

The Dual-Use Frontier of AI-Enabled Biotechnology

Civilian Opportunities, National
Security Threats, and the
Governance Challenge

Ana Florescu-Ciobotaru
Caleb Workman



HARVARD Kennedy School
BELFER CENTER

50 YEARS
OF RESEARCH, POLICY,
AND LEADERSHIP

SEPTEMBER 2026

Belfer Center for Science and International Affairs

Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org

Statements and views expressed in this report are solely those of the author(s) and do not imply endorsement by Harvard University, Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

Copyright 2026, President and Fellows of Harvard College

The Dual-Use Frontier of AI-Enabled Biotechnology

**Civilian Opportunities, National
Security Threats, and the
Governance Challenge**

Ana Florescu-Ciobotaru
Caleb Workman



HARVARD Kennedy School
BELFER CENTER

50
YEARS
OF RESEARCH, POLICY,
AND LEADERSHIP

SEPTEMBER 2026

About the Defense, Emerging Technology, and Strategy Program

The Defense, Emerging Technology, and Strategy Program examines defense policy and the role of emerging technologies in shaping international security. For more, visit belfercenter.org/programs/defense-emerging-technology-and-strategy.

About the Author

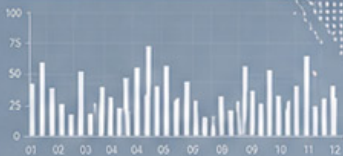
Ana Florescu-Ciobotaru is a third-year PhD Candidate in the Department of Chemistry and Chemical Biology at Harvard Griffin Graduate School of Arts and Sciences. Her research interests span the interface of chemical reactivity discovery and sustainable applications, while she is trained as a synthetic chemist. Prior to this, Ana graduated from MIT (Class of 2024) with a double major in Chemistry & Biology and Chemical-Biological Engineering.

Caleb F Workman is a joint Master in Public Policy and Master of Business Administration candidate at Harvard Kennedy School and Harvard Business School. His academic and professional interests focus on defense innovation and national security policy. Before attending Harvard, Caleb served as an active-duty U.S. Army Intelligence officer in the 25th Infantry Division, where he gained experience across the Indo-Pacific. He holds a B.S. in Economics and an M.S. in Engineering & Technology Management from the Colorado School of Mines.

Table of Contents

Executive Summary	2
1. Introduction	5
1.1 AlxBio Technology Stack	6
1.1.1 The Artificial Intelligence Layer.....	6
1.1.2 The Biological Data Layer	10
1.1.3 The Biotechnology Manufacturing Infrastructure Layer.....	12
1.2 Civilian Applications.....	14
1.2.1 AI-assisted Small Molecule Therapeutics.....	14
1.2.2 mRNA Therapies.....	15
1.2.3 CRISPR-Cas9 Therapies.....	16
1.2.4 Cell Therapies	17
1.2.5 Metagenomic Next-Generation Sequencing	18
1.2.6 Readiness and Validation Bottlenecks.....	19
1.3 Misuse Potential and National Security Consequences.....	20
1.3.1 AI-Enabled Democratization of Existing Bio Threats.....	20
1.3.2 Emergence of New Biological Threat Pathways	21
1.3.3 National Security Risks	22
2. AlxBio Risk Trajectory.....	23
2.1 Current Risk Baseline	25
2.2 Near-Term Outlook (0 to 2 Years).....	26
2.3 Medium- to Long-Term Outlook (2 to 5+ Years)	27
2.4 Risk Accelerants and Indicators	28
3. AlxBio Governance Gaps	30
3.1 Insufficient Mandates for Built-In AI-Biosecurity Safeguards in Frontier Models	30
3.1.1 Shortcomings of Voluntary Self-Regulation.....	31
3.1.2 U.S. Federal AI Biosecurity Regulation Efforts and Absence.....	32
3.2 Insufficient Regulation of the DNA Synthesis Industry	35
3.3 Insufficient Early Outbreak Detection and Response Protocols.....	37
4. Policy Recommendations	39
4.1 Frameworks for Enforcing Built-In AI-Biosecurity Safeguards in Frontier Models	40
4.1.1 Private Regulatory Markets	41
4.1.2 Private Insurance Markets.....	42
4.1.3 Government-Led Regulatory Actions	43
4.1.4 Technical Standards as an Enforcement Framework.....	45
4.2 Frameworks for Regulating the Biotechnology and Synthesis Industry.....	46
4.2.1 Nucleotide Screening Regulations	46
4.2.2 Laboratory Equipment Licensing Regulations	48
4.3 Frameworks for Early Outbreak Detection and Response.....	49
4.3.1 Proactive Outbreak Monitoring.....	49
4.3.2 Outbreak Responses.....	50
5. Conclusion.....	53
Endnotes.....	55

THREAT ANALYSIS



PATHOGEN GENOMIC SEQUENCING



OUTBREAK PROJECTION



SITUATIONAL AWARENESS



CONFIRMED CASES	128,017	■■■■■■■■■■
ACTIVE CASES	34,709	■■■■■■■■■■
RECOVERED	91,315	■■■■■■■■■■
FATALITIES	1,477	■■■■■■■■■■

RESPONSE READINESS



Executive Summary

AIxBio combines artificial intelligence (AI), biological data, and biotechnology manufacturing layers into a stack that transforms biological information into therapeutic design and, eventually, physical production. Its civilian upside is substantial: faster small-molecule discovery, more efficient messenger ribonucleic acid (mRNA) design, improved clustered regularly interspaced short palindromic repeats (CRISPR) and individualized cell therapies, and breakthroughs in personalized medicine. Its security risk is equally severe, since the same tools can reduce the expertise, time, cost, and iterations required to design or manufacture biological weapons.

The United States must preserve its AI and biotechnology lead against strategic competitors, but current governance is fragmented and slow. Frontier model safeguards are mostly voluntary, deoxyribonucleic acid (DNA) synthesis screening does not bind the full private market, and outbreak detection remains too reactive. This report assesses where AIxBio risk is growing, where U.S. policy falls short, and which governance models can reduce catastrophic biological risk without slowing legitimate biomedical innovation.

Key Assessments

- **AIxBio is a dual-use technology stack.** The civilian benefits are promising, but novel threats are emerging too. The risk stems from the combination of frontier AI models, biological datasets, and biotechnology manufacturing. Each layer is useful on its own; together, they can turn digital biological designs into physical outputs.
- **In the near term, the most immediate misuse risk is barrier reduction.** Large language models (LLMs) and open-source biological tools can help users search literature, reason through protocols, troubleshoot workflows, and substitute for previously tacit knowledge acquired with decades of experience. This phenomenon **lowers** informational barriers that once slowed inexperienced actors.
- **In the long term, AI-assisted pathogen design is the highest-consequence threat pathway.** Open viral sequence databases, genome language models, CRISPR tools, and nucleic acid synthesis could enable malicious actors to

enhance pathogen modifications to transmissibility, virulence, host range, or immune evasion. Viral design is also a near-term concern because viral genomes are shorter and easier to synthesize than more complex biological systems.

- **Physical bottlenecks still matter, but they are weakening.** Laboratories, trained personnel, specialized equipment, synthesis providers, and experimental validation are still barriers to misuse. Insider threats, supply-chain compromise, fragmented DNA orders, unscreened vendors, and open-source models outside **corporate** safety systems can reduce the effectiveness of those barriers.
- **Current frontier AI governance is too dependent on voluntary restraint.** Corporate preparedness frameworks, red-teaming, and model-use policies are useful but nonstandardized and vulnerable to competitive pressure. The United States lacks a comprehensive federal regime for mandating model-weight security **standards**, pre-deployment review, third-party audits, incident reporting, and stop-deployment authorities.
- **DNA synthesis screening is a major access-control gap.** Existing U.S. frameworks improve screening for federally funded research, but they do not create binding rules for all private synthesis providers. Without customer verification, sequence screening using best practices, split-order detection, updated sequences of concern, and mandatory reporting, malicious actors can exploit weak providers.
- **Outbreak detection remains too reactive for AI-enabled biological risk.** Public health systems often identify threats after spread has already begun. AI-enabled epidemic intelligence, wastewater monitoring, bioaerosol sampling, genomic **surveillance**, and metagenomic next-generation sequencing (mNGS) could reduce the time between biological anomaly detection and coordinated response.
- **Poorly calibrated governance creates competing national security risks.** Overreaching regulation could slow U.S. biomedical and AI innovation; weak regulation could permit **catastrophic** misuse. The policy challenge is targeting vulnerabilities without sacrificing the technological dominance that strengthens U.S. national security.

Recommendations

Enforcing Built-In AI-Biosecurity Safeguards in Frontier Models

- Establish a government-authorized private regulatory market where licensed technical auditors enforce AI-biosecurity safeguards for frontier models.
- Use government-defined safety outcomes and National Institute of Standards and Technology (NIST) or Center for AI Standards and Innovation (CAISI) technical standards to augment private audits.
- After establishing U.S. safeguards, expand the framework internationally through treaties and shared technical standards.

Regulating the Biotechnology and Synthesis Industry

- Require universal screening of synthetic nucleic acid orders longer than 50 nucleotides, including private-sector orders, with customer verification and mandatory reporting of failed legitimacy checks.
- Build an AI-enabled centralized screening system to detect fragmented orders and model the potential human-cell effects of ordered genetic sequences before synthesis.
- Create a federal licensing regime for sensitive laboratory equipment, requiring buyer verification, pre-purchase approval, ownership registration, and transfer tracking.

Early Outbreak Detection and Response

- Build an AI-enabled epidemic intelligence system that integrates the National Syndromic Surveillance Program (NSSP), the One CDC Data Platform, wastewater, bioaerosol, genomic, and clinical surveillance.
- Fund nationwide upgrades to wastewater and bioaerosol monitoring, including rural coverage and Biomedical Advanced Research and Development Authority (BARDA)-supported detection infrastructure.
- Standardize and approve mNGS diagnostics while securing scalable mRNA vaccine manufacturing capacity through government-backed private partnerships.

“In this age, in this world, the application of artificial intelligence will define the future, and our country must once again develop new capabilities, new tools, and, as General Eisenhower said, new doctrine.”

– Jake Sullivan, National Security Advisor, 2024 [1]

1. Introduction

By March 2020, SARS-CoV-2 had reached nearly every country in the world. Supply chains shattered, global markets collapsed, and public health systems buckled under the ensuing crisis. The world knew pandemics were possible and had been warned well in advance. It knew coronaviruses posed serious risks, with the potential to become more transmissible and deadly than a routine outbreak. There were existing precautions, institutions, and vaccine infrastructure to mitigate the threat of pandemics. Still, the world was unprepared.

Now, imagine that the world is hit with something it could not have expected. It is not another familiar pandemic produced by nature, but a plague, famine, or biological zero-day attack created by an individual with minimal training, only determination and technology. Such a threat would be difficult to foresee, nearly impossible to prepare for, and closer than policymakers assume.

Rapid advances in AI and biological manufacturing are making this threat increasingly real. These dual-use technologies expand the realm of possibility for breakthroughs in therapeutic discovery, but also scale the reach of possible harm. The same tools that enable new cures may also facilitate the engineering of a weapon. The danger is that innovation may outpace the guardrails meant to control it.

Prevention requires recognizing the threat before it arrives. The steps taken today will determine whether AI-biosecurity becomes manageable or catastrophic. AI development is moving quickly, and strategic competition with China makes American dominance essential. The United States cannot assume that rivals will accept the same ethical limits, nor can it sacrifice technological advantage in the name of caution. It must avoid a failure of imagination by building safeguards that reduce existential biological risk without constraining the innovation that gives the United States its advantage.

