



Lawrence Livermore National Laboratory 

# Biosecurity 2026: New Challenges, New Opportunities?

## Annotated Bibliography

**March 18-19, 2026**



## Annotated Bibliography

### Biosecurity 2026: New Challenges, New Opportunities?

Center for Global Security Research  
Livermore, California, March 18-19, 2026

Prepared By: Monica Graham, Leo Keay, Lesley Kucharski, Celine Lee,  
and Phoebe Pham<sup>1</sup>

#### Key Questions:

- What are the main challenges to biosecurity?
- How does technological change contribute to the problem and the solutions?
- Where do we stand today in meeting these challenges?
- How can strategies to mitigate or eliminate threats or risks be strengthened in the context of fewer resources and authorities?
- How can essential partnerships be strengthened?

#### Panel Topics:

1. Calibrating the Threats Posed by State Adversaries
2. Calibrating the Threats Posed by Bioterrorists
3. Calibrating the Risks of Outbreaks
4. Tracking the Changing Strategy and Policy Context
5. Understanding the Twin Impacts of S&T Competition
6. Embracing Opportunity
7. Aligning Public Health Preparedness with National Security Preparedness
8. Aligning Public and Private Sector Capabilities and Capacities
9. Ensuring Essential International Partnerships

---

<sup>1</sup> The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.



## Panel 1: Calibrating the Threats Posed by State Adversaries

- What biothreats does the United States face from state adversaries?
- Has it changed in recent years? If so, why?

Robert P. Kadlec, “A Critical Review of Covid-19 Origins: ‘Hidden in Plain Sight,’” Muddy Waters Update: Second Installment, Scowcroft Institute of International Affairs, Texas A&M University (July 2025). <https://bush.tamu.edu/wp-content/uploads/2025/07/A-Critical-Review-of-COVID-19-Origins.pdf>.

In this second and final report in a series examining the origins of Covid-19, Robert Kadlec highlights how high-containment lab work—especially when tied to military or state priorities—can generate strategic harm even without an intentional attack. Focusing on Covid-19, he argues that the pandemic began with a lab escape rather than a natural animal spillover event, emphasizing that it should be understood as a state-linked biosafety and accountability risk rather than “just” a public-health accident. He also highlights the role of China’s People’s Liberation Army (PLA) in pursuing coronavirus-related vaccine research, particularly in relation to its interest in the neurocognitive effects of pathogens. Kadlec’s main conclusion is that the spread of high-containment labs and opaque state-linked biological research should be treated as a security problem that can produce mass consequences, not only as a medical or scientific issue, making prevention, early detection, and stronger biosafety standards more urgent than in prior decades.

Glenn A. Cross and Seth Carus, “Is a biological weapons arms race on the horizon: impact of scientific advances and strategic competition?” *Frontiers in Political Science* 7 (October 2025). <https://doi.org/10.3389/fpos.2025.1675963>.

Glenn Cross and Seth Carus seek to counter alarmist interpretations of the state-based biosecurity threat, arguing that advances in biotechnology do not automatically translate into new national bioweapons programs. The authors conclude that fears of a near-term biological weapons arms race are overstated, highlighting how states have historically struggled to find operationally effective military applications for bioweapons, as well as flagging the political costs of being associated with them. Acknowledging the U.S. government’s unease about Russia’s and North Korea’s pursuit of offensive biological weapons programs, as well as its compliance concerns around Iran and China, the article frames the threat in terms of “persistent problem actors,” rather than a universal rush to build bioweapons. The authors also acknowledge that new technologies, including AI, can lower some barriers, but argue the biggest practical bottlenecks still sit in real-world testing and delivery. They conclude by highlighting the need to prioritize intelligence and defenses against a limited set of capable and motivated states, rather than preparing for a bioweapons arms race.

Al Mauroni and Glen Cross, “Will China Force a Rethink of Biological Warfare?” *War on the Rocks* (June 2025). <https://warontherocks.com/2025/06/will-china-force-a-rethink-of-biological-warfare/>.



Al Mauroni and Glen Cross argue that the state-adversary biological threat from China is more operationally serious than Cold-War era “spray-a-city” antecedents because advances in biotechnology and AI enable Beijing to develop more tailored, conflict-relevant options. While open sources do not prove an active offensive program today, extensive Chinese dual-use research activity could be shifted toward weaponization if Chinese national leaders so chose. The article highlights how the growing integration of China’s civilian biotechnology base with the PLA could enable Beijing to mobilize civilian capacity quickly, as well as how China’s position as a major nuclear power makes threats of U.S. retaliation against bioweapon employment less credible in a fast-moving regional war. Their main takeaways are that Washington should assume Beijing could use limited or novel biological effects during a regional crisis, and that it should update concepts, planning, and protection accordingly.

## Panel 2: Calibrating the Threats Posed by Bioterrorists

- Does the United States face a bioterrorism threat? Why? What kind?
- Does it also face a risk of the criminal use of bio-agents?

Dan Scherr and Tanya M. Scherr, “Agroterrorism: A persistent but overlooked threat,” *Domestic Preparedness* (March 2025). <https://www.domesticpreparedness.com/articles/agroterrorism-a-persistent-but-overlooked-threat/>.

Agroterrorism is the deliberate introduction of animal or plant diseases for the purpose of generating fear, causing economic losses, or undermining social stability. Scherr and Scherr discuss that an agroterror attack against U.S. food or agriculture sectors can cause significant public health crises, economic losses, social panic, and break down of food supply chains. Leading agroterror threats to the United States are pests, contamination, pathogens, and cybersecurity attacks, with intentional spread of foot-and-mouth disease named the most dangerous. Major vulnerabilities include insufficient security and surveillance, and the overall lack of attention to biosecurity threats to the food and agriculture sectors. Significant cross-sector participation is needed to prevent agroterror events, particularly between government entities and the private sector. The authors highlight U.S. participation in international agriculture outbreak alert and response networks as a vital component of monitoring and responding to potential agroterror threats.

Ali Abbas Ahmadi, “Chinese nationals accused of smuggling ‘dangerous biological pathogen’ into US,” *BBC News* (June 4, 2025). <https://www.bbc.com/news/articles/c4gkdpymk4o>.

