BIPARTISAN COMMISSION ON BIODEFENSE

Atlantic Council
SCOWCROFT CENTER FOR STRATEGY AND SECURITY

AN UPDATE TO

THE APOLLO PROGRAM FOR BIODEFENSE

WINNING THE RACE AGAINST BIOLOGICAL THREATS

July 2026

ARTIFICIAL INTELLIGENCE

INTRODUCTION

Artificial intelligence (AI) is changing how biological threats can be created, detected, and countered. Following its June 4, 2026, public meeting, "Pandora's Prompt: AI and the Biological Threat," the Bipartisan Commission on Biodefense at the Atlantic Council established AI as the sixteenth technology priority in *The Apollo Program for Biodefense*. The Commission assesses AI's offensive biological risks and defensive opportunities and calls on the United States, working with industry and international partners, to invest in AI-enabled disease surveillance and diagnostics, medical countermeasure development, microbial forensics and attribution, model evaluation and safeguards, and adaptive nucleic acid synthesis screening.

A FUNDAMENTAL TRANSFORMATION

Artificial intelligence is not a sector-specific technology but one that accelerates discovery, analysis, and design across biology, chemistry, and all other technical domains nearly simultaneously. AI fundamentally transforms the biological threat landscape. AI systems capable of analyzing, synthesizing, and drawing inferences from vast biological datasets compress timelines to develop capabilities that once required years of specialized expertise and costly laboratory infrastructure. Large language models can now provide meaningful technical guidance across the pathogen engineering process, and biological design tools can design new proteins, predict how genetic changes will affect an organism, and ultimately engineer molecules that never existed in nature.

> Uplift is the measurable increase in a person's ability to cause biological harm when assisted by an AI system, compared to what that person could accomplish without it.

Controlled uplift trials have shown that individuals with modest scientific backgrounds produce significantly stronger biological weapons acquisition plans when given access to a frontier AI model, and that gap closed across successive model generations in mere months. For more than two decades, we have relied on screening commercially synthesized DNA sequences against databases of known pathogens and toxins as a way of defending against misuse. This approach has become increasingly insufficient over the years as researchers demonstrated in late 2025 that AI protein design tools could redesign dangerous proteins such that each retained its function while presenting a genetic sequence that most commercial screening programs failed to detect.[1] No mandatory federal framework yet exists that requires AI developers to evaluate biological risk before public release of their models. The capacity to evaluate such risks requires a defensive technology in its own right, one in which the United States has woefully underinvested.[2]

The same capabilities that create risk for offense hold extraordinary promise for defense. AI can synthesize thousands of scientific studies in seconds, flag unusual disease patterns across fragmented human, animal, and plant health data systems, accelerate medical countermeasure design, improve biological detection and environmental surveillance, and strengthen the US' ability to determine whether a biological event was natural, accidental, or intentional. Models purpose-built for biology can predict protein structures, model pathogen evolution, and triage vast streams of surveillance data faster and at lower cost than any prior method,[3] extending the reach of ubiquitous sequencing, digital pathogen surveillance, and forecasting described elsewhere in *The Apollo Program for Biodefense*.[4]

Realizing this potential will require secure access to state-of-the-art AI systems, curated biological datasets, and personnel trained in both AI and biodefense. The US, and the world, should develop standardized benchmarks for biological capability, repeatable uplift trials measured against meaningful baselines,[5] structured red-teaming, and secure infrastructure needed to test the most sensitive capabilities. These capabilities require establishing datasets, testbeds, and experts in advance of, rather than during, a crisis.

Making AI a biodefense technology priority, with practical benefits for many stakeholders, including defense, intelligence, law enforcement, public health, academia, industry, and nongovernmental organizations, will require investments in:

- AI-enabled surveillance, forecasting, and anomaly detection across human, animal, plant, and environmental data streams;
- AI-assisted diagnostics, countermeasure discovery, evidence synthesis, identification of the most promising research and testing approaches, and response planning;
- AI-enabled microbial forensics and attribution tools, including reference databases, detection algorithms, laboratory-of-origin analysis methods, and computational screening tools capable of distinguishing natural from AI-generated or AI-optimized sequences;
- Watermarking, fingerprinting, and provenance tools for biological design systems to detect and trace AI-generated sequences;
- Secure red-teaming and evaluation infrastructure for frontier, open-weight, and specialized biological AI models before deployment; and
- Adaptive screening and monitoring of DNA synthesis providers, cloud laboratories, benchtop synthesis platforms, and other points where digital designs could become physical biological material.

