academic research community to explore opportunities for proactive governance that balances openness and scientific innovation with security.
- Initiatives such as the AIxBio Global Forum, established by NTI | bio, bring together a wide range of stakeholders, which include international experts and policymakers, with the goal of developing shared norms, practices, and standards. Building greater international support for this forum could help develop a shared understanding of biosecurity risks associated with AI. It also could support cooperative efforts to develop and share tools and practices to protect the beneficial application of AIxBio capabilities while guarding against risks. Further, it could encourage adoption of national and global governance mechanisms to manage risks.

Recommendation 4

Global scientific and national security communities should actively leverage AI's beneficial applications in biosecurity and pandemic preparedness.

- National and international biosurveillance missions should leverage AI tools to enhance capabilities and enable rapid detection and attribution of disease outbreaks, including those of unknown or suspicious origin. Such systems may be able to quickly analyze genetic data to identify engineered pathogens while also monitoring global health data for early warning signs of biological threats.
- Research institutions and pharmaceutical companies should leverage AI to strengthen biological defenses by accelerating development of vaccines and therapeutics. AI can design more effective triggers for the immune system—which is important for vaccine development—and predict successful drug candidates before costly clinical trials, enabling rapid responses to emerging threats. Faster and more accurate development of medical countermeasures can reduce the appeal of biological weapons development by helping to ensure threats are more quickly detected and contained (i.e., successful development can act as a deterrent).
- Intelligence and security communities should explore the use of AI tools to identify and disrupt malicious actors attempting to develop or disseminate biological weapons. This includes analyzing patterns across supply chains, financial transactions, equipment purchases, and communications data that may indicate biological weapons programs, enabling early interdiction before threats materialize.

Appendix

EXERCISE SCENARIO EPIDEMIOLOGICAL MODEL

The exercise scenario was modeled using a compartmental model based on ordinary differential equations. The outbreak began with index cases in the fictional country of Ankovia, followed by local domestic transmission and international spread via passenger airline flights. The model is initiated after infections have been seeded in countries worldwide, with neo-enterovirus disease (NVD) spread in each of the six World Health Organization (WHO) regions being modeled separately.[1] All modeling was completed using the R software package.[2] The model structure is shown in Figure A–1, with the primary scenario model parameters in Table A–4.

The disease and treatment scenario parameters (Tables A–1 and A–2) were primarily derived using empirical data from outbreaks of enterovirus D68 (EV-D68), which is the parent species from which the neo-enterovirus was engineered. Data on the efficacy and implementation of nonpharmaceutical interventions (NPIs), such as social distancing and masking, from the COVID-19 pandemic were also used to derive NPI parameters. The basic reproduction number (R0) was selected based on the median peak time-varying reproduction numbers (Rt) of 2.1–2.7 reported for 2022 EV-D68 outbreaks in Canada and the United States.[3] The R0 is subsequently reduced by 40 percent at day 30 in the model due to the implementation of NPIs, which were assumed to be similarly effective at preventing infection as during the COVID-19 pandemic, given that both viruses are primarily transmitted via respiratory droplets.[4] The incubation period was 4 days and the infectious period length was 10 days, based on EV-D68 outbreak data and published clinical guidelines.[5] The rate of development of severe acute flaccid myelitis (AFM) requiring mechanical ventilation to prevent respiratory failure and death was 10 percent, which is approximately 200–400 times greater than the rate of respiratory failure from poliomyelitis.[6]

While the natural strain of EV-D68 primarily infects young children and those who are immunocompromised, the scenario assumed that all age and sex groups were equally susceptible to infection with the neo-enterovirus and the population had no background immunity. Similar to EV-D68, most infections were asymptomatic or caused mild illness, and these infected, nonparalyzed individuals were the primary drivers of disease spread during their 10-day contagious period. In contrast, the scenario presumed that severely paralyzed individuals (10 percent of infections) were less infectious following paralysis, as they were presumed to no longer be ambulatory and thus had fewer community contacts.

The model assumed that no medical countermeasures were effective at preventing or treating NVD until the introduction of a vaccine at day 400. Asymptomatic and mild cases did not require treatment, and 100 percent of infections in this category were assumed to recover without intervention. For cases that developed severe AFM leading to respiratory failure, the scenario parameters assumed that only 90 percent presented for treatment, which accounts for unattended deaths prior to hospitalization and inefficient ventilator allocation. The recovery rate for those not treated with mechanical ventilation was 0 percent (i.e., the fatality rate was 100 percent), which could be because either individuals did not seek treatment or no ventilators were available because hospital treatment capacity was overwhelmed. For cases with severe AFM that were treated with a ventilator, the duration of ventilation was 28 days, drawn from a study that reported the median duration of intubation in a small cohort of children with EV-D68-associated AFM.[7] The efficacy of mechanical ventilation at preventing death was 95 percent to account for additional deaths due to ventilator-associated

pneumonia, which frequently develops in patients ventilated for more than two days.[8] To calculate treatment capacity (*see Table A-3*), the estimated number of ventilators in each WHO region was based on estimates of per capita intensive care unit (ICU) beds.[9] Although ICU bed capacity is typically estimated as higher than ventilator capacity, the scenario assumed capacity would quickly scale to at least match available ICU beds.