In 2025, two Chinese foreign nationals, Yunqing Jian and Zunyong Liu, were accused of attempting to smuggle *Fusarium graminearum* fungus into the United States. *Fusarium graminearum* is described in scientific literature as a potential agent of agroterrorism, which can kill off crops and cause vomiting and liver damage if consumed via contaminated food. Mr. Liu claimed he attempted to smuggle the fungus into the United States for study at a University of Michigan laboratory where his girlfriend, Yunqing Jian, worked. U.S. officials



described the allegations as a grave concern of national security, but Chinese officials have claimed no nefarious action or association with the case.

Abi Olvera, “The Cyber-Biosecurity Nexus: Key Risks and Recommendations for the United States,” Council on Strategic Risks (September 2023).

<https://councilonstrategicrisks.org/2023/09/14/the-cyber-biosecurity-nexus-key-risks-and-recommendations-for-the-united-states/>.

Cyber security risks across biology-relevant sectors in the United States have increased in recent years—which the author refers to as “cyberbiosecurity.” While technology integration into healthcare, food, agriculture, and biology sciences sectors has provided automation and production advances, sufficient cybersecurity has not kept pace with threats. Olvera explains that the largest cyberbiosecurity vulnerabilities are network security and data security for these sectors, citing several real-life examples to support this assertion. Most examples of misuse of biological materials Olvera cites are controlled, researched-based scenarios. To improve U.S. cyberbiosecurity, Olvera recommends passage of federal legislation that strengthens healthcare data privacy and cybersecurity through cooperation between the Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Department of Health and Human Services (HHS). The federal government should designate bioeconomy sectors, like food and agriculture, as critical infrastructure to allow increased access to cybersecurity funding and protection. Federally funded and non-federally funded biolabs should be required to follow federal cybersecurity regulation frameworks to tighten security of biological materials and data. Finally, Olvera states that more responsibility needs to be shifted to software providers to build increased cybersecurity protections into the software and hardware used in biology-relevant sectors.

Derrick Tin, Pardis Sabeti, and Gregory R. Ciottone, “Bioterrorism: An analysis of biological agents used in terrorist events,” *The American Journal of Emergency Medicine* 54 (April 2022), pp. 117-121. <https://doi.org/10.1016/j.ajem.2022.01.056>.

Rapid progress in synthetic biology, microbiology, and biological data connectivity contribute to increased risks of bioterrorism attacks. In this study, Tin et al. sought to create an epidemiological description of all terrorism-related attacks using biological agents between 1970-2019, with the goal to provide insights into potential future bioterror attacks. Using the Global Terrorism Database, they found that a total of 33 bioterrorism attacks were recorded between 1970 and 2019, resulting in 9 deaths and 806 injuries. The most common target of these attacks were government institutions and workers. Anthrax was the most commonly used biological agent, used in 20 attacks, and it accounted for the highest proportion of deaths caused by bioterror attacks. Salmonella was the second most commonly used agent and accounted for the highest proportion of injuries caused by bioterror attacks. Interestingly, almost one-third of all recorded bioterrorism events occurred in the U.S. in 2001 during the “Amerithrax” attacks. The authors found that bioterrorism was extremely rare, making up only 0.02% of all known terror attacks. The authors note the increased casualty risk of bioweapons over conventional weapons and the likelihood of bioattacks going unreported due to their “surreptitious” nature.



### Panel 3: Calibrating the Risks of Outbreaks

- Another pandemic? Naturally-occurring or accidental release?
- Against targeted populations?

Nita K. Madhav, Ben Oppenheim, Nicole Stephenson, Rinette Badker, Dean T. Jamison, Cathine Lam, and Amanda Meadows, “Estimated Future Mortality from Pathogens of Epidemic and Pandemic Potential” Chapter 2 in *Investing in Pandemic Prevention, Preparedness, and Response: Volume 2, Fourth Edition* (Eds. Siddhanth Sharma et al.), World Bank Group (2025), pp. 33-71. <https://documents1.worldbank.org/curated/en/099301511192520131/pdf/IDU-8282e225-6f71-444f-aa42-053d8f969f1b.pdf>.

The authors—a team from Ginko Bioworks and the University of California, San Francisco—argue that a Covid-19 level pandemic is not a “once in a century” event. Over the next 25 years, the probability of occurrence is roughly 50% for influenza and novel coronavirus pandemics, as well as Ebola and Marburg epidemics, judging from computational epidemiology and extreme events modeling simulations. The authors conclude that these estimates and risk modeling tools can help policymakers overcome challenges—such as uncertainty about the scale and timing of future pandemics, recency bias, and over-calibrating historical experience—to developing and prioritizing prevention, mitigation, and response strategies and plans.

Angela Fanelli, Alessandro Cescatti, Juan-Carlos Ciscar, Gregoire Dubois, Dolores Ibarreta, Rachel Lowe, Nicola Riccetti, Marine Robuchon, Ilaria Capua, Wojtek Szewczyk, and Emanuele Massaro, “Assessing the risk of diseases with epidemic and pandemic potential in a changing world,” *Science Advances* 11, iss. 30 (2025). <https://www.science.org/doi/10.1126/sciadv.adw6363>.

How do different human activities impact the emergence of epidemic and pandemic zoonotic pathogens? To answer this question, Fanelli et al. utilized predictive modeling to investigate relationships between World Health Organization (WHO) priority diseases and human-induced drivers of outbreak risk. Climate factors were identified as key drivers of increased outbreak risk, including increased annual temperatures and increased annual precipitation. Environmental factors, such as livestock density and land-use change, have more complex impacts on outbreak risk. The authors highlighted that population density is the strongest driver for outbreak risk, outweighing the contributions of all other drivers. The authors developed an epidemic risk index to measure a country's capacity to respond to a zoonotic outbreak, but they warn this model should be interpreted with caution due to the self-reported nature of the data used to create this model. Overall, the authors demonstrate a foundation for using predictive modeling for assessing the risks human activities place on zoonotic outbreaks.

Jennifer Nuzzo, “To Stop a Pandemic: A Better Approach to Global Health Security,” *Foreign Affairs* 100, iss. 1 (2021), pp. 36-43. <https://www.jstor.org/stable/26985863>.