This report will discuss how AI and biological manufacturing intensify biosecurity risk, where current policy falls short, and what regulations can reduce biological threats, while preserving American technological dominance.

1.1 AIXBio Technology Stack

AIXBio refers to a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments related to human health and biotechnology innovations [2]. AIXBio's predictive capabilities, paired with faster biotechnology manufacturing, are transforming drug discovery, clinical trials, disease treatment, and the biological risk landscape [3].

The AIXBio technology stack operates through three layers: artificial intelligence, biological data, and biotechnology manufacturing. The **AI layer** generates predictions and designs, the **data layer** supplies the biological inputs that make those outputs useful, and the **manufacturing layer** turns digital instructions into physical outputs.

1.1.1 The Artificial Intelligence Layer

The artificial intelligence layer converts biological data into predictive outputs. In AIXBio, this layer uses AI systems to convert biological inputs into candidate targets and therapeutic designs. This layer can include large language models, biological foundation models, graph neural networks, generative models, molecular docking systems, and tools to predict absorption, distribution, metabolism, excretion, and toxicity (ADMET) [4].

AI's **large language models** and related machine-learning systems can learn statistical patterns from biological and chemical data, process large bioinformatics databases, optimize candidates against specific properties, and offer predictive outputs about potentially efficacious therapeutic candidates and targets. AIXBio's systems can be trained through an iterative trial-and-error process, learning to adjust assessments of novel therapeutic design [4].

This process is compute-heavy and nonlinear, often relying on **artificial neural networks (ANNs)**, a class of **machine learning (ML)** models. Loosely inspired by human neural networks, ANNs are computational models made of layers of mathematical units that learn statistical relationships in data. **Deep learning** uses multi-layer artificial neural networks and can involve supervised, unsupervised, self-supervised, semi-supervised, or reinforcement-learning methods [5, 6].

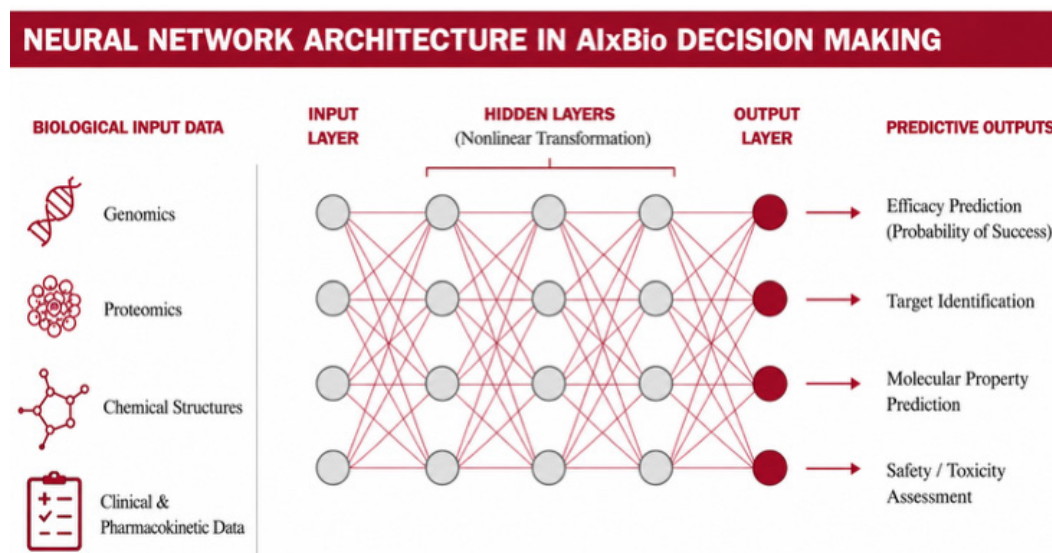


Figure 1: Neural network architecture involved in AIxBio decision-making processes. Adapted from Gupta, “Neural Network Layers Explained,” and modified by the authors for AIxBio applications.

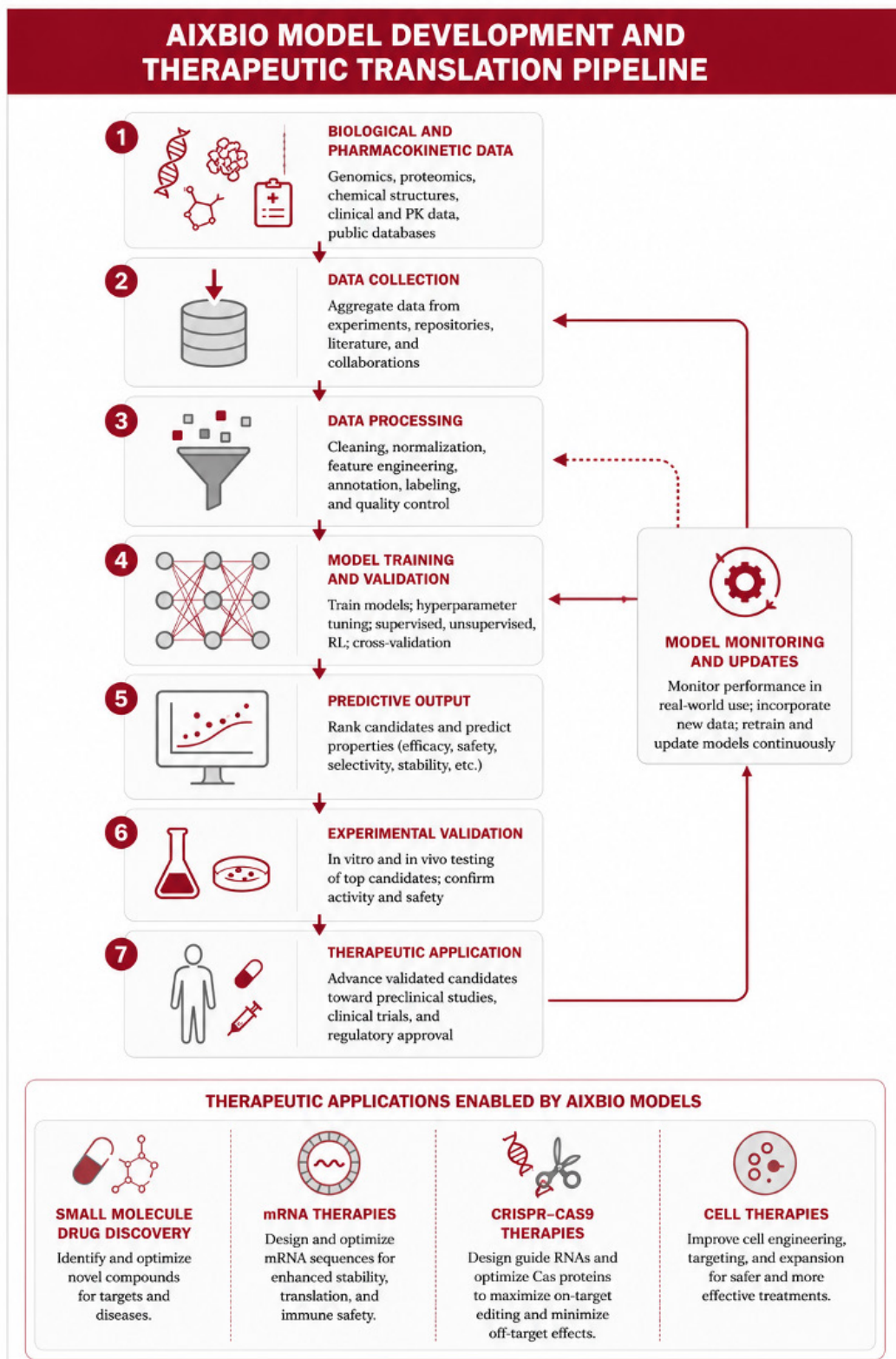


Figure 2: AlxBio model development and therapeutic translation pipeline. The figure shows biological and pharmacokinetic data moving through data collection, data processing, model training and validation, predictive output generation, experimental validation, therapeutic application, and model monitoring. Adapted from InfoDiagram's predictive AI model development process diagram and Zhang et al.'s generative mRNA design framework, and modified by the authors for AlxBio applications.

AIxBio's model-development process can be illustrated through the small-molecule drug development workflow. In machine learning, **training** is the process of optimizing model parameters to minimize an error function, allowing the model to learn patterns from development data [7, 8, 9]. **Tuning** involves adjusting hyperparameters or model configurations to improve performance before final evaluation [10]. The development dataset is typically divided into training, validation, and test data. Training data teach the model, validation data refine and check it, and held-out test data evaluate final performance [11]. Historical drug-discovery data and relevant parameters, including chemical structure, binding sites, gene sequence, and mRNA or protein targets, are provided to the ANN as training data.

The model is then tuned on subsets of the dataset to test how different configurations affect performance and to ensure the model responds consistently across smaller data samples [11]. Once model generation is complete, researchers evaluate its final performance with a dataset it had not trained on. Both the training and validation datasets would include information on approved drugs, including pharmacokinetic parameters, chemical structure, dosage, and in vivo binding sites. **Pharmacokinetic parameters** describe how a drug is absorbed, distributed, metabolized, and eliminated by the body [12]. The more accurate and diverse the biological datasets are, the higher the predictive power of the machine learning tool [12].

New computational biology models enable advancements in the evaluation phases by using artificial intelligence to predict functions and behaviors of biological structures. Two recent breakthrough examples are **AlphaFold 3**, which predicts biomolecular complexes, and **Evo 2**, which models genome-scale biological sequences [13, 14]. These tools can reduce development time and cost, allowing researchers to prioritize promising candidates in experimentation.

Any promising small molecules generated by AIxBio would still need to go through regulatory approval, including preclinical testing in animals and clinical trials in humans [14]. As a result, any AIxBio prediction that a novel drug candidate will be more effective remains uncertain until confirmed through laboratory testing and clinical validation [15, 16].

1.1.2 The Biological Data Layer

The biological data layer makes AIXBio useful through two main categories of data: human genomic and pharmacogenomic data, and pathogen or viral genomic data. Together, these datasets allow AIXBio systems to identify clinically meaningful patterns while also creating dual-use risks.

1.1.2.1 Human Genomic and Pharmacogenomic Data for Precision Medicine

Precision medicine (PM) is a major next-generation approach to human medicine, using genomic, molecular, clinical, and lifestyle data to tailor prevention, diagnosis, treatment selection, and dosing for each individual [17]. The development of PM is characterized by prevention, personalization, prediction, and participation [18].

The field of **translational bioinformatics** is key to PM: the merging of biology, computer science, and information technology. By tailoring therapies to patients' genomic and molecular data, PM enables improved and specialized treatment plans, generating enhanced diagnosis, prevention, treatment selection, and dosing. Precision medicine depends on large **bioinformatics databases** that include patients' genomic and molecular data, as well as **pharmacogenomic data** showing how treatment responses vary by genetic signatures, disease stage, age, sex, and other factors.

President Obama announced the *Precision Medicine Initiative* in 2015, and the National Institutes of Health (NIH) *All of Us* Research Program opened national enrollment in 2018 to collect health data from one million or more U.S. participants. These programs initially focused on cancer, with a longer-term goal of improving the understanding of how genes, environment, lifestyle, and health care affect health and disease across diverse populations [19, 20].