The Apollo Program for Biodefense is an ambitious goal-directed program to develop and deploy the technologies needed to defend against all biological threats, empower public health, and prevent pandemics, no matter what the source.

Governments at all levels, together with industry and international partners, should also invest in the safety infrastructure needed to keep these tools beneficial. Commercial guardrails must be continually hardened against attempts to bypass them, yet even hardened guardrails are not sufficient. Open-source models can be downloaded, modified, and run without company oversight, and AI-designed sequences can evade traditional screening, creating gaps that no single intervention can close.[6]

A successful biodefense strategy must connect prevention, deterrence, preparedness, detection, response, attribution, recovery, and mitigation across the full range of biotechnologies and capabilities. This will require sustained public-private cooperation. AI developers need biological threat information from the government to build meaningful safeguards, and federal departments and agencies need access to advanced commercial models to understand what those systems can do. Just as cybersecurity depends on threat information moving between government and industry, AI-biodefense will require a shared understanding of how adversaries could misuse models, data, synthesis, automation, and laboratory infrastructure.[7]

The Bipartisan Commission on Biodefense at the Atlantic Council establishes AI as the sixteenth technology priority in *The Apollo Program for Biodefense*, and recognizes AI as a means of strengthening the other fifteen technology priorities in the program. With sustained investment, interagency coordination, and public-private collaboration, the United States, countries around the world, industry, academia, and nongovernmental organizations can ensure that AI becomes an incredibly powerful tool in the arsenal for biodefense rather than the most dangerous addition to that of the attacker.

ENDNOTES

[1] Wittmann, Bruce J., et al. "Strengthening Nucleic Acid Biosecurity Screening against Generative Protein Design Tools." *Science*, vol. 390, no. 6768, 2 Oct. 2025, pp. 82-87, www.science.org/doi/10.1126/science.adu8578.

[2] O'Brien, John T., and Nelson, Cassidy. "Assessing the Risks Posed by the Convergence of Artificial Intelligence and Biotechnology." Health Security, vol. 18, no. 3, 2020, pp. 219-227, www.liebertpub.com/doi/10.1089/hs.2019.0122. See also Bipartisan Commission on Biodefense. "Pandora's Prompt: AI and the Biological Threat." Atlantic Council, 4 June 2026, www.atlanticcouncil.org/event/pandoras-prompt-ai-and-the-biological-threat.

[3] OpenAI. "Introducing GPT-Rosalind for Life Sciences Research." OpenAI, 17 Apr. 2026, openai.com/index/introducing-gpt-rosalind. See also OpenAI, "Strengthening Societal Resilience with Rosalind Biodefense," 29 May 2026, openai.com/index/strengthening-societal-resilience-with-rosalind-biodefense.

[4] Bipartisan Commission on Biodefense. *The Apollo Program for Biodefense: Winning the Race Against Biological Threats.* Bipartisan Commission on Biodefense, Jan. 2021, biodefensecommission.org/reports/the-apollo-program-for-biodefense.

[5] Götting, Jasper, et al. "Virology Capabilities Test (VCT): A Multimodal Virology Q&A Benchmark." *arXiv* preprint, 21 Apr. 2025, arxiv.org/abs/2504.16137.

[6] Nelson, Cassidy. "ADAPT: A Programme for the Advanced Detection of AI-Enabled Pathogenic Threats." *Frontiers in Bioengineering and Biotechnology*, vol. 14, 2026, article 1819372, doi.org/10.3389/fbioe.2026.1819372. See also Altman, Sam, et al. "In Support of Mandatory Nucleic Acid Synthesis Screening and Recordkeeping." Open letter, 3 June 2026, screendna.org.

[7] OpenAI. "Biodefense in the Intelligence Age." OpenAI, 4 June 2026, openai.com/index/biodefense-in-the-intelligence-age.