Jennifer Nuzzo argues that much of the global health infrastructure is built to respond to outbreaks with limited geographic spread, and that preparing for the next pandemic will



require fundamental changes in how countries think about global health security. The ineffective global response to Covid-19 exposed interdependent factors that made the world unprepared for such a pandemic. These factors included: the absence of a global outbreak surveillance system; inadequately prepared global health systems; delayed declarations and education from the WHO; the absence of an enforcement mechanism within the WHO; and insufficient incentives for governments to report detected cases of Covid-19. Nuzzo explains the cross-sector cooperation needed to improve global pandemic preparedness. A top priority is an ongoing global surveillance network for tracking emerging pathogens, with standardized methods and centralized efforts for government and nongovernmental organizations to report surveillance data. Centralized global funding needs to be put towards building proactive capacities to improve global health responses to outbreaks of novel pathogens. Importantly, the WHO and its agencies need enforcement mechanisms for trade and travel restrictions upon reports of an outbreak that do not negatively penalize reporting countries.

Juan S. Izquierdo-Condoy et al., “Beyond the acute phase: a comprehensive literature review of long-term sequelae resulting from infectious diseases,” *Frontiers in Cellular Infection and Microbiology* 14 (2024). <https://doi.org/10.3389/fcimb.2024.1293782>.

Long-Covid has brought renewed attention to post-infection “sequelae,” or health conditions that persist after infection has resolved with varying effects on quality of life. In this review, Izquierdo-Condoy et al. identified 274 unique sequelae caused by approximately 82 unique pathogens, including pandemic-potential pathogens. Sequelae range from mild to life-threatening, with approximately one-third of cases causing disabling conditions. Treatment of acute infection can burden healthcare systems, and treating sequelae increases healthcare costs long after acute infection has ended. The authors propose that long-term effects of sequelae are not an extension of initial infection, but a new phase of illness that demands attention and resources to combat. Public health efforts that bolster baseline population health, like vaccinations, are critical to prevent health consequences of sequelae. The authors conclude that significant investment, research, and vigilance are needed to understand and mitigate post-infection sequelae.

## Panel 4: Tracking the Changing Strategy and Policy Context

- How has the Trump administration framed these challenges?
- How has it adapted U.S. strategy and policy?
- What challenges lie ahead?

Max Kozlov, Jeff Tollefson, Dan Garisto, Kim Albrecht, “Lost Science: U.S. science after a year of Trump,” *Nature* (20 January 2026), <https://www.nature.com/immersive/d41586-026-00088-9/index.html>.

The authors provide visual analysis of the historic cuts to U.S. science and its workforce made by the Trump administration in its first year since returning to the White House in 2025. The visuals illustrate unprecedented cuts particularly to the National Institutes of



Health (NIH), which is the largest global funder of biomedical research. They also indicate that the funding cuts and freezes to biological research targeted specific topics, including misinformation, vaccine hesitancy, infectious diseases, under-represented communities, clinical trials, as well as research and infrastructure at cancer centers.

In 2025, the Trump administration took several actions related to biosecurity strategy and policy. Listed from newest to oldest, these actions include:

1. Bobby McMillin, Daniel A. Kracov, Ronald D. Lee, Kristin M. Hicks, Pari R. Mody, Claire W. Dennis, and Katherine Rohde, “The BIOSECURE Act Becomes Law in the United States: A New Era of Restrictions on Global Biotech Equipment and Service Providers,” Advisory, Arnold & Porter (December 23, 2025). <https://www.arnoldporter.com/en/perspectives/advisories/2025/12/the-biosecure-act-becomes-law-in-the-united-states>.

Legal experts from the Arnold & Porter law firm provide an overview of the BIOSECURE Act, which was signed into law as part of the FY26 National Defense Authorization Act (NDAA). The Act prohibits the federal government from procuring biotechnology equipment or services from providers that are designated by the Director of the Office of Management and Budget (OMB) as “biotechnology companies of concern (BCCs).” It similarly prohibits the federal government from entering into a contract with any entity that uses biotechnology equipment or services from BCCs. Arnold & Porter note that the Act underwent revisions regarding the definition of “BCCs” and “contract,” the prohibition effective dates, and BCC designation removal requests.

2. The White House, *Launching the Genesis Mission*, Executive Order (EO) 14363 (November 24, 2025). <https://www.whitehouse.gov/presidential-actions/2025/11/launching-the-genesis-mission/>.

This EO on advancing AI-accelerated innovation and discovery through a coordinated national effort called the “Genesis Mission” includes biotechnology in the list of 20 science and technology challenges of national importance that the Genesis Mission will address. The EO directs the Secretary of Energy to establish and operate the “American Science and Security Platform” as the Mission’s infrastructure to provide high-performance computing, AI modeling and analysis frameworks, computational tools, domain-specific foundation models, secure access to datasets, and experimental and production tools.

3. U.S. Department of Health and Human Services, “HHS Winds Down mRNA Vaccine Development Under BARDA,” Press Release (August 5, 2025). <https://www.hhs.gov/press-room/hhs-winds-down-mrna-development-under-barda.html>.

In this press release, HHS announced that the Biomedical Advanced Research and Development Authority (BARDA) is terminating 22 mRNA vaccine development investments. It indicates that HHS conducted a review of mRNA vaccines and concluded that they fail to protect against upper respiratory infections. Moving forward, BARDA will prioritize investments in vaccines with stronger safety records and transparent clinical and manufacturing practices, such as whole-virus vaccines.



4. The White House, *Winning the Race: America's AI Action Plan* (July 2025). <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>.

Pillar 3 on leading in international AI diplomacy and security includes a section that calls for investment in biosecurity. It details three policy recommendations:

- Require all institutions receiving Federal funding for scientific research to use nucleic acid synthesis tools and synthesis providers that have robust nucleic acid sequence screening and customer verification procedures. Create enforcement mechanisms for this requirement rather than relying on voluntary attestation.
  - Led by the White House Office of Science and Technology Policy (OSTP), convene government and industry actors to develop a mechanism to facilitate data sharing between nucleic acid synthesis providers to screen for potentially fraudulent or malicious customers.
  - Build, maintain, and update as necessary national security-related AI evaluations through collaboration between the Center for AI Standards and Innovation (CAISI) at the Department of Commerce, national security agencies, and relevant research institutions.
5. The White House, *Improving the Safety and Security of Biological Research*, EO 14292 (May 5, 2025). <https://www.whitehouse.gov/presidential-actions/2025/05/improving-the-safety-and-security-of-biological-research/>.