Human genomic data encompass the full DNA sequence of three billion base pairs, which contribute to an individual's physical traits and medicinal responses. **Pharmacogenomic data** describe how genetic variation affects response to therapeutic treatment, such as drug efficacy and dosing [21]. By combining individuals' genomic data across multiple population groups in the United States with electronic health records and surveys, researchers can

understand how genetically inherited and environmentally acquired traits impact health [22]. The data layer is stored internally, and individual-level private data are described as “anonymized”.

This database was an important step toward personalized medicine, helping tailor future treatments to match each person’s condition and physical profile. Through pharmacogenomics, clinicians could come closer to administering the optimal medication in the optimal dosage to each individual, mitigating the risk of a lack of response or the adverse effects that are commonly seen in traditional medicine [23].

However, a large-scale population database providing biological information on different U.S. population subsets puts them at biological risk as well. Examples of leaked genomic data and ancestry information have occurred [24]. Notably, in the 2023 *23andMe* data breach, genetic and ancestry data from millions of users were exposed by credential-stuffing attacks. When combined with AI-driven clustering, these data could be used to identify genetically similar subpopulations, increasing precision medicine capabilities and biosecurity risks [25].

Proteomics refers to the presence, abundance, modifications, and cross-interactions between all types of proteins expressed in an individual’s body [26]. In parallel to the genomic database, researchers are also building proteomic databases of protein biomarkers associated with specific conditions or diseases, gathered through sampling and testing from adult individuals. When coupling genomic sequencing with proteomics data, such as disease-specific markers, the linkage between genotypic markers and specific phenotypes emerges [27]. This mapping is a critical step toward precision medicine. Proteomics data are compiled through mass spectrometry and affinity-based protein profiling techniques for large-scale protein identification and analysis [28, 29].

Genetic and proteomics data collection plays a major role in both reducing health risks and treating disease. Millions of individuals carry inherited or developed mutations correlated with an increased chance of developing cancer or other life-threatening conditions throughout their lifetimes [30, 31, 32]. If genomic and molecular testing are performed early on in life and risks are mitigated through emerging precision gene and/or cell therapies or prophylactic treatment, many lives will be saved or at least prolonged [33, 34].

AIxBio is especially useful for classification and clustering, which can help identify genetic signatures linked to higher disease risk. However, population-level clustering can expose specific subgroups to biologically targeted risks, even though the goal is disease prevention. Population profiling is therefore plausible if large-scale pharmacogenomic databases are constructed and data are made publicly available. Targeted bioweapon design is feasible, but to date remains technically difficult. Monitoring precision medicine's evolution will shed light on the interplay between the medical benefit and emerging risk.

1.1.2.2 Pathogen Genomic Data for AIxBio Model Generation

Beyond human genomic and clinical datasets, AIxBio model development relies on large-scale pathogen and viral sequence databases, which expand the scope of analysis from individual health to population-level and cross-species biological systems.

The International Nucleotide Sequence Database Collaboration, or INSDC, is composed of three major public nucleotide sequence databases: National Center for Biotechnology Information (NCBI) GenBank, the DNA Databank of Japan, and the European Nucleotide Archive. These databases archive viral genomic sequence information and metadata, such as sample host species, location, date, and links to related publications. Demographic information, antiviral treatment data, and treatment histories are sometimes included, but are not consistently available across viral sequence records [35].

A recent report shows that the GPT-4o application programming interface (API) can help identify published studies linked to GenBank submission sets and extract relevant data from them [35]. This kind of streamlining could support the development of viral databases that combine genomic data, treatment information, and demographic details about infected populations.

1.1.3 The Biotechnology Manufacturing Infrastructure Layer

The biotechnology manufacturing layer translates AIxBio-generated designs into physical biological products through controlled chemical and biological processes. This layer encompasses the infrastructure and process optimization strategies required to scale from molecular design to deployable therapeutics.

Analytical instrumentation measures biological specimens and systems to determine their composition and functional characteristics. This category includes high-parameter flow cytometers, cell sorters, and liquid chromatography mass spectrometry instruments. These platforms can develop large biological datasets that can improve AIxBio model development [36].

Small-molecule manufacturing relies on fume hoods, flash chromatography systems (e.g., Biotage), and rotary evaporators during early-stage research, and transitions to reactors, extractors, evaporators, crystallizers, and filtration systems during process scale-up [37].

mRNA vaccine sequences are traditionally manufactured with the use of filtration setups, ion exchange, hydrophobic interaction, and size exclusion chromatography for purification, and tangential flow filtration setups for downstream concentration [38]. The linearized DNA templates used in mRNA synthesis consist of synthetic gene sequences produced through automated synthesis [39]. The Coalition for Epidemic Preparedness Innovations (CEPI) is exploring AI and machine learning to optimize decentralized, automated mRNA vaccine manufacturing. The goal is to move from centralized batch production toward modular, microfluidic-based systems [40]. Such a modular setup is expected to support rapid vaccine production in outbreak regions through end-to-end modular integration of the payload (mRNA) production with capsule (lipid nanoparticle) manufacturing.

DNA synthesis links deoxyribonucleotides into a single strand of DNA using DNA synthesis instruments. The first strand serves as a blueprint for the complementary strand synthesized by the DNA synthesis enzyme [41]. Emerging DNA synthesis methods include enzymatic DNA synthesis (EDS) and are shifting the paradigm from chemical synthesis of the template DNA strand to one carried by the natural enzyme [42]. mRNA is produced by transcribing a linearized DNA sequence, with RNA polymerase adding RNA nucleotides in the order specified by the DNA template [43]. Software is also part of this stack, helping convert digital nucleotide sequence information into instructions for constructing biologically active genetic components [44].

1.2 Civilian Applications

AIxBio's civilian applications will be most impactful in therapeutic development, where AI systems can make biological discovery more targeted and efficient. The technology can accelerate the development of viable treatment candidates, reducing the time and cost of early-stage development.

1.2.1 AI-assisted Small Molecule Therapeutics

Small molecule drugs are low-molecular-weight chemicals that account for 90% of the currently approved medications worldwide [45]. Despite their dominance, research and development (R&D) productivity has declined sharply: between 1950 and 2012, the number of approved drugs per \$1 billion in inflation-adjusted R&D funding fell by half roughly every nine years [46]. An AIxBio-driven boost in predicting novel small-molecule drug candidates would be highly desirable for the pharmaceutical sector.

Large language models are actively deployed for optimizing small molecule structures targeted at specific biological activities. However, there are still few comprehensive databases showing exactly how drugs bind to biological targets and produce therapeutic effects. Documented AIxBio use is still concentrated in preclinical research, accounting for almost 40% of studies. Later-stage use remains less common because validation becomes slower and more complex as candidates move closer to clinical testing [47]. This phenomenon highlights the transformative potential for AIxBio in early-stage drug discovery and identification of lead candidates.

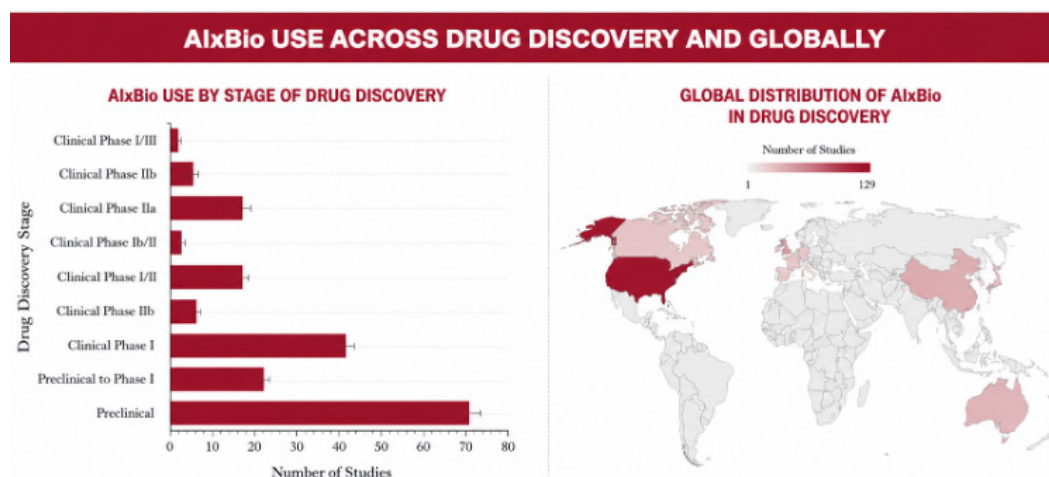


Figure 3: Categorization of AIxBio use per stage of drug discovery and validation (left). Global distribution of AIxBio in drug discovery (right). Adapted from Dermawan and Alotaiq (2025) and modified by the authors.

Consequently, investment in AI-assisted drug discovery is substantial in the United States, which is a major hub for AI development and advanced biotechnology firms [48].

Simultaneously, scientists have concluded that improving algorithms alone does not solve the scarcity of comprehensive databases of drug candidates suitable for lab testing. Limitations exist both in the data quality (data biases and noisy data) as well as method validation (unpacking of the performance gains and upgrading the robustness of testing) [12].

AI has already contributed to small-molecule drug discovery and repurposing. One example is baricitinib, a Food and Drug Administration (FDA)-approved AI-identified candidate for SARS-CoV-2 drug repurposing, and several other AI-discovered or AI-designed small-molecule candidates have already entered early-stage clinical trials [49].

Nevertheless, the clinical stage of the AIxBio-generated drug validation lasts a similar length of time as traditionally discovered drug candidates. Experts agree on the need for experimental validation at each stage of drug development and a hybrid human-AIxBio approach to technological evaluation. More comprehensive databases of drug testing, including both true positive and false negative candidates, built through expert crowdsourcing, could support faster drug-candidate discovery [49].

1.2.2 mRNA Therapies

mRNA vaccines recently emerged as a tunable, scalable, and efficient platform for viral infections, most notably SARS-CoV-2. The platform consists of the vehicle, lipid nanoparticles able to penetrate the cell membrane, and the cargo, mRNA ready to be translated into proteins. Once released inside the cell, mRNA generates an immunogenic protein that signals the immune system to mount a response against it. This immune response primes the patient's immune system to neutralize the virus/pathogen upon subsequent exposure [50].

mRNA sequences, albeit short compared to the human genome, exhibit high combinatorial diversity when conceived and synthesized *de novo*. For instance, there are an estimated 10632 ways to code for the SARS-CoV-2 spike protein sequence [51]. This astronomical number could not possibly be tested in a

laboratory setting, but could be dimensionally reduced through AIxBio's models to a smaller number of optimal mRNA structures to test for in the lab. The combinatorial diversity creates the need to match the mRNA coding regions with untranslated regions, creating an interdependency between optimization metrics of each component [52]. AIxBio models are accounting for this challenge.

A 2025 study highlights the development of a generative AI-driven framework, generative models for RNA (*GEMORNA*), for constructing the mRNA sequence targeting a specific protein. *In vitro* (outside the body) testing of the most effective mRNA shows an increase of up to 121-fold in mRNA expression compared to a benchmark. Platforms such as *GEMORNA* are expected to become increasingly more common [8].

1.2.3 CRISPR-Cas9 Therapies

CRISPR-Cas9 represents a gene-editing platform effectively equivalent to molecular scissors for repairing or modifying human DNA. The CRISPR platform operates by using a short guide RNA sequence as the targeting mechanism for the payload. This payload is the CRISPR enzyme, which cuts or modifies the specific gene sequence it is guided to [5, 53].