A single-dose vaccine was introduced at day 400 of the model, and it was assumed to be 100 percent effective at preventing neo-enterovirus infection with no waning immunity during the time period modeled. The global vaccination rate was modeled as 4 million daily doses, which is close to the peak observed for vaccine distribution during the COVID-19 pandemic.[10] However, the effects of the pandemic were already catastrophic by the time of vaccine initiation when the scenario ends, with almost 860 million total cases and approximately 60 million deaths.

TABLE A–1. Neo-enterovirus Disease Parameters and Their Values

Parameter	Definition	Value	Source
R-naught (R0)	Basic reproduction number, or the average number of individuals that each infected individual will infect	2.4	3
Nonpharmaceutical intervention (NPI) strength	Reduction in R0 due to NPIs—1 implies no effect, 0 is perfect protection, and 0.6 implies 40% of cases are eliminated	0.6	4, 5
NPI initiation	Reduction in cases due to NPIs occurs at this time	30 days	4
Incubation period	Time between exposure and disease onset	4 days	6
Contagious period	Contagious period following disease onset	10 days	6
Severe acute flaccid myelitis (AFM) incidence	Incidence of severe AFM development, leading to respiratory failure and requiring mechanical ventilation	0.1	Scenario

TABLE A–2. Neo-enterovirus Treatment Parameters and Their Values

Parameter	Definition	Value	Source
Proportion presenting for treatment	Proportion of population requiring mechanical ventilation presenting for treatment, accounting for inefficient ventilator allocation and unattended deaths	0.9	Scenario
Recovered probability	Reduction in R0 due to NPIs — 1 implies no effect, 0 is perfect protection, and 0.6 implies 40% of cases are eliminated	0.6	4, 5
(no ventilator required)	All patients who do not develop acute flaccid myelitis (AFM) survive	1.0	Scenario
Recovered probability	Time between exposure and disease onset	4 days	6
(ventilator required/ untreated)	All patients who develop severe AFM requiring mechanical ventilation and do not receive a ventilator die	0.0	Scenario
Recovered probability	Incidence of severe AFM development, leading to respiratory failure and requiring mechanical ventilation	0.1	Scenario
(ventilator required/ treated)	Accounts for deaths from ventilator-associated pneumonia	0.95	9, 10
Time on ventilator	Patient time on ventilator before recuperation or death	28 days	8
Vaccine start date	Time in model for global vaccination initiation	400 days	Scenario
Vaccine distribution	Global vaccination rate	4,000,000 per day	Scenario
Vaccine efficacy	Efficacy of single-dose vaccination at preventing severe AFM requiring mechanical ventilation	1.0	Scenario

TABLE A–3. WHO Regions, Population Totals, and Additional Treatment Parameters and Their Values

Region	Region Name	Population Total	Estimated Number of Ventilators
Region 1	African Region (AFR)	1,162,658,000	3.1/100,000 people (36,042 total)
Region 2	Region of the Americas (AMR)	1,029,510,000	21.5/100,000 people (220,830 total)
Region 3	South-East Asian Region (SEAR)	2,056,473,000	2.4/100,000 people (50,041 total)
Region 4	European Region (EUR)	930,809,000	13.1/100,000 people (122,108 total)
Region 5	Eastern Mediterranean Region (EMR)	766,542,000	10.9/100,000 people (83,361 total)
Region 6	Western Pacific Region (WPR)	1,932,809,000	7.5/100,000 people (145,844 total)

FIGURE A-1. Base Compartmental Model Used for All Six WHO Regions

Compartments are represented as Susceptible (S), Exposed (E), Infectious (I), Paralyzed (P), Ventilated (Vt), Vaccinated (Vx), Recovered (R), and Deceased (D). The force of infection (λ) is shown within the dotted square equation, with N representing the population size. The remaining parameters are described in Table A-4. Cumulative cases are the sum of all individuals in the exposed, infected, paralyzed, ventilated, recovered, and deceased compartments, while cumulative deaths are the total population in the deceased compartment.