This EO mandates the Director of OSTP lead an interagency process to establish guidance to immediately end federal funding of dangerous gain-of-function research conducted by foreign entities in countries of concern or where there is inadequate oversight. It likewise orders an end to federal funding of other life-science research under similar circumstances that could reasonably pose a threat to public health, public safety, and economic or national security. The EO also directs the interagency process to revise or replace existing oversight frameworks, develop a risk management framework, increase accountability and public transparency of gain-of-function research, and develop enforcement terms for future research contracts or grant awards. The EO defines “dangerous gain-of-function research” as “scientific research on an infectious agent or toxin with the potential to cause disease by enhancing its pathogenicity or increasing its transmissibility.”

6. The White House, *Initial Rescissions Of Harmful Executive Orders And Actions*, EO 14148 (January 20, 2025). <https://www.whitehouse.gov/presidential-actions/2025/01/initial-rescissions-of-harmful-executive-orders-and-actions/>.

The White House, *Additional Rescissions of Harmful Executive Orders and Actions*, EO 14236 (March 14, 2025). <https://www.whitehouse.gov/presidential-actions/2025/03/additional-rescissions-of-harmful-executive-orders-and-actions/>.

These EOs rescinded a total of 96 EOs issued by the Biden Administration. Among the rescissions are EOs related to biosecurity, including:

- Executive Order 13987 of January 20, 2021 (Organizing and Mobilizing the United States Government To Provide a Unified and Effective Response To Combat COVID-19 and To Provide United States Leadership on Global Health and Security).



- Executive Order 13990 of January 20, 2021 (Protecting Public Health and the Environment and Restoring Science To Tackle the Climate Crisis).
- Executive Order 13992 of January 20, 2021 (Revocation of Certain Executive Orders Concerning Federal Regulation).
- Executive Order 13995 of January 21, 2021 (Ensuring an Equitable Pandemic Response and Recovery).
- Executive Order 13996 of January 21, 2021 (Establishing the COVID-19 Pandemic Testing Board and Ensuring a Sustainable Public Health Workforce for COVID-19 and Other Biological Threats).
- Executive Order 13997 of January 21, 2021 (Improving and Expanding Access to Care and Treatments for COVID-19).
- Executive Order 13999 of January 21, 2021 (Protecting Worker Health and Safety).
- Executive Order 14000 of January 21, 2021 (Supporting the Reopening and Continuing Operation of Schools and Early Childhood Education Providers).
- Executive Order 14002 of January 22, 2021 (Economic Relief Related to the COVID-19 Pandemic).
- Executive Order 13994 of January 21, 2021 (Ensuring a Data-Driven Response to COVID-19 and Future High-Consequence Public Health Threats).
- Executive Order 14081 of September 12, 2022 (Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy).

7. The White House, *Withdrawing the United States from the World Health Organization*, EO 14155 (January 20, 2025). <https://www.whitehouse.gov/presidential-actions/2025/01/withdrawing-the-united-states-from-the-worldhealth-organization/>.

This EO outlines actions to enable U.S. withdrawal from the WHO, citing WHO's mishandling of the Covid-19 pandemic, its failure to adopt reforms, its inability to demonstrate independence from inappropriate political influence, and its demands of unfairly onerous payments from the United States. In lieu of WHO membership, the EO directs the National Security Council to undertake necessary efforts to safeguard public health and fortify biosecurity. Similarly, it directs the Secretary of State and the Director of the OMB to identify alternative international partners. Additionally, it orders the Director of the White House Office of Pandemic Preparedness and Response Policy to review, rescind, and replace the 2024 U.S. Global Health Security Strategy.

## Panel 5: Understanding the Twin Impacts of S&T Competition

- How will S&T competition and the changes it generates impact both threat and response?
- Does the answer differ by technology sector (AI, high performance computing, advanced manufacturing, innovative delivery systems, etc.) or are the impacts inseparable?
- Are there significant trade-offs between risks and benefits?
- Do the answers to these questions differ significantly between public and private sector actors? If so, what can be done to narrow them?



Kimberly Peh and Mike Albertson, eds., *In Search of Strategic Advantage: Understanding the Landscape of Technology Competition* (Livermore, CA: Center for Global Security Research, 2025). [https://cgsr.llnl.gov/sites/cgsr/files/2025-11/CGSR-Occasional-Paper-Technology-Competition\\_web\\_final.pdf](https://cgsr.llnl.gov/sites/cgsr/files/2025-11/CGSR-Occasional-Paper-Technology-Competition_web_final.pdf).

This CGSR Occasional Paper explores the dimensions of science and technology competition across domains, actors, and the spectrum of conflict. Contributing authors offer various definitions of “strategic advantage” and pathways to achieve it, and they identify trade-offs between its risks and benefits. For example, Zack Davis argues that “strategic advantage is achieved when a nation exploits the latent potential of technology to increase its power relative to other countries, who are also competing for advantage in the international system.” Additionally, Caroline Wesson discusses China’s “innovate around” strategy to counter U.S. export controls policies aimed at maintaining leadership over China in the design of advanced semiconductors.

Sameul H. King, Claudia L. Driscoll, David B. Li, Daniel Guo, Aditi T. Merchant, Garyk Brix, Max E. Wilkinson, and Brian L. Hie, “Generative Design of Novel Bacteriophages with Genome Language Models,” bioRxiv preprint (September 2025). <https://doi.org/10.1101/2025.09.12.67591>.

This pre-print manuscript presents the training of a genome language model to generate novel genomes. The authors sought to generate novel bacteriophage genomes using a single bacteriophage species as their design template. They chose to work with bacteriophage to mitigate biosafety concerns. Throughout the manuscript, the authors emphasize the importance of building robust biosafety frameworks into their language model. Their key safety layer was excluding human-infected viruses from the model's training data, and they further limited training data to genomic data from a single bacteriophage viral family. Additional constraints were added to their language model to create novel bacteriophage genomes, including specifications for genome length, genomic gene order, and sequence identity to original reference genome. It is important to note that this manuscript is posted on a pre-print website and has not been peer-reviewed or published by an accredited scientific journal. Claims made by the authors, biosafety review, and ethical review of publishing this work are not yet formally supported by the scientific community.