AIxBio has been used for more than a decade to improve predictions about CRISPR-Cas9 gene editing performance. At its core, AI primarily improves guide RNA (gRNA) design through a process similar to the mRNA optimization described above. Additionally, the protein structure of Cas9 undergoes iterative AI-based optimization [5].

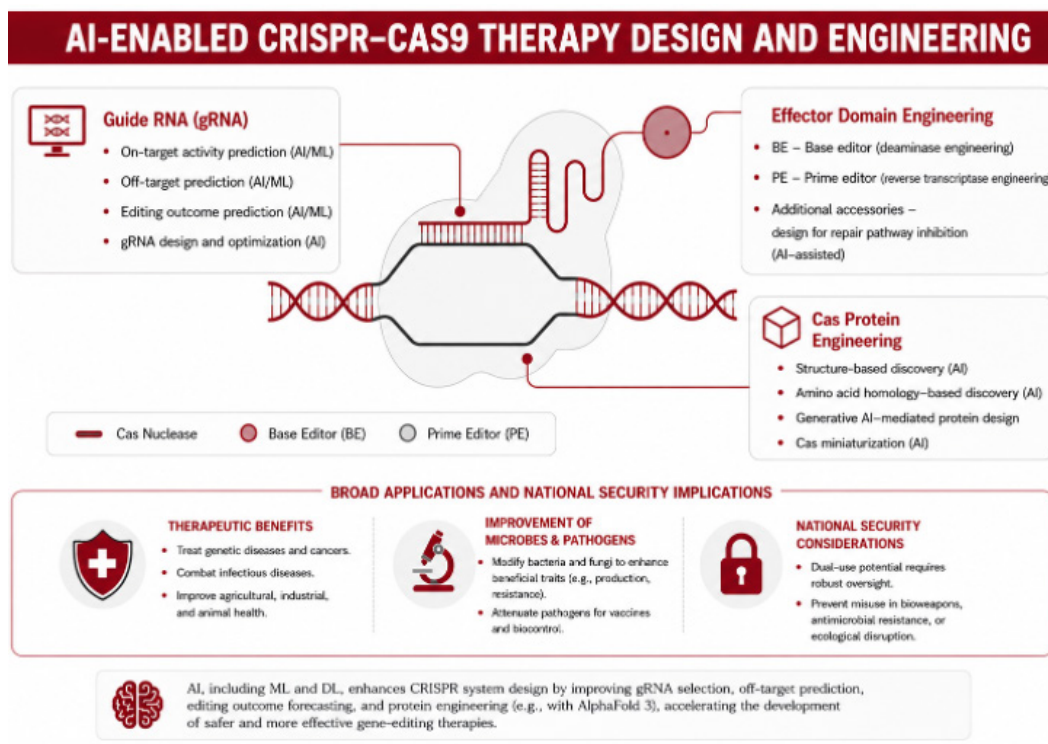


Figure 4: AI-enabled CRISPR-Cas9 design and engineering framework. Machine learning (ML) and deep learning (DL) models enhance guide RNA design, off-target prediction, editing outcome prediction, and Cas protein engineering. These capabilities support applications across therapeutic development, microbial engineering, and pathogen modification, with dual-use and national security implications. Adapted from Experimental & Molecular Medicine (2025) and modified by the authors.

Multiple CRISPR therapies are undergoing clinical trials. The only FDA-approved therapy as of August 2026 remains *Casgevy*, an ex vivo CRISPR-Cas9 therapy that edits a regulatory element of the BCL11A gene in a patient's blood stem cells to increase fetal hemoglobin production [54].

1.2.4 Cell Therapies

Cell therapies include the transplant, transfusion, or tissue grafting using cells from the patient or a donor for the purpose of restoring normal function [55]. Although cell therapies are already used in personalized treatment, AI/ML development in this field remains limited by the lack of comprehensive training datasets and the difficulty of continuously monitoring living cells' response. Part of this challenge comes from assessing the performance of therapies in live cells, a barrier Harvard scientists came close to addressing in 2025 [56]. Advances in combining AI with regenerative biology are expected over the next few years through high-risk pilot projects [57].

Preliminary reports suggest that AI may accelerate cancer-treatment research and development based on a previously existing chimeric antigen receptor T-cell therapy (CAR-T) treatment platform for specific on-site tumor cell targeting [58]. However, AI's predictive power is limited by the availability of the well-established therapeutic CAR-T platform and the biological database of model training and validation. Coupling AIxBio with the CRISPR-Cas9 editing platform for designing chimeric antigen receptors (CARs) could foster the transition from a constrained made-to-order model for cell therapies to a broader and tunable platform for on-demand specific therapeutic manufacturing [59, 60].

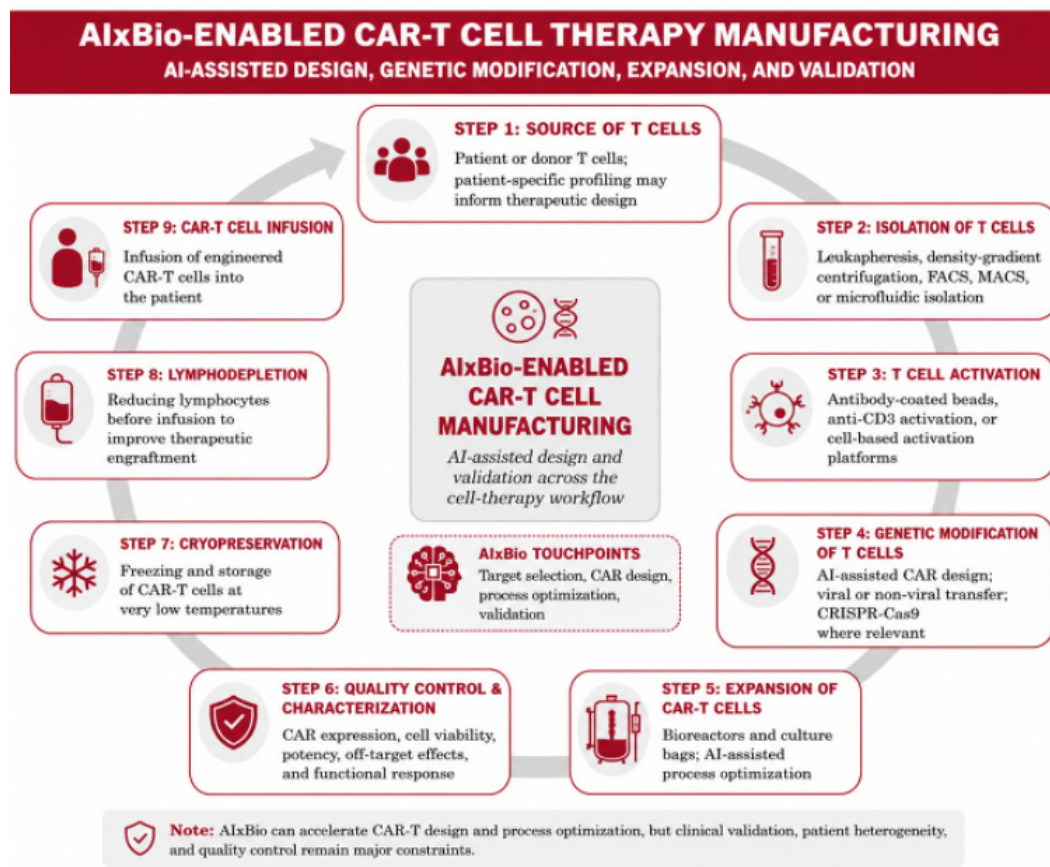


Figure 5: AIxBio-enabled CAR-T cell therapy manufacturing workflow. Adapted from Colina et al.'s overview of CAR-T cell manufacturing steps and modified by the authors.

1.2.5 Metagenomic Next-Generation Sequencing

Next-generation sequencing refers to the high-throughput sequence identification of billions of nucleotide base pairs, producing readouts much faster than classical sequencing methods. **Metagenomic next-generation sequencing** yields sequence readouts without requiring prior knowledge of the organism of origin in a high-fidelity way, meaning newly emerging pathogenic sequences, if present, can be detected in human samples [61].

The main advantage of the mNGS technology lies in its lack of bias toward unprecedented pathogenic infections, because mNGS does not require background knowledge on a specific pathogen [62]. Emerging mNGS platforms could provide real-time information on bacterial detection and genotyping within minutes [63]. The shotgun variation of mNGS has the advantage of simultaneously identifying viruses, bacteria, fungi, and parasites in a sample, making it useful for deconvoluting co-infection cases [64]. The information gathered from shotgun mNGS could be further applied in profiling antibiotic resistance in bacteria and virulence genes of emerging pathogens [63, 65, 66].

For an active mNGS deployment, standardization across sample types, quantity of host DNA, the sequencing platform used, number of reads generated, selected reference database, and data analysis tools are necessary [67]. Despite cost and expertise constraints, long-term investment is justified by the potential to dramatically improve detection of novel pathogens, including those maliciously generated with AIxBio.

1.2.6 Readiness and Validation Bottlenecks

In civilian applications, AIxBio's impact will depend on translation from model prediction to experimentally validated products. A major advance in AIxBio may come from unsupervised deep learning, which could allow models to detect hidden patterns in biological data and identify potential therapeutic candidates with less reliance on labeled datasets, although experimental validation would still be required [59].

The **technology readiness level (TRL)**, which measures the technology's maturity, is particularly challenging for emerging AIxBio, because products still face clinical-testing and clinical-trial validation. Common clinical-trial hurdles include patient heterogeneity, multiyear monitoring periods, and noncompliance with treatment protocols. AIxBio remains constrained by the quality of its training data, with bottlenecks arising from batch effects that reflect processing artifacts rather than true biological signals, inconsistent measurement protocols, and inadequate metadata documentation [68, 69, 70]. AIxBio also performs best when applied to biological systems that are already well understood, making it less reliable for studying new or poorly understood biology.

1.3 Misuse Potential and National Security Consequences

AI-enabled biotechnology poses two converging dangers: it democratizes the development of existing biological threats by reducing reliance on tacit knowledge, and it creates new threat pathways through improving pathogen design and delivery. Together, these capabilities heighten the risks of terrorism, coercion, sabotage, targeted attacks, and broader national security disruption.

1.3.1 AI-Enabled Democratization of Existing Bio Threats

The major foreseeable biological threat with AI is the acceleration and democratization of bioweapon manufacturing. Non-state or lone actors, such as criminals or terrorists, and malicious state actors can use prompt obfuscation and open-source, jailbroken, or internally built LLMs throughout the development process to substitute for tacit knowledge.

Tacit knowledge is the intangible know-how, like using a micropipette or douncing HeLa cells, that people acquire by working in laboratory environments. For decades, technology and the internet have eroded the importance of tacit knowledge in scientific work, cutting the learning curve for non-professionals to perform tasks previously requiring decades of experience [71].

Artificial intelligence will likely accelerate this phenomenon. Leading LLMs are already outperforming human experts in tests designed to assess virology knowledge [72]. A nonexpert could theoretically use an unrestricted LLM for assistance in scientific reasoning, accelerated search and synthesis of data and research, navigating computing tools, troubleshooting, and testing across a complex technical workflow. This substitution would not immediately replace hands-on expertise entirely, but it could lower cognitive and informational barriers that once slowed inexperienced actors [72, 73, 74].