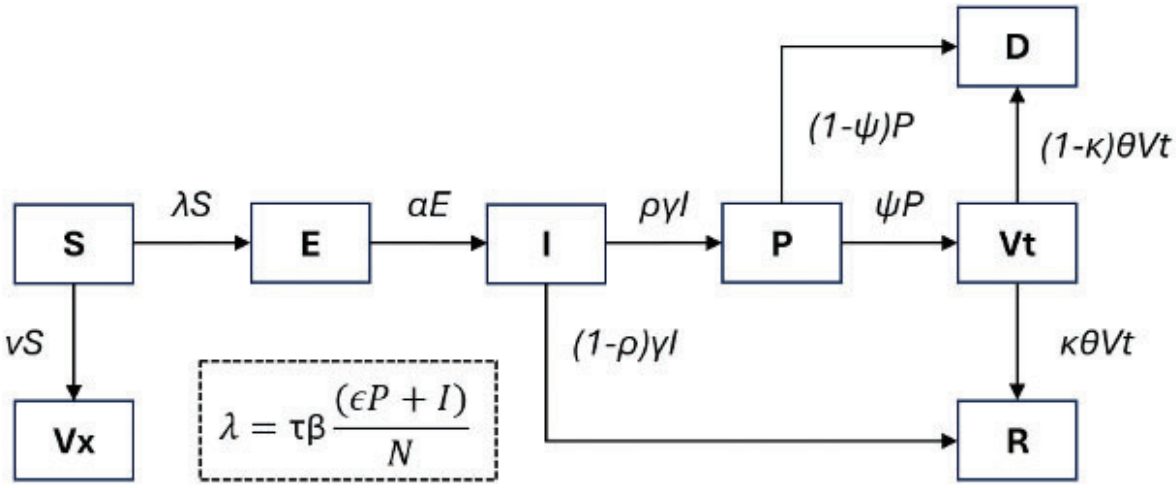


TABLE A-4. Scenario Model Parameters and Their Values

Parameter	Definition	Value	Source
β	Base transmission rate at T = 0, based on an R0 of 2.4 and contagious period of 10 days	0.24	3
τ	Reduction in R0 due to nonpharmaceutical interventions—1 implies no effect, 0 is perfect protection, and 0.6 implies 40% of cases are eliminated	0.6	4, 5
α	Rate of progression from exposed compartment, based on an incubation period of 4 days	0.25	6
γ	Rate of progression to recovered compartment for non-AFM cases, based on an infectious period of 10 days—equivalent to the rate of progression to AFM development for severe AFM cases	0.1	6
δ	Rate of progression to the recovered or deceased compartments for severe AFM cases that receive mechanical ventilation, based on a treatment time of 28 days	0.0357	8
κ	Survival probability for severe AFM cases that receive mechanical ventilation, accounting for deaths from ventilator-associated pneumonia	0.95	9, 10
ρ	Incidence of AFM development requiring mechanical ventilation	0.1	Scenario
ψ	Probability of receiving treatment, accounting for inefficient ventilator allocation and unattended deaths	0.9	Scenario
ϵ	Relative infectiousness of cases with severe AFM	0.25	Scenario
ν	Global vaccination rate	4,000,000 per day	Scenario

APPENDIX REFERENCES

[1.] WHO Regional Offices, World Health Organization (WHO) (website), accessed June 1, 2025, https://www.who.int/about/who-we-are/regional-offices.

[2.] "R: A Language and Environment for Statistical Computing," Version 4.5.1, The R Core Team, June 13, 2025, https://www.R-project.org/.

[3.] Martin Grunnill et al., "Inferring Enterovirus D68 Transmission Dynamics from the Genomic Data of Two 2022 North American Outbreaks," *npj Viruses* 2, no. 34 (2024), doi:10.1038/s44298-024-00047-z.

[4.] You Li et al., "The Temporal Association of Introducing and Lifting Non-pharmaceutical Interventions with the Time-Varying Reproduction Number (R) of SARS-CoV-2: A Modelling Study across 131 Countries," *The Lancet* 21, no. 2 (2021): 193–202, doi:10.1016/s1473-3099(20)30785-4; and Jeremy Howard et al., "An Evidence Review of Face Masks against COVID-19," *PNAS* 118, no. 4 (2021), doi:10.1073/pnas.2014564118.

[5.] Valeria Fabre, "Enterovirus," Johns Hopkins Medicine ABX Guide, accessed June 1, 2025, https://www.hopkinsguides.com/hopkins/view/Johns_Hopkins_ABX_Guide/540204/all/Enterovirus.

[6.] "Poliomyelitis," Fact sheet, World Health Organization (WHO), October 22, 2024, updated April 2, 2025, https://www.who.int/news-room/fact-sheets/detail/poliomyelitis.

[7.] Jelte Helfferich et al., "Acute Flaccid Myelitis and Guillain-Barré Syndrome in Children: A Comparative Study with Evaluation of Diagnostic Criteria," *European Journal of Neurology* 29, no. 2 (2022): 593–604, doi:10.1111/ene.15170.