Katarzyna P. Adamala et al., “Confronting Risks of Mirror Life,” *Science* 386, iss. 6278 (2024), pp.1351-1353. <https://doi.org/10.1126/science.ads9158>.

A working group of world-leading biologists is calling for increased analysis and broader discussion of the risks of “mirror life,” which are lifeforms composed entirely of mirror-image biological molecules. While they judge that the capability to create mirror life is at least a decade away, they call for preemptive development of frameworks to address its “unprecedented and largely overlooked” risks. The working group’s initial analysis on mirror bacteria indicated that it would likely cause lethal infection in humans, animals, and plants that can spread in nature. Further, the working group could not rule out spread across ecosystems. In view of these risks, the working group advocates prohibiting research that aims to create mirror bacteria. It also proposes biocontainment and biosafety approaches to reduce risks, noting that countermeasures appear very unlikely to stop or reverse the spread of mirror bacteria.



Report of the National Security Commission on Emerging Biotechnology, *Charting the Future of Biotechnology: An action plan for American security and prosperity* (April 2025). <https://www.biotech.senate.gov/final-report/chapters/>.

In the Fiscal Year 2022 NDAA, Congress established the bipartisan National Security Commission on Emerging Biotechnology (NSCEB) with the mandate to conduct a comprehensive review of emerging biotechnology's impact on national security and provide practical recommendations to preserve American dominance in this field. The report of this review concludes that the United States must act in the next three years to remain competitive with China in biotechnology, or risk "a setback from which we may never recover." The Commission recommends a series of actions for the executive and legislative branches under six pillars: 1) Prioritize Biotechnology at the National Level; 2) Mobilize the Private Sector to get U.S. Products to Scale; 3) Maximize the Benefits of Biotechnology for Defense; 4) Out-Innovate our Strategic Competitors; 5) Build the Biotechnology Workforce of the Future; and 6) Mobilize the Collective Strengths of our Allies and Partners.

Helia Samani, "Congress Must Act to Secure U.S. Biotechnology," Risky Business Blog, Nuclear Threat Initiative (September 2025). <https://www.nti.org/risky-business/congress-must-act-to-secure-u-s-biotechnology/>.

In this blog post, NTI offers four recommendations for Congress to address the tradeoffs between benefits and risks of biotechnology competition, building upon recommendations from the NSCEB. First, establish a national agency for biotechnology governance to resolve the challenge of fragmented oversight. Second, dedicate funding to biosecurity and biosafety innovation to mitigate the risks posed by biodesign tools. Third, mandate pre-funding biosecurity reviews and incentivize DNA synthesis screening, which NTI describes as the frontline defense for preventing misuse. Fourth, provide annual funding for CAISI to develop standards and guardrails.

Anthropic, "Why do we take LLMs seriously as a potential source of biorisk?," Red Anthropic, (September 2025). <https://red.anthropic.com/2025/biorisk/>.

This blog post discusses Anthropic's approach to balancing the risks and benefits of frontier AI models for biosecurity. While Anthropic seeks to advance scientific discovery by offering tools that help structure biological data, speed up analysis, and automate experimental design, it also implements measures aimed at identifying, measuring, and mitigating misuse of these tools. These biorisk mitigation measures span across three lines of effort. First, Anthropic is increasing information sharing aimed at understanding whether non-experts can misuse Anthropic models to help develop biological weapons. Second, Anthropic is developing and implementing safeguards to block potentially harmful information. Third, Anthropic supports the U.S. AI Action Plan's recommendations to conduct national security evaluations and bolster nucleic acid synthesis screening.

## Panel 6: Embracing Opportunity



- In long-term historical perspective, what opportunities are created by new technological forces?
- How are they best seized?

Drew Endy, Sarah Moront, Vossilis Andrea Alexopoulos, Raj Patel, Rhea Join, and Britney Bennett, “Biosecurity Really: A Strategy for Victory” (Palo Alto, CA: Hoover Institution, 2025).

[https://www.hoover.org/sites/default/files/research/docs/Moront\\_BiosecurityReally\\_web-251007.pdf](https://www.hoover.org/sites/default/files/research/docs/Moront_BiosecurityReally_web-251007.pdf).

This Hoover Institution report presents biotechnology as a general-purpose technology, describing its transformation from a centralized, capital-heavy production toward more distributed, flexible production (analogous to how biology already works in nature). The authors explore the potential upsides of this development, particularly for resilience: distributed biomanufacturing could enable societies to more quickly respond to shocks by standing up production capacity closer to where the need is greatest. Realizing this potential requires sustained, long-term public investment in foundational capabilities and tools, rather than private sector capital alone. The authors also underscore the importance of building an enabling ecosystem—including regulations and lab-to-market pathways—for helping the bioeconomy scale reliably rather than staying stuck in one-off breakthroughs.

“Biotechnology and Synthetic Biology,” chapter in *The Stanford Emerging Technology Review 2025: A report on ten key technologies and their policy implications*, Herbert Lin, ed. (Palo Alto, CA: Hoover Institution, 2025). <https://setr.stanford.edu/technology/biotechnology-synthetic-biology/2025>.

This chapter of the Stanford Emerging Technology Review 2025 describes policy implications of advancements in biotechnology and synthetic biology. The policy implications stem from a key argument that advancements in these technologies are enabling the transformation of commercial biotechnology into a more distributed system that reflects natural biology. In this new system, fermentation facilities can, for example, be set up wherever there are sugar and electricity, making it easier to quickly respond to increases in demand that occur during disease outbreaks. The authors notes that biotechnology—defined as the use of biological systems to produce medicines, materials, and services—is a rapidly growing industry that currently makes up approximately 5% of the U.S. GDP. They further note that synthetic biology—defined as an interdisciplinary subset of biotechnology that focuses on engineering and constructing new biological functions through sequencing and synthesis of DNA—has many applications, including in medicine (e.g., mRNA vaccines), agriculture (e.g., drought-resistant crops), and the on-demand production of medicines or fuels. As such, synthetic biology can boost manufacturing capabilities and strengthen the industrial base.

Tal Feldman and Jonathan Feldman, “The U.S. Cannot Prevent Every AI Biothreat—But It Can Outpace Them,” *Lawfare* (2025). <https://www.lawfaremedia.org/article/the-u.s.-cannot-prevent-every-ai-biothreat-but-it-can-outpace-them>.