In bioterrorism cases like Bruce Ivins, the possible perpetrator of the 2001 Anthrax letter attacks, actors often come from senior, specialized research backgrounds with access to scientific equipment, laboratories, pathogens, and the tacit know-how needed to work with them. As AI reduces the barriers to informal development, that background may no longer be a strict requirement [73].

1.3.2 Emergence of New Biological Threat Pathways

The democratization of biotechnology development will be compounded by the unforeseen threats emerging from new biotechnology and enhanced AI capabilities. The realm of possibilities will expand in the coming years, including novel methods for developing, delivering, and increasing the virulence of pathogens. Malicious actors may be able to increase the transmissibility, lethality, host range, and immune evasion of existing microorganisms, including ones that are currently harmless [75].

Gain-of-Function Pathways for Designing and Modifying Novel Pathogens

- AI models may enable the creation of novel biological molecules, including toxins, pathogen-associated proteins, and proteins that interact with critical targets in the human body [75].
- Bacterial and fungal candidates may be modified using CRISPR-based and related gene-editing methods [76, 77].
- AI-enabled construction of viruses may soon be possible, as scientists in 2025 designed bacteriophage genomes computationally, synthesized them into DNA, and introduced them into bacterial hosts, yielding phages that infected *E. coli* [78].

Potential novel delivery mechanisms magnify the threat of enhanced pathogen capabilities by introducing harmful biological payloads into hosts and reducing the technical barriers to delivery. For example, technologies, such as CRISPR, could theoretically offer pathways for *in vivo* delivery using vectors to introduce malicious gene-editing payloads into target cells and exploit genotype-linked susceptibilities in specific individuals. Adenoviral vectors are already used to deliver CRISPR, but a hypothetical adenovirus-based CRISPR system capable of spreading beyond the intended recipient would present a serious biosecurity concern, unlike standard therapeutic vectors, which are typically engineered to be replication-deficient [79, 80]. Further, recent advances in non-viral oral delivery methods for CRISPR suggest potential future avenues for using emerging biotechnology to threaten national security [81].

1.3.3 National Security Risks

Use cases for these enhanced AIxBio threats and delivery methods carry serious national security implications. When combined with the data layer mentioned in Section 1.1.2, it could be possible to target specific individuals or subpopulations with specific genetic traits [82]. Over time, AI could further optimize biological attack scenarios by enabling malicious actors to model transmission dynamics and identify vulnerable populations.

Non-state and lone actors could employ these methods for terrorism, targeted killings, or a biological extortion scenario while threatening bioweapon release. State actors developing these novel bioweapons may accidentally release them or deliberately conduct disruption and sabotage operations to achieve broader political or military objectives. Similar capabilities could also be directed against crops and livestock to create food supply shocks with downstream national security impacts.

As of 2026, the development of these biotechnologies remains dependent on laboratories, specialized instrumentation, trained personnel, and scientific infrastructure. Even with these constraints, workarounds are possible through insider threat access and supply-chain compromise. A cyberattack on a laboratory, including an AI-enabled one, could also cause an incident, such as the accidental release or synthesis of a pathogen. AI may also increase the risk that malicious actors circumvent existing nucleic acid screening safeguards when ordering synthesized DNA [83]. Advances in artificial intelligence may reduce the need for some of these inputs, and governance cannot wait until these material constraints are made obsolete.

2. AIBio Risk Trajectory

This section assesses how AIBio risk changes as models improve, biological data become easier to use, DNA synthesis access expands, and wet-lab automation advances. It also evaluates whether governance can contain misuse pathways. The trajectory is outlined on a stepwise timeline, beginning with a current natural-outbreak baseline and moving through near-term and medium- to long-term AIBio-enabled scenarios. Across each stage, the assessment considers whether AIBio capabilities increase the likelihood, impact, speed, or controllability of a possible infectious epidemic or pandemic.

Risk in this scenario is ranked using the Risk Assessment Matrix below, which weighs likelihood against expected impact. Scores range from 1 to 5, with 1 representing a low-likelihood, manageable event and 5 representing a likely scenario with severe public health or security consequences. Likelihood is assessed as low when the scenario is 0 to 10% plausible within the timeframe, medium at 10 to 40%, and high above 40%. Impact is assessed as low when effects are localized and manageable, medium when consequences are material for public health, research, or security, and high when consequences rise to severe epidemic, national-security, or catastrophic risk. The ranking also reflects whether available governance and operational controls are likely to contain the threat before it escalates.

Emerging Biological Threat Risk Outlook

PRESENT

0 TO 2 YEARS

2 TO 5+ YEARS

2.1 Current Risk Baseline

Risk level



Core drivers

- Humanitarian, climate, environmental, and geopolitical stress raise exposure.
- Pandemic history shows surveillance, governance, and response gaps.
- Zoonotic spillover remains the dominant baseline hazard.
- Scenario concern: long incubation, weak signal, delayed tracing.
- Operational race: isolation and tracing versus invisible spread.
- Missing capability: field bioaerosol detection and rapid metagenomic sequencing.

2.2 Near-Term Outlook

Risk level



Core drivers

- AI agents enter biological discovery workflows.
- RAG and NLP improve access to tacit biotech know-how.
- Open-source AIxBio models raise dual-use screening pressure.
- Uneven nucleotide procurement controls leave external outbreak risk.
- Watch: data bottlenecks, guardrails, and predictive power.
- Primary concern: design pathways outpace governance.

2.3 Medium/Long-Term Outlook

Risk level

Unmitigated



Mitigated



Core drivers

- AI-guided workflows mature while validation data remains limiting.
- mRNA, CRISPR, cell therapy, and small-molecule design expand.
- Oversight grows for enhanced virology and high-containment labs.
- Threats may shift toward synthetic toxins and resistant bacteria.
- Population genomic data becomes critical infrastructure.

Risk Assessment Matrix

		IMPACT		
		LOW	MEDIUM	HIGH
		Limited operational disruption; localized effects.	Material public health, research, or security consequences.	Severe national security, epidemic, or catastrophic risk.
LIKELIHOOD	LOW 0-10% plausible within timeframe	1	2 2.1 Current Baseline	3
	MEDIUM 10-40% plausible within timeframe	2	3 2.2 Near Term 2.3 Mitigated	4 2.3 Unmitigated
	HIGH 40%+ plausible within timeframe	3	4	5

2.4 Risk Accelerants and Indicators

- Public biological data released for model training.
- Compromised genomic population databases.
- Open-source high-performance AIxBio tools for gain-of-function prediction.
- Poorly regulated nucleotide sequence procurement.
- International regulatory, oversight, and accountability gaps.

2.1 Current Risk Baseline

Natural Outbreak: Medium Impact, Low Likelihood

Risk Level: 2/5

This section assesses the likelihood of an emerging epidemic under current global mobility and geopolitical conditions. The risk baseline scenario identifies operational hazards that could worsen an emerging biological threat without AIxBio involvement.

The escalating climate crisis, environmental degradation, and increasing geopolitical instability increase the risk of health emergencies and put the most financially insecure populations in greatest danger [84]. The impact of an infectious epidemic is evaluated as medium.

The COVID-19 pandemic exposed critical gaps in global health governance, showcasing the missing strategies for preventing, detecting, responding, and containing an outbreak. According to the World Health Organization (WHO) director, “epidemics of SARS, H5N1, H1N1, MERS, Ebola and Zika have emerged, only to be followed by a pattern of panic and neglect, in which concern during emergencies gives way to apathy and underinvestment in their aftermath” [84].

The baseline resembles the pre-COVID-19 risk environment, where zoonotic spillover remains the largest concern. The WHO R&D Blueprint identifies priority pathogens with epidemic or pandemic potential [85, 86]. The 2018 R&D blueprint included information on the respiratory viruses MERS and SARS, with the latter emerging into the COVID-19 pandemic [85]. These viruses constitute emerging threats because unintentional spread from animals to humans is possible. For 2026, the assessment rates the likelihood of an emerging epidemic or pandemic akin to the COVID-19 pandemic as low [87].

Examples, such as the 2026 cruise ship hantavirus outbreak, point to risks in misdiagnosing the first carriers of infectious diseases [88]. Prolonged incubation periods and limited test sensitivity among asymptomatic or presymptomatic individuals make early outbreak responses difficult to calibrate, risking either overbroad restrictions or insufficient containment [89]. If asymptomatic transmissibility is underestimated, officials may miss the point at which local spread becomes exponential epidemic growth. Officials categorize contacts by

exposure risk, and isolation guidance evolves as more outbreak data become available [90, 91, 92].

Containment depends on whether isolation measures can move faster than undetected viral spread before cases grow exponentially. The risk is operational, and the global strategic preparedness response determines whether outbreak spread is stalled before it becomes an epidemic. In this scenario, field-ready bioaerosol detection tools are not yet available. These include low-cost metagenomic sequencing platforms for rapid pathogen detection and outbreak response, discussed in Section 4.3 [93].

2.2 Near-Term Outlook (0 to 2 Years)

AIxBio-Enabled: Medium Impact, Medium Likelihood

Risk Level: 3/5

By late 2027, AI agents will be increasingly integrated into biological research tools. In this scenario, LLMs continue to improve, validation data from labs are fed into algorithms for reinforcement learning, and automation steadily replaces humans in the scientific discovery loop [72]. Higher-fidelity AIxBio tools shorten the path from research goal to computational design to biological manufacturing. While this enables significant breakthroughs in novel therapies, the fewer rounds of trial-and-error also make the likelihood of a biological weapon assisted by AIxBio design more plausible than ever before.

Large genome models, such as *Evo 1* and *Evo 2*, were developed to advance biological sequence modeling and support therapeutic discovery, but they also showcase AIxBio's ability to lower the barriers to harmful pathogen design [78]. Given the nature of the open-source code and models, ethical concerns arise over such AIxBio tools accelerating the design and production of a biological weapon.

Additionally, AI retrieval of well-sourced tacit biotechnology knowledge will increase. Retrieval-augmented generation (RAG) will expedite the search and cross-referencing of a large body of academic research papers and laboratory protocols, becoming more precise at teaching an outsider the know-how of an expert [94]. Moreover, the enhanced natural language processing (NLP) ability of commercial AIxBio will only facilitate the acquisition of expert knowledge by someone without any technical expertise [72].

As a result, the estimated risk of an AI-accelerated bioweapon production depends on the predictive accuracy of LLMs and assistive models. The highest risk across the emerging technologies is represented by the novel viral sequences generated by open-source models. On the manufacturing side, in the absence of a binding framework for control over nucleotide sequences, operational biosecurity risks arise from failing to identify dangerous actors early enough.

Simultaneously, tightening control over domestic nucleic acid sequence procurement transfers the risk to a strategic one: not being prepared for an externally generated viral outbreak. Without international consensus on biotechnology nonproliferation, limitation of Biological Safety Level 4 (BSL-4) labs, and clear oversight of high-containment laboratories, non-state actors' capabilities remain uncertain [95]. The primary risk is that politically motivated actors could generate novel viruses with high transmissibility and broad, nonspecific population effects.

The next two years will be critical for assessing three key factors: 1) AIxBio data bottlenecks; 2) insufficient guardrails for AIxBio use and its international nonproliferation regulation; 3) AIxBio's predictive power. The future of public health and policymaking will depend on whether effective AIxBio guardrails can keep pace with the rapid growth of biological know-how. As AIxBio's TRL evolves, tacit knowledge improves, and predictive power expands, the unmitigated risk level is an estimated 3/5.