[8.] Anita Rae Modi and Christopher S. Kovacs, "Hospital-Acquired and Ventilator-Associated Pneumonia: Diagnosis, Management, and Prevention," *Cleveland Clinic Journal of Medicine* 87, no. 10 (2020): 633–39, doi:10.3949/ccjm.87a.19117; and Laurent Papazian, Michael Klompas, and Charles-Edouard Luyt, "Ventilator-Associated Pneumonia in Adults: A Narrative Review," *Intensive Care Medicine* 46, no. 5 (2020): 888–906, doi:10.1007/s00134-020-05980-0.

[9.] "ICU Beds per Capita by Country 2024," World Population Review, accessed December 1, 2025, https://worldpopulationreview.com/country-rankings/icu-beds-per-capita-by-country; Jessica Craig, Erta Kalanxhi, and Stephanie Hauck, "National Estimates of Critical Care Capacity in 54 African Countries," preprint, submitted May 16, 2020, doi:10.1101/2020.05.13.20100727; Arooj Jalal et al., "Health Workforce Capacity of Intensive Care Units in the Eastern Mediterranean Region," *PLoS ONE* 18, no 6 (2023): e0286980, doi:10.1371/journal.pone.0286980; and Richard D. Branson and Dario Rodriquez Jr., "COVID-19 Lessons Learned: Response to the Anticipated Ventilator Shortage," *Respiratory Care* 68, no. 1 (2023): 129–50, doi:10.4187/respcare.10676.

[10.] "Coronavirus (COVID-19) Vaccinations," Our World in Data, accessed June 1, 2025, https://ourworldindata.org/covid-vaccinations.

About the Authors

Hayley Anne Severance, MPH

Deputy Vice President, Global Biological Policy and Programs, NTI

Ms. Hayley Anne Severance joined NTI May 2018. As deputy vice president, she supports and leads the team's efforts to reduce biological risks that imperil humanity. She previously served as a senior policy advisor in the U.S. Office of the Deputy Assistant Secretary of Defense for Countering Weapons of Mass Destruction, where she developed strategic policy guidance for the Cooperative Threat Reduction's Cooperative Biological Engagement Program (CBEP) and led the Department of Defense's efforts to advance the U.S. commitment under the Global Health Security Agenda. Severance holds an MPH in infectious disease epidemiology from the School of Public Health and Health Services at George Washington University and a BS in public health from the Edward J. Bloustein School of Planning and Public Policy at Rutgers University.

Kevin P. O'Prey, PhD

Managing Partner, The Palisades Group LLC

Dr. Kevin P. O'Prey has served as the facilitator for the annual Nuclear Threat Initiative's biosecurity tabletop exercises at the Munich Security Conference. As managing partner at the Palisades Group, O'Prey oversees analytical and facilitation projects for the U.S. government, private sector, and international organizations. Previously, he was cofounder and president of Obsidian Analysis Inc. and president of DFI Government Services. He earned his PhD in political science at MIT's Security Studies Program.

Nikki Teran, PhD

Managing Member, Emerging Technology Solutions LLC

Dr. Nikki Teran serves as a consultant to NTI | bio on issues at the intersection of artificial intelligence and biosecurity. As managing member of Emerging Technology Solutions LLC, she provides strategic consulting on biosecurity risk assessment, AI safety systems, and policy development. Previously, she served as senior biosecurity fellow at the Institute for Progress, where she led policy development on pandemic preparedness and secured congressional funding for far-UVC research. She has also held research and policy positions with SecureBio, Blueprint Biosecurity, and the National Academies' Committee on International Security and Arms Control. Teran holds a PhD in genetics from Stanford University and a BS in molecular biophysics and biochemistry from Yale University.

Jaime M. Yassif, PhD

Vice President, Global Biological Policy and Programs, NTI

Dr. Jaime Yassif has more than 20 years of experience working at the interface of science, technology, public health, and international security in government and civil society. As NTI vice president for Global Biological Policy and Programs, she oversees the organization's work to reduce catastrophic biological risks, strengthen biosecurity and pandemic preparedness, and drive progress in advancing global health security. She previously served as a program officer at Open Philanthropy, where she led the Biosecurity and Pandemic Preparedness initiative, recommending and managing approximately $40 million in biosecurity grants, which rebuilt the field and supported work in several key areas. Before this, Yassif served as a science and technology policy advisor at the U.S. Department of Defense and worked on the Global Health Security Agenda at the U.S. Department of Health and Human Services. She holds a PhD in biophysics from the University of California, Berkeley, an MA in science and security from the King's College London Department of War Studies, and a BA in biology from Swarthmore College.

BUILDING A SAFER WORLD

1776 EYE STREET, NW, SUITE 1000

WASHINGTON, DC 20006

(202) 296–4810

WWW.NTI.ORG

NTI.ORG

NTI_WMD

NTI_WMD

NUCLEAR THREAT INITIATIVE