This article examines the severity of biosecurity risks presented by protein language models (PLMs), a new class of AI systems originally developed to accelerate drug discovery that can now design novel proteins for potential bioweapons. The authors argue that current U.S.



biosecurity strategies are inadequate because they focus on synthesis screening for known pathogens, while PLMs generate unknown proteins whose danger cannot be reliably predicted from sequence alone and require experimental testing. Furthermore, growing availability of benchtop synthesis machines allows actors to bypass screening entirely, shifting the danger upstream to the model output itself. Rather than attempting to prevent every threat, the authors suggest that the United States must develop AI systems explicitly trained to manufacture therapeutics and establish a national infrastructure for rapid biomanufacturing capabilities to outpace emerging biothreats from this dual-use technology.

Artem A. Trotsyuk et al., “Toward a framework for risk mitigation of potential misuse of artificial intelligence,” *Nature Machine Intelligence* 6 iss.12 (2024), pp.1435–1442.

<https://doi.org/10.1038/s42256-024-00926-3>.

This article presents a methodological approach to assist researchers in mitigating potential AI misuse risks in biomedical research. The authors argue that current ethical standards and regulations are inadequate to mitigate potential misuse threats, especially as AI becomes increasingly powerful and accessible. Building upon current ethical review processes, the authors present a five-pronged risk mitigation framework: 1) researchers must systematically identify potential pathways for misuse of AI to cause harm; 2) researchers must consider all stakeholders who would be impacted by potential misuse; 3) researchers must consider specific mitigation strategies to address identified potential misuse; 4) governance processes must integrate these assessments as a standard component; and 5) if potential misuse cannot be mitigated, researchers must consider modifying their approach or considering alternative research questions. The authors suggest applying this framework to research areas that present high risks for misuse, such as drug and chemical discovery, synthetic data, and ambient intelligence.

## **Panel 7: Aligning Public Health Preparedness with National Security Preparedness**

- What are the key areas of alignment? What are the key disconnects?
- How does resilience in the public health sector contribute to deterrence?
- How can the synergy between these efforts be improved?

Kenneth Bernard, “Biodefense Leadership and National Security: Lessons from the Goldwater-Nichols Reforms,” *Think Global Health* (April 5, 2022).

<https://www.thinkglobalhealth.org/article/biodefense-leadership-and-national-security-lessons-goldwater-nichols-reforms>.

Kenneth Bernard—a former Assistant Surgeon General who worked at the White House on biosecurity in the Bill Clinton and George W. Bush administrations—makes a case for reorganizing the relationship between public health and national security professionals, drawing inspiration from the Goldwater-Nichols Department of Defense Reorganization Act of 1986. Bernard argues that the U.S. pandemic and biothreat preparedness and response



enterprise would benefit from a similar reorganization of command, control, and communications. Specifically, he calls for embedding in the White House a permanent structure that is tasked with developing operational plans and response capabilities. This “combatant commander” for countering pandemics and other biothreats must also be accompanied by concerted efforts to ensure institutional and cultural adaptation.

Juan Siliezar, “Are we ready?,” Brown School of Public Health (May 7, 2025).  
<https://sph.brown.edu/news/2025-05-07/areweweready>.

Experts from Brown University’s School of Public Health warn that the knowledge and tools developed throughout the Covid-19 pandemic can disappear without continued support. The United States made strides in virus testing and surveillance, vaccine production and distribution, telemedicine, support for the healthcare workforce, and rebuilding public trust in science. Reduced investment in these key areas risk eroding progress and repeating mistakes, ultimately hamstringing future response efforts to the next biological threat.

Ben C. Snyder, Gerald L. Epstein, Josh Wentzel, Robert P. Kadlec, and Gerald W. Parker, “Envisioning an Independent Bioresponsibility Authority to Safeguard U.S. Leadership in the Life Sciences,” Scowcroft Institute of International Affairs, Texas A&M University (January 2025).  
<https://bush.tamu.edu/wp-content/uploads/2025/01/Envisioning-an-Independent-Bioresponsibility-Authority-Jan-2025-2.pdf>.

In this report, biosecurity experts from the Scowcroft Institute of International Affairs propose a modernized biosafety and biosecurity governance framework for early-stage research that keeps pace with rapid technological advancements. This framework is rooted in the concept of “bioresponsibility,” which the authors define as “the commitment to conducting life science research in an ethical, secure, and safe manner to reduce the risk of misuse and accidents.” Specifically, they recommend establishing an independent federal bioresponsibility agency and creating a bioresponsibility regulatory framework. These measures would improve the current fragmented biological risk management structure by closing gaps in oversight, information sharing, and training, while also alleviating pressure from some compliance requirements that are overly burdensome.

Gabriel Seidman et al., “An ‘Always On’ Approach to Health Care and Public Health Systems: Building Standing Capabilities That Can Respond to Shocks and Emergencies”, Chapter 11 in *Investing in Pandemic Prevention, Preparedness, and Response: Volume 2, Fourth Edition* (Eds. Siddhanth Sharma et al.), World Bank Group, 2025, pp. 283-310,  
<https://documents1.worldbank.org/curated/en/099301511192520131/pdf/IDU-8282e225-6f71-444f-aa42-053d8f969f1b.pdf>.

The authors argue that the “stop-start approach” of responding to public health shocks and emergencies like the Covid-19 pandemic should be abandoned for an “always on approach,” which offers more health and economic benefits. The authors describe “always on” as health systems that “consistently provide quality clinical and public health services in routine settings while contributing to emergency preparedness, prevention, and response for shocks and emergencies.” Examples of systems that would benefit from an “always on” approach include adult vaccination, clinical research, and pathogen surveillance. Key



limitations to this approach stem from resource allocation and political economy challenges.

## Panel 8: Aligning Public and Private Sector Capabilities and Capacities

- What is the role of the private sector, including the philanthropic sector, in public health preparedness? In national security preparedness?
- What new roles are necessary and possible as public sector policies and approaches evolve?
- What more needs to be done to ensure that the two sectors are ready to cooperate in the next major health crisis?

Alanna S. Fogarty, Rachel A. Vahey, Alexander G. Linder, Aishwarya Nagar, Kathryn M. Hogan, Julia Cizek, Clair J. Standley, and Erin M. Sorrell, “One Health Transboundary Assessment for Priority Zoonoses,” Johns Hopkins Research Data Repository, V1 (2025). <https://doi.org/10.7281/T1C557B5>.