2.3 Medium- to Long-Term Outlook (2 to 5+ Years)

AIxBio-Enabled (Unmitigated): High Impact, Medium Likelihood
Unmitigated Risk Level: 4/5

AIxBio-Enabled (Mitigated): Medium Impact, Medium Likelihood
Mitigated Risk Level: 3/5

Wet-lab biological workflows with increasing automation and AI-based model validation capacity will develop over the coming years [72]. AIxBio's capabilities are projected to exceed human-level performance. However, progress will remain limited by the slow accumulation of biological validation data.

Predictive modeling of a broader range of emerging biotechnologies, including mRNA-based therapeutics, CRISPR-Cas9-based editing tools, more generalized cell therapies, and better-designed small molecule pharmaceuticals, will reshape the landscape of traditional medicine toward AI-guided and precision medicine. Broad access to open-source LLMs, genomic data, and molecular data increases the risk that legitimate medical research tools can also support novel pathogen design.

At the same time, a better understanding of the AIxBio TRL will emerge. Policymakers and public health officials will optimize the regulatory biosafety frameworks and impose guardrails on AI-enabled biological proliferation risks. Significant regulatory oversight of the enhanced virology capabilities of AIxBio and gain-of-function research will advance.

The threat landscape could shift toward *de novo* harmful small-molecule toxins (akin to biotoxins but lab-generated) or bacterial infections with abnormal resistance. In the landscape of infectious-disease treatment design, AIxBio will continue to be a double-edged sword.

Outside nonspecific infectious pathogen generation, pharmacogenomic patient data could become a critical national security asset. If non-state actors can cluster populations by inherited or acquired genetic signatures, they may gain tools for targeting specific population subsets.

The unmitigated risk level is estimated at 4/5, driven by overreliance on AIxBio and a shift toward workflows that remove human review from the loop. The mitigated risk level drops to 3/5, as procurement of potentially harmful biomaterial will face tighter regulations. Similarly, a thorough assessment of AIxBio's capabilities in novel viral prediction should impose guardrails on open-source AI models. International regulation will continue to evolve and better regulate pandemic-level threats.

2.4 Risk Accelerants and Indicators

The following risk accelerants are assessed against the current biotechnology stack, the projected development of AIxBio capabilities, and the strength of existing biosecurity and nonproliferation rules:

- **Bottleneck removed by public release of high-value biological training data:**
The availability of genomic sequences from model organisms is reshaping the

genome-function predictions. Data fed into platforms, such as *Evo 2*, will evolve to predict gain-of-function gene modifications and achieve specific biological outcomes. Some linkage predictions will be necessary for precision medicine advancements; others point to increased pathogenicity of a *de novo* virus. Decoupling beneficial from harmful in terms of biological data use for LLM training is not straightforward.

- **Compromised genomic population databases:** Advancements in precision medicine through the buildup of population genomic databases are not secure against leaks and misuse by outsiders. Population clustering based on genetically inherited or environmentally acquired signatures exposes individuals to targeted bioweapons.
- **Open-source highly performant AIxBio tools for gain-of-function prediction:** Tools, like *Evo 2* and *AlphaFold 3*, maintain the academic norm of open release and are made available to the general public. The code inside these platforms could be tuned by malicious actors to obtain harmful gain-of-function effects of novel nucleotide or protein sequences.
- **Poorly regulated nucleic acid synthesis procurement on a national basis:** Lack of U.S. regulatory control over the private sector's nucleic acid synthesis procurement (discussed in Section 3.2) leaves an opening for any gain-of-function biological assembly. Voluntary control checkpoints vary on a case-by-case basis and do not prevent a malicious target assembly. Federal agencies face operational challenges in tracking a multitude of biological orders and determining which orders are potentially harmful.
- **International regulatory, oversight, and accountability gap in biological nonproliferation:** International regulation, mainly through the Biological Weapons Convention, is decentralized and operates on mutual trust that state actors will block the development and stockpiling of bioweapons [96]. Through AIxBio, non-state actors will gain unprecedented biomanufacturing know-how, and durable biological weapons nonproliferation enforcement mechanisms are missing.

3. AIBio Governance Gaps

AIBio governance suffers from fragmented oversight, as U.S. oversight is divided among agencies, executive orders, voluntary standards, and state laws. Poorly calibrated regulation could hinder biomedical innovation and weaken U.S. AI leadership, making effective oversight difficult. Foreign model users and developers may operate under different or weaker rules, creating spillover risks beyond U.S. legal control. This fragmentation produces three major regulatory deficiencies: insufficient frontier-model safeguards, DNA synthesis screening requirements, and early outbreak detection and response.

3.1 Insufficient Mandates for Built-In AI-Biosecurity Safeguards in Frontier Models

Although their models may have catastrophic biosecurity implications, companies are primarily oriented toward expanding model capabilities rather than safeguards. Academic studies are similarly misaligned, with less than three percent of AI publications focused on safety. This imbalance is compounded by the limited number of binding safety mandates governing frontier models [97].

AI models are safer when they use built-in safeguards that can prevent malicious misuse. These safeguards include technical, behavioral, operational, and governance controls embedded across the model and deployment environment: robustness against adversarial inputs, refusal behavior, jailbreak resistance, usage monitoring, automated enforcement, restricted permissions, and Know Your Customer (KYC) checks [98, 99]. Another potential safeguard is mandated model-weight security standards to protect the learnable parameters that contain a frontier model's core capabilities from theft, leakage, uncontrolled release, or use outside the developer's safety architecture. These protections are important because, once model weights are accessed outside controlled deployment systems, safeguards, such as refusal behavior, usage monitoring, and access restrictions, may be weakened or bypassed [100].

Despite this need, the U.S. government lacks the existing legal authority to provide comprehensive frontier AI oversight. Although federal agencies can partially regulate frontier AI under authorities, such as the Defense Production Act, the Export Administration Regulations, and the International Emergency Economic

Powers Act, comprehensive oversight would require new legislation. Furthermore, because these standards are not codified by Congress, any requirements imposed under them can be revised or rescinded by a subsequent administration. Consequently, the federal framework remains fragmented, lacking a single AI-biosecurity regulator, licensing authority for frontier models, mandatory pre-deployment review, mandatory third-party audits, a federal incident-reporting baseline, and clear stop-deployment power [101].

As of August 2026, the U.S. government has not passed a sweeping, federal statute related to AI use and biosecurity. Instead, oversight relies on limited state legislation, voluntary standards, and agency guidance [102].

3.1.1 Shortcomings of Voluntary Self-Regulation

Voluntary self-regulation is important to mitigate risk, as AI developers understand the technology more than the government can. However, they will invoke these restrictions insofar as they improve their public reputation, prevent regulators from imposing tougher restrictions, and reduce legal liability [103]. These firms effectively make policy choices with public consequences while operating within corporate governance structures and remaining beholden to shareholders and profit incentives, not society at large. This misalignment means the social costs of unsafe or premature deployment are not fully reflected in their decision-making. Internal restraint is costly to oversee and enforce, and can slow deployment and limit innovation. Because of heavy competition and market pressures, AI developers have strong reasons to adopt only those constraints consistent with their commercial interests rather than the level of restraint the public interest may require [104]. Regardless, some firms have made voluntary statements, but their effectiveness and binding force are uncertain.

In its April 2025 *Preparedness Framework*, OpenAI, the *ChatGPT* developer, stated that it uses capability testing, internal review, disclosure commitments, and safeguard thresholds that can delay or block deployment at higher risk levels. This oversight framework defined High and Critical risk levels for the model's ability to facilitate biological weapons development, along with the thresholds that would trigger self-imposed restrictions. However, the framework notably includes a clause that would allow OpenAI to adjust its constraints if a competitor deployed a model without equivalent protections [99].

By contrast, Anthropic, the developer of *Claude*, maintains a *Responsible Scaling Policy*. Anthropic's oversight framework defined capability thresholds for Claude's potential to enable non-novel and novel chemical and biological weapons production, which would trigger corresponding safeguards and deployment restrictions. Notably, Anthropic does not use a competitor adjustment clause like OpenAI [105]. While Anthropic's safety policies are stronger than OpenAI's, its adherence to these standards depends on the company's governance structure and commitment to its mission.

These limitations indicate that voluntary corporate commitments are an insufficient safeguard against AI-enabled biological threats. These commitments are revocable and non-transparent, with self-defined thresholds, non-standardized methods, and compliance vulnerable to competitive pressure.

3.1.2 U.S. Federal AI Biosecurity Regulation Efforts and Absence

In 2023, President Biden issued Executive Order (EO) 14110: *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. This order directed agencies, such as NIST, the Department of Energy (DOE), the Department of Homeland Security (DHS), and the Department of Commerce (DOC), to develop standards, studies, frameworks, and evaluation tools for high-risk AI, including red-teaming and auditing to assess how advanced models could enable biological weapons risks. It also invoked Defense Production Act authorities to require model developers to report on models trained with biological sequence data and potential opportunities for AI-enabled biological misuse [2].

In 2025, President Trump rescinded EO 14110 with EO 14148, *Initial Rescissions of Harmful Executive Orders and Actions*. He then issued EO 14179, *Removing Barriers to American Leadership in Artificial Intelligence*, which did not directly address biosecurity risks [106, 107]. In July 2025, the Administration's *AI Action Plan* contained biosecurity-related recommendations for AI models, including DOC-led evaluations of frontier-model risks involving biological weapons [108].

The AI Action Plan also attempted to deter state AI regulation by urging federal agencies to weigh states' AI regulatory regimes in funding decisions, reducing funding where regimes were viewed as restrictive [108]. This stance was formalized in EO 14365, *Ensuring a National Policy Framework for Artificial*

Intelligence [109]. Regardless, California and New York enacted SB 53 and the RAISE Act in 2025, respectively, both imposing transparency, safety frameworks, and incident-reporting requirements on large frontier AI developers to address catastrophic risks [110, 111].

In June 2026, the administration issued EO 14409, *Promoting Advanced Artificial Intelligence Innovation and Security*. However, the order is limited to model cybersecurity provisions, lacking a binding effect on private developers or AIxBio-specific safeguards [112].

Since 2023, Members of Congress have also introduced several bills with AI-biosecurity provisions that did not advance, including the 2023 *Artificial Intelligence and Biosecurity Risk Assessment Act* [113], the 2023 *Strategy for Public Health Preparedness and Response to Artificial Intelligence Threats Act* [114], and the 2025 *Strategy for Public Health Preparedness and Response to Artificial Intelligence Threats* [115]. Of note, the *Generative AI Terrorism Risk Assessment Act* passed the House in 2025 and had provisions that would require DHS to assess terrorist use of generative AI for recruitment and chemical, biological, radiological, and nuclear (CBRN) capabilities. However, it did not establish mandatory AI-biosecurity controls or model-security standards [116].

The Trump Administration’s innovation-centered approach to AI regulation is light on mandates, imagining AI development as a “race” against adversaries. With this perspective, any restriction may create a disadvantage for American developers building what could prove to be a transformative technology with consequential military and national security applications [107, 108].