The One Health Transboundary Assessment for Priority Zoonoses (OHTAPZ) is a five-phase methodology by Johns Hopkins Center for Health Security for strengthening transboundary zoonotic disease coordination at Points of Entry (PoEs). The adaptable assessment tool uses stakeholder mapping, tabletop exercises to map communication flows, SWOT analysis, comprehensive PoE checklists (95-133 questions), and simulation exercises with after-action reviews to recommend actions that address operational gaps across different levels of coordination. OHTAPZ was piloted in Libya, Tunisia, Iraq, and Jordan, demonstrating the tool's capacity to consolidate initial processes required by the International Health Regulations (IRH), Performance of Veterinary Services (PVS), and the Quadripartite One Health Joint Plan Action (2022-2026). The authors emphasize the need for a continuous cycle of collaboration and evolution in approaches to assessment, evaluation, and capacity building to improve communication and coordination systems between the human, animal, and environmental health sectors for preventing, detecting, responding to, and recovering from zoonotic diseases.

Jeremy Thomas, “LLNL scientists use AI to optimize antibodies against mutations and accelerate pandemic preparedness,” Lawrence Livermore National Laboratory (April 7, 2025). <https://www.llnl.gov/article/52716/llnl-scientists-use-ai-optimize-antibodies-against-mutations-accelerate-pandemic-preparedness>.

This LLNL news article shares how a public-private partnership used AI to preemptively optimize antibodies against viral evolution to enhance future pandemic preparedness. The public-private partnership brought together LLNL's government-funded supercomputing capabilities with AstraZeneca's clinical antibody development expertise to develop the Using the Generative Unconstrained Intelligent Drug Engineering (GUIDE) platform. Using the GUIDE platform, researchers analyzed over 10 billion potential antibody modifications to develop an optimized clinical antibody, 3152-1142. This optimized antibody demonstrated 100-fold improved potency against viral variants that emerged during the study, validating



the approach's predictive power. The project participants propose this approach as a cost-effective, generalizable model for future biodefense, enabling rapid antibody redesign that could qualify for expedited regulatory approval to address current and emerging biothreats.

OpenAI, *Preparing for future AI capabilities in biology*, (June 18, 2025).  
<https://openai.com/index/preparing-for-future-ai-capabilities-in-biology/>.

In this article, OpenAI outlines its comprehensive approach to managing dual-use risks as AI models advance toward "high" biological capability thresholds that could assist novice actors in creating biothreats. The company explains that it implements layered safeguards, including: trained refusals for harmful requests; always-on detection systems; end-to-end red teaming with domain experts; and security controls protecting model weights. OpenAI also describes public-private sector alignment as central to its strategy, noting partnerships with the U.S. and UK AI Safety Institutes and Los Alamos National Laboratory. Additionally, OpenAI hosted a biodefense summit in July 2025 to deepen collaboration with the U.S. and allied governments. OpenAI advocates granting vetted institutions access to maximally helpful models for biodefense research while calling for coordinated investment in synthesis screening, pathogen detection infrastructure, and biosecurity startups. It seeks to position the private sector as an essential partner in strengthening societal biological defenses beyond AI safeguards alone.

Bipartisan Alliance for Global Health Security, *Protecting Americans from Biological Threats*, Working Group Report, Center for Strategic and International Studies (February 4, 2026).  
<https://www.csis.org/analysis/protecting-americans-biological-threats>.

In this working group report, the CSIS Bipartisan Alliance for Global Health Security argues that declining U.S. biodefense capabilities require urgent public-private integration to address escalating biological threats. The working group, comprising over 60 bipartisan experts, identified the private sector as essential to national security and public health preparedness through four critical domains: 1) modernizing biosurveillance; 2) ensuring biosafety and biosecurity; 3) improving the declining biodefense enterprise; and 4) strengthening response and recovery coordination. The report references Operation Warp Speed as a viable model that enabled public-private partnerships to deliver rapid countermeasures by combining federal funding with private sector innovation and manufacturing. Key report recommendations include requiring private sector participation in all federal bio-preparedness programs, creating authorities for flexible public-private workforce development, and establishing partnership models with liability protections. The authors emphasize that cooperation readiness demands sustained high-level political commitment, clear federal coordination through a proposed White House Office of Bio-preparedness, and treating biodefense as an integrated system rather than separate government and industry spheres.

## Panel 9: Ensuring Essential International Partnerships

- What should and can be done to reform international institutions?
- What should and can be done to strengthen international norms?



- What are the prospects for cooperation for biosecurity with Russia and China?

Jean Pascal Zanders, “A very thin gruel, indeed,” *The Trench* (January 8, 2026). <https://www.the-trench.org/a-very-thin-gruel-indeed>.

Jean Pascal Zanders expresses skepticism of the U.S.-led international effort to strengthen the Biological and Toxin Weapons Convention (BWC) and the U.S. proposed AI-driven verification system. Zanders notes that President Donald Trump seemed to overturn decades of U.S. opposition to BWC verification during his speech in September 2026 at the United Nations General Assembly. However, after the BWC Meeting of States Parties (MSP) in December 2026, Zanders concludes that the verification initiative has not progressed beyond an idea. Reflecting on remarks by U.S. Under Secretary for Arms Control and International Security Thomas DiNanno and other U.S. representatives from the Department of War, HHS, and the Department of Energy at a U.S.-hosted side event, he notes that the U.S. administration has not shared concept notes, working papers, or public statements that substantively elaborate the details of its thinking.

James Giordano, “Biotechnologies and the Treaty Gap: Why Biological Weapons Governance Is Falling Behind; and Some Thoughts on How to Fix It,” *Institute for National Strategic Studies, National Defense University* (December 22, 2025). <https://inss.ndu.edu/Media/News/Article/4363698/biotechnologies-and-the-treaty-gap-why-biological-weapons-governance-is-falling/>.

James Giordano argues that the accelerated development and spread of biotechnology have created a “treaty gap” in which the BWC and other related instruments have normative value but are increasingly becoming disassociated with modern approaches to the development, distribution, and possible weaponization of biocapabilities. This has resulted in five key areas of undergovernance: 1) the unclear and 1970s-era definitions of biotechnology, which are unable to adequately categorize platform technologies and upstream enabling activities; 2) the undermining of verification and transparency, especially with the addition of AI, which can be used for monitoring and undermining compliance; 3) non-state actors, despite the requirements of UN Security Council Resolution 1540; 4) the inability of the BWC and other related instruments to manage the distribution of biotechnology and “intangible transfers” of sequence information, cloud laboratories, and other virtualized activities; and (5) the disconnect between the cooperative requirements of the BWC and the security and economic interests of states in biotechnology. To bridge these gaps, Giordano suggests developing a “living” annex under the BWC to provide regular updates on national implementation, and a multi-stakeholder governance structure through which states, industry, and academia can come together to develop norms, best practices, and a culture of duty of care.

Diane DiEuliis, Elise Annett, and James Giordano, “Artificial Intelligence: A Double-Edged Sword in Support and Subversion of the Biological Weapons Convention; Part Two: Implications and Recommendations”, *Institute for National Strategic Studies, National Defense University* (December 15, 2025). <https://inss.ndu.edu/Research-and-Commentary/View-Publications/Article/4359602/artificial-intelligence-a-double-edged-sword-in-support-and-sub>.



The authors argue that AI represents a double-edged sword in the context of the BWC because it holds the promise of significantly improving biosurveillance, verification, and response, while at the same time providing actors with the means to avoid detection, distort information, and erode trust in compliance. They note that AI has the capability for simulating biosurveillance thresholds and their variability, which in turn enables the design, production, and release of agents in patterns that are below the thresholds and mimic the natural world. To counter these risks, the authors make a series of recommendations, including: 1) establish AI countermeasures as a key biodefense imperative; 2) strengthen intelligence and data fusion across health, cyber, supply chain, and environmental domains; 3) conduct red-, blue-, and white-team AI simulation and wargaming; and 4) develop specific international regulatory initiatives for AI in life sciences, including a means of controlling secure DNA synthesis, constraining high-risk AI models and platforms, and responding to violations.

David Stiefel, Gabrielle Essix, Eva Siegmann, Katherine Budeski, Nathan A. Paxton, and Jaime M. Yassif, “Enhancing Transparency for Bioscience Research and Development,” Nuclear Threat Initiative (August 2025). <https://www.nti.org/analysis/articles/enhancing-transparency-for-bioscience-research-and-development/>.

The report's main takeaway is that states must test new options for enhancing BWC transparency rather than relying on the current mechanisms. The authors argue that the current level of transparency provided by Confidence-Building Measures (CBMs) is not enough to build confidence in the peaceful nature of bioscience R&D in the face of a rapidly changing international security context. To move towards enhanced transparency, the authors propose incorporating three politically realistic and incremental BWC measures: 1) scientific and technical tools, including structured data collection and analysis in the context of bioscience R&D; 2) procedural modalities, which refer to standardized approaches in the areas of information gathering, dissemination, and review; and 3) institutional arrangements, which refer to the institutions that oversee the implementation and maintenance of the transparency initiative.

Jaime Yassif, Shayna Korol, and Angela Kane, “Guarding Against Catastrophic Biological Risks: Preventing State Biological Weapon Development and Use by Shaping Intentions,” *Health Security* 21, iss. 4 (2023), pp. 258-265. <https://doi.org/10.1089/hs.2022.0145>.

In this article, NTI analysts argue that the most effective means of limiting the catastrophic threats from state-run biological weapons programs is to alter the incentives to acquire and pursue biological weapons such that they are no longer cost-effective or attractive. Instead of focusing on limiting capabilities, the authors propose focusing prevention efforts on the following three pillars: 1) greater transparency regarding bioscience and biodefense; 2) better attribution for high-consequence events; and 3) more credible accountability for non-compliance. Enhanced transparency—such as improved information-sharing and voluntary peer review or compliance assessment visits under the BWC—is intended to increase assurance about states’ activities without requiring full verification. Strengthened attribution, including a better-resourced UN Secretary General’s Mechanism and potentially a new Joint Assessment Mechanism, is meant to raise the likelihood that responsible actors can be credibly identified after suspicious events. Finally, by linking detection and attribution to predictable political and material consequences, the authors maintain that



states can be deterred from pursuing biological weapons, thereby lowering the probability of global catastrophic biological incidents.

#### Past CGSR Workshops on Biosecurity Topics:

- Madeleine Lambert, Ryan Christenson, Ray Hughes, Daniel Kroth, Daeyeon Lee, and Kaitlyn Lenkeit, *Biosecurity Amidst Technological and Geopolitical Dynamism*, Workshop Summary Report, Center for Global Security Research (March 14-15, 2024). <https://cgsr.llnl.gov/sites/cgsr/files/2024-08/2024-03-Biosecurity-Amidst-Technological-and-Geopolitical-Dynamism-Annotated-Bibliography.pdf>.
- Lauren Borja, Alexander Campbell, Marigny Kirschke-Schwartz, Brian Radzinsky, and Brandon Williams, *Rethinking U.S. Biosecurity Strategy for the Decade Ahead*, Workshop Summary Report, Center for Global Security Research (October 27-29, 2020). [https://cgsr.llnl.gov/sites/cgsr/files/2024-08/RETHINKING\\_US\\_BIOSECURITY\\_STRATEGY\\_FOR\\_THE\\_DECADE\\_AHEAD\\_workshop-summary.pdf](https://cgsr.llnl.gov/sites/cgsr/files/2024-08/RETHINKING_US_BIOSECURITY_STRATEGY_FOR_THE_DECADE_AHEAD_workshop-summary.pdf).
- Joseph Johnson and Donald Prosnitz, *Maintaining Innovation and Security in Biotechnology: Lessons Learned from Nuclear, Chemical, and Information Technologies*, Workshop Summary Report, Center for Global Security Research (October 2017). [https://cgsr.llnl.gov/sites/cgsr/files/2024-08/Biotech\\_2017\\_Summary\\_Final.pdf](https://cgsr.llnl.gov/sites/cgsr/files/2024-08/Biotech_2017_Summary_Final.pdf).
- *Dogs that Haven't Barked: Towards an Understanding of the Absence of Expected Technological Threats*, Workshop Summary Report, Center for Global Security Research (July 6-7, 2016). <https://cgsr.llnl.gov/sites/cgsr/files/2024-08/DogsSummaryReportFinal.pdf>.