U.S. Federal AI-Biosecurity Governance Actions, 2023–2026

EXECUTIVE ACTION

YEAR	TITLE	AI-MODEL BIOSECURITY COVERAGE	NUCLEIC ACID SYNTHESIS SCREENING COVERAGE	LEGAL MECHANISM	STATUS
2023	EO 14110 Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence	●	●	Executive directive Agency-wide AI mandates	RESCINDED
2023	HHS Screening Guidance Screening framework guidance for providers and users of synthetic nucleic acids	○	●	Agency guidance Voluntary screening standard	FINAL GUIDANCE
2023	U.S. AI Safety Institute / AISI NIST-led AI Safety Institute and AI Safety Institute Consortium	●	○	Advisory forum Standards and testing body	RENAMED CAISI
2024	OSTP Screening Framework Framework for nucleic acid synthesis screening	●	●	Funding condition Federal awards condition	UNDER REVISION
2024	DURC/PEPP Policy USG policy for oversight of dual-use research of concern and PEPP	○	○	Funding condition Federal research oversight	UNDER REVISION
2024	DHS AI-CBRN Risk Report Reducing the risks at the intersection of AI and CBRN threats	●	○	Advisory report Report to Congress	DELIVERED
2024	NIST SP 800-218A Secure software development practices for generative AI and dual-use foundation...	●	○	Agency guidance Technical guidance	FINAL GUIDANCE
2024	AISI Model-Testing MOUs Pre- and post-release model access with OpenAI and Anthropic	●	○	Voluntary agreement Lab-government MOUs	ACTIVE
2024	AI National Security Memorandum Memorandum on advancing U.S. leadership in artificial intelligence	●	●	Executive directive National security directive	ISSUED
2024	TRAINS Taskforce Interagency testing of AI risks, including biological and chemical security	●	○	Advisory forum Interagency testing forum	ACTIVE
2025	EO 14148 Initial rescissions of harmful executive orders and actions	○	○	Executive directive Revokes EO 14110	ACTIVE
2025	EO 14179 Removing barriers to American leadership in artificial intelligence	●	○	Executive directive Directs AI action plan	ACTIVE
2025	NIST AI 800-1, 2nd Draft Managing misuse risk for dual-use foundation models	●	○	Agency guidance Draft technical guidance	DRAFT
2025	EO 14292 Improving the safety and security of biological research	●	●	Executive directive Orders biosecurity review	ACTIVE
2025	CAISI Center for AI Standards and Innovation	●	○	Advisory forum Federal testing center	ACTIVE
2025	America's AI Action Plan Winning the AI Race: America's AI Action Plan	●	●	Advisory roadmap Policy roadmap	ROADMAP

LEGISLATIVE ACTION

YEAR	TITLE	AI-MODEL BIOSECURITY COVERAGE	NUCLEIC ACID SYNTHESIS SCREENING COVERAGE	LEGAL MECHANISM	STATUS
2023	S. 2346 Strategy for Public Health Preparedness and Response to AI Threats Act	●	○	Proposed bill Would bind if enacted	EXPIRED / NOT ENACTED
2023	S. 2399 / H.R. 4704 Artificial Intelligence and Biosecurity Risk Assessment Act	●	○	Proposed bill Would bind if enacted	EXPIRED / NOT ENACTED
2024	H.R. 9194 Nucleic Acid Standards for Biosecurity Act, 118th Congress	●	●	Proposed bill Would bind if enacted	EXPIRED / NOT ENACTED
2024	H.R. 9626 AIxBio Defense Sandbox Act for secure AI-on-bio-data testing	●	○	Proposed bill Would bind if enacted	EXPIRED / NOT ENACTED
2024	FY25 NDAA, Secs. 236 / 6503–6504 DOD AI-biotech pilot, biological data, and NSA AI security center	●	○	Binding law Enacted statute	ENACTED
2025	S. 501 Strategy for Public Health Preparedness and Response to AI Threats Act	●	○	Proposed bill Would bind if enacted	INTRODUCED
2025	S. 1085 Medical AI-enabled pandemic preparedness and response program	●	○	Proposed bill Would bind if enacted	INTRODUCED
2025	H.R. 1736 Generative AI Terrorism Risk Assessment Act	●	○	Proposed bill Would bind if enacted	PASSED HOUSE
2025	S. 1387 / H.R. 2756 National Biotechnology Initiative Act, AI tools and biosecurity coordination	●	○	Proposed bill Would bind if enacted	INTRODUCED
2025	H.R. 3029 Nucleic Acid Standards for Biosecurity Act, 119th Congress	●	●	Proposed bill Would bind if enacted	ADVANCED FROM COMMITTEE
2025	S. 2676 Cloud LAB Act, cloud labs with biosecurity and cybersecurity safeguards	●	○	Proposed bill Would bind if enacted	INTRODUCED
2025	FY26 NDAA, Secs. 245 / 6614–6615 Biological data for AI plus domestic synthetic DNA/RNA procurement	●	●	Binding law Enacted statute	ENACTED
2025	BIOSECURE Act / FY26 NDAA Federal procurement restrictions for biotechnology companies of concern	○	○	Procurement restriction Enacted procurement bar	ENACTED
2026	S. 3741 Biosecurity Modernization and Innovation Act, synthesis security regulation	○	●	Proposed bill Would bind if enacted	INTRODUCED

Coverage key: ● Direct coverage ○ Partial or indirect coverage ○ No meaningful coverage

Status key: □ In place, active, or enacted ■ Dead, draft, pending, or not fully in force

Coverage markings: Direct - expressly regulates, funds, directs, requires, or establishes governance for the target area; partial/indirect - addresses the target through adjacent AI, biotechnology, biological data, national security, procurement, or research oversight mechanisms; none - broadly biosecurity relevant but does not materially govern that target area.
 Legal effect note: Proposed bills are coded by expected mechanism, not current legal force; they bind only if enacted.
 Sources: White House; Federal Register; Congress.gov; GovInfo; NIST; HHS; ASPR; OSTP; DHS; NIH; DOE.
 Scope note: Selected federal actions relevant to AI-biosecurity and nucleic acid synthesis; not exhaustive.

Status checked May 5, 2026.

3.2 Insufficient Regulation of the DNA Synthesis Industry

Nucleic acid synthesis screening is the process by which providers compare synthetic DNA or RNA orders, and often the customer, against databases of regulated pathogen and toxin sequences, called ‘**sequences of concern**’ (SOC), and public sequence repositories before fulfilling an order [117]. This process is crucial because it prevents the procurement of dangerous pathogens or toxin-related genetic material by malicious or unauthorized actors.

Current DNA vendors, such as Integrated DNA Technologies and Twist Bioscience, can deliver cloned DNA vectors of 3,000 and 300 to 5,000 base pairs, respectively. For reference, the Omicron variant’s spike protein, while not a whole pathogen, is on the order of 3,800 base pairs [118]. As a result, a pathogenic sequence, if not verified, can be contained within the length of an ordered sequence from a DNA synthesis provider.

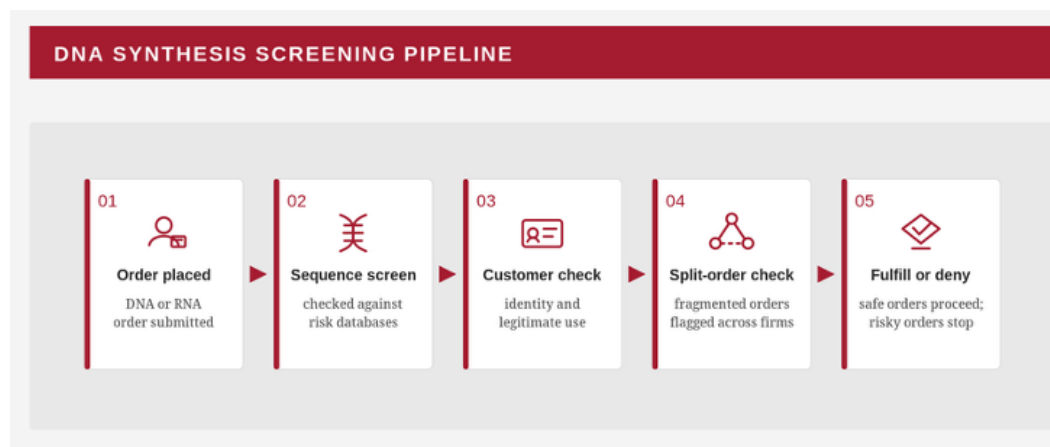


Figure 6: DNA synthesis screening pipeline.

This ordering capacity creates a policy concern. In addition to AI oversight, President Biden’s EO 14110 contained provisions that directed the Office of Science and Technology Policy (OSTP) to produce a framework for synthetic nucleic acid screening, which was released in April 2024 [2]. This framework developed criteria for potentially harmful sequences and standardized screening methods [119]. After April 2025, NIH funds are to be spent only on DNA synthesis providers that adhere to the framework [120]. EO 14110 also mandated the development of the 2024 *Dual Use Research of Concern and Pathogens with Enhanced Pandemic Potential Policy* (DURC/PEPP) [121], governing high-risk federally funded life sciences research, and the 2023 *Department of Health and Human Services (HHS) Screening Framework*

Guidance, establishing baseline screening standards for synthetic nucleic acid orders. The HHS guidance, for example, replaced the earlier 200-nucleotide screening window with a smaller 50-nucleotide window to improve detection of risky shorter fragments that could later be assembled into a dangerous pathogen [117].

In 2025, President Trump released EO 14292, *Improving the Safety and Security of Biological Research*. The order directed the revision or replacement of the Biden-era DURC/PEPP and nucleic acid synthesis screening frameworks, while imposing an interim pause on covered dangerous gain-of-function work. In practice, its clearest legal effect is through federal funding conditions, especially for NIH-funded research, rather than through a generally applicable rule for the full private sector [122]. The administration's July 2025 *AI Action Plan* contains similar biosecurity proposals, but it is a policy roadmap that does not create enforceable obligations for private actors [108].

The FY2026 National Defense Authorization Act's BIOSECURE Act addresses an adjacent supply-chain risk by restricting federal agencies, contractors, and grant recipients from using biotechnology equipment or services from designated biotechnology companies of concern, especially those that could expose U.S. genetic data or sensitive research to foreign adversaries. It does not, however, create generally applicable DNA synthesis screening rules for private providers [123].

None of these measures creates a comprehensive federal regime for private actors outside federally funded research. Without congressional regulation, agencies have limited authority to bind companies that do not rely on NIH funds.

The *Biosecurity Modernization and Innovation Act of 2026* would require the DOC to issue binding regulations for nucleic acid synthesis security, replacing the current voluntary federal approach with mandatory screening rules for covered providers. Those rules would include sequence screening, customer verification, split-order detection across providers, a regularly updated list of sequences of concern, provider auditing and conformity assessment, and civil enforcement for violations. The bill stalled in committee, and other similar bills either rely on voluntary standards or never advanced beyond introduction [124, 125, 126].

This regulatory gap leaves much of the private DNA synthesis market outside of binding federal oversight. As a result, malicious actors could still obtain dangerous sequences from companies that either do not use best practices to screen customers and sequences or do not screen orders at all.

3.3 Insufficient Early Outbreak Detection and Response Protocols

Public health systems often recognize epidemic and pandemic threats only after transmission has spread far enough to trigger a formal response. The timeline between the early infectious-cluster monitoring, response, and the large-scale epidemic countermeasures defines the ultimate course of the epidemic.

The United States does not clearly govern travel restrictions during ambiguous emerging outbreaks. For example, the WHO was informed of an outbreak of a virus of unknown origin emerging in Wuhan, China, on December 31, 2019 [127]. The first attributable SARS-CoV-2 case was confirmed on December 8, 2020 [128], with the first reports on transmissivity and viral incubation published in late January, 2020 [129]. A public health emergency was declared on January 31, 2020, with only seven cases detected. However, by the time of the National Emergency Proclamation on March 13, 2020, more than 1,600 cases had spread throughout the United States [130]. During this period, around eight million overseas arrivals to the United States were recorded [131]. These statistics show the delay between identifying an outbreak and implementing protective measures, while vaccine development shapes the longer-term response.

Additionally, the COVID-19 pandemic highlights the need for the Centers for Disease Control and Prevention (CDC) to access and use public data at the federal level for informed and efficient public health decision-making [132]. The United States does not mandate interoperable data-sharing among federal, state, and private labs. Slow data collection and analysis delay the activation of an early-warning triggering protocol for an emergency response.

The United States does not maintain standardized national protocols for detecting novel pathogens or engineered-pathogen anomalies. Syndromic, wastewater, bioaerosol, genomic, and clinical signals, if collected, are fed into fragmented platforms. Rural U.S. areas, additionally, are poorly covered. Further, the lack of federally mandated early-warning trigger protocols that connect epidemic intelligence to more proactive monitoring or an early response is notable [132].

As a result, the known countermeasures, such as testing, contact tracing, travel screening, isolation policies, and even federal resource deployment to the focal area, would lag behind the infectious spread. This vulnerability is particularly exploitable in the case of a novel AIxBio-generated pathogen, when the available testing platforms may perform poorly, and early-detection systems may malfunction due to unprecedented metrics.

The United States lacks a coherent framework for detecting unprecedented biological threats early enough to assess risk and respond effectively. American public health authorities generally do not subject such early detection points to metagenomic next-generation sequencing for an unbiased assessment of the pathogen [132].

These procedural and legislative gaps shift the paradigm from preventive early detection to reactive outbreak response. The latter occurs after infectious cases have already reached the clinical stage and containment strategies have been activated.

4. Policy Recommendations

This report makes the following recommendations to the United States government to close the regulatory gaps outlined in Section 3 and reduce AI-enabled biological risk across AI model development, biotechnology capabilities access, and outbreak preparedness.

Main Recommendations

Enforcing Built-In AI-Biosecurity Safeguards in Frontier Models

- Establish a government-authorized private regulatory market where licensed technical auditors enforce AI-biosecurity safeguards for frontier models.
- Use government-defined safety outcomes and NIST/CAISI technical standards to augment private audits.
- After establishing U.S. safeguards, expand the framework internationally through treaties and shared technical standards.

Regulating the Biotechnology and Synthesis Industry

- Require universal screening of synthetic nucleic acid orders longer than 50 nucleotides, including private-sector orders, with customer verification and mandatory reporting of failed legitimacy checks.
- Build an AI-enabled centralized screening system to detect fragmented orders and model the potential human-cell effects of ordered genetic sequences before synthesis.
- Create a federal licensing regime for sensitive laboratory equipment, requiring buyer verification, pre-purchase approval, ownership registration, and transfer tracking.

Early Outbreak Detection and Response

- Build an AI-enabled epidemic intelligence system that integrates NSSP, One CDC Data Platform, wastewater, bioaerosol, genomic, and clinical surveillance.
- Fund nationwide upgrades to wastewater and bioaerosol monitoring, including rural coverage and BARDA-supported detection infrastructure.
- Standardize and approve mNGS diagnostics while securing scalable mRNA vaccine manufacturing capacity through government-backed private partnerships.

4.1 Frameworks for Enforcing Built-In AI-Biosecurity Safeguards in Frontier Models

A major policy challenge is determining how to mandate that AI-biosecurity safeguards be built into frontier AI models. These safeguards can include watermarking, harm-refusal tuning, unlearning of dangerous information, anti-jailbreak defenses, AI agent defense layers, red-teaming, mandatory reporting, and monitoring [133].

Unforeseen risks in a rapidly evolving technical landscape and severe information asymmetries create a unique regulatory challenge for frontier AI. Effective oversight requires highly specialized technical expertise, yet that expertise is scarce and often commands far higher compensation in industry than in government. At the same time, firms may not have sufficient incentives to support regulation on their own, especially where compliance is costly or constrains deployment [104].

Any enforcement regime must mitigate catastrophic biosecurity risk while avoiding restrictions on AI development likely to meaningfully hinder innovation. Because frontier model developers operating outside the United States are not easily regulated by U.S. law, the most durable approach is one that is scalable and interoperable across jurisdictions, whether through international coordination, reciprocal recognition arrangements, or other diplomatically developed baseline standards.

A viable framework must also account for the constraint that the same highly specialized practitioners are needed both inside firms and within licensing or oversight bodies. This bottleneck heightens the risk of regulatory capture and revolving-door corruption. Policymakers must also develop red-teaming and auditing mechanisms that do not require disclosure of trade secrets or sensitive proprietary information. This dilemma creates opportunities for public-private regulatory models that vary by the degree of public involvement and enforcement authority.

Four enforcement frameworks are most relevant: **private regulatory markets, private insurance markets, government-led regulatory action, and technical standards**. While each could improve on the status quo, this report argues that private regulatory markets are the strongest model because they offer realistic oversight without excessively hindering innovation. Technical standards, detailed in Section 4.1.4, can also augment these private regulatory markets by giving auditors requirements for compliance evaluation.

4.1.1 Private Regulatory Markets

A hybrid model, particularly one proposed by economist Gillian Hadfield and Anthropic Co-Founder Jack Clark, would delegate technical aspects of regulation to government-licensed private regulators with relevant expertise. The federal government would determine desired outcomes and guardrails designed to maximize public benefit and minimize harm, while granting the bodies the authority to impose requirements and fines on AI developers. Using the government's desired end states for public safety, government-appointed expert groups assess how these specialized regulatory firms conduct audits and red-teaming [104].

Model developers would be required to pay for auditing and red-teaming services from licensed private providers, creating a stable, government-authorized market demand for those firms. This guaranteed demand would likely attract investment into red-teaming capacity and technical evaluation infrastructure. The system would align incentives by creating a market for licensed oversight firms that maintain government-defined safety standards [104].

This model carries several structural risks. Competing private regulators could collude or consolidate, weakening competition in oversight, while revolving-door dynamics and regulatory capture could emerge if evaluators are financially dependent on the firms they assess. This scenario would reproduce problems similar to those created by credit rating agencies during the 2008 financial crisis [104]. Critics, including David Sacks, argue that complex regulatory systems can create barriers to entry and favor large incumbents, who can better afford to adapt to requirements [134].

To mitigate these risks, technical talent working within licensing firms must be heavily compensated and also be subject to post-employment restrictions that limit their ability to join firms they previously audited. Developers should fund the system, but should not be able to choose or directly compensate the firms that evaluate them. To prevent barriers to entry, AI developers can be given scaled requirements based on deployment risks and model capabilities.

4.1.2 Private Insurance Markets

Another delegated model, modeled after Weil *et al.* but adapted to include biosecurity-specific requirements, would use insurance as a governance mechanism for AI. Under this approach, the government would require developers and deployers of higher-risk systems to carry liability insurance or demonstrate financial capacity to cover harms. Insurers would become a quasi-regulatory mechanism by enforcing safety through underwriting. AI firms that adopt stronger safeguards, audits, evaluations, red-teaming, and other biosecurity risk-mitigation measures would be easier to insure and would face lower premiums. The risk-based premiums would incentivize developers to prioritize safer design and deployment to reduce costs. Insurance would also serve a risk-sharing function and help ensure compensation for those harmed by AI-enabled biological incidents [135]. For catastrophic risks, Congress could adopt a Price-Anderson-style framework that guarantees protection above an industry-funded liability threshold, so long as regulated firms remain in compliance [136].

This model may impose less of a barrier to entry than other licensing models because premiums can scale with risk. Non-frontier firms, which would likely present lower biological misuse risks, could face lower premiums than frontier developers. At the same time, this approach would push insurers to develop new actuarial methods, risk forecasting models, and mitigation tools for emerging AI harms, aligning incentives by making safer systems cheaper to build and deploy [137]. Another advantage is that insurers may be less vulnerable to revolving-door corruption than specialized regulators, because their expertise is based more on underwriting and risk pricing than on technical knowledge and ties to the firms they oversee.

As currently designed, this model has several weaknesses that would need to be addressed. It depends on a clear liability framework with rules for assigning legal responsibility, yet responsibility for AI-related harms may be difficult to assign among users, developers, deployers, or third parties. AI also currently presents many uncertainties that make pricing difficult and could limit insurers' willingness to enter the market. Regardless, companies like Armilla and Munich Re now offer insurance products for AI-specific risks [137, 138].

4.1.3 Government-Led Regulatory Actions

Government regulation is the most direct mechanism for imposing AI-biosecurity safeguards on frontier model developers, but it is among the most difficult to implement well. For government regulation to be fully binding on private developers, it would likely need congressional authorization rather than reliance on temporary executive action alone.

Congressional regulation carries significant drawbacks. The legislative process is slow to react, while the frontier AI environment evolves quickly. Effective regulation would also require technical expertise in machine learning, cybersecurity, biological risk assessment, and model evaluation, yet that expertise is scarce and expensive. A poorly resourced agency could become dependent on the same firms it regulates, leading to a revolving-door scenario. Similar to private markets in Section 4.1.1, heavy requirements could also favor incumbents if compliance costs are too high [104, 139].

For these reasons, government regulation is not the recommended model, but it may be better than no framework at all. Regulators should receive high compensation and face post-employment restrictions. In practice, the two most plausible government pathways are regulating biological data inputs and licensing frontier models. The United States should also pursue diplomatic agreements to extend safeguards internationally.

4.1.3.1 Biological Data-Based Government Framework

Allison Berke of the Johns Hopkins Center for Health Security recommends a tiered system for biological data inputs in AI systems. Similar to the U.S. government classification of information, biological data would be subject to higher control measures as its potential impact on national security increases.

The framework includes a phased implementation pipeline that uses executive orders and agency directives in the short term to ensure governmental and voluntary compliance. HHS would issue governance guidelines, NIST would set technical and auditing standards, CAISI would reassess risks as AI capabilities evolve, the Bureau of Industry and Security (BIS) would oversee export controls, and OSTP would coordinate the interagency process. This pilot program would be followed by sweeping congressional mandates that would bind private entities

to the same standards. Finally, the framework would expand internationally through coordination with allied biosecurity agreements, including the Biological Weapons Convention [140].

4.1.3.2 Government Licensing Framework

A government licensing model would require frontier AI developers to obtain approval from a designated federal authority, such as the Department of Commerce, before training, deploying, or materially modifying systems above defined capability or risk thresholds. The government would establish binding safety requirements, including cybersecurity controls, red-teaming, model evaluations, monitoring, and incident reporting, as conditions for obtaining and maintaining a license. Rather than delegating authority to private regulators, as in private regulatory markets, the state would retain direct control over approval, renewal, suspension, and revocation decisions [139].

Licensing could apply across the frontier AI lifecycle, including hardware acquisition, model training, and deployment. Developers would be required to demonstrate compliance before market access and maintain compliance through post-deployment monitoring. This architecture would make biosecurity safeguards a condition of operation instead of a voluntary commitment [139].

This model carries structural risks similar to the delegated regulation model. High compliance costs could favor large incumbents, while agency dependence on scarce industry expertise could increase regulatory capture and revolving-door concerns.

4.1.3.3 International AI-Biosecurity Treaty

Once the United States adopts safeguards, it should work diplomatically to expand them to states with jurisdiction over major AI models and biotechnology developers. This International AI-Biosecurity Treaty would require domestic laws mandating AI-biosecurity safeguards for frontier models, including audits, red-teaming, model-weight security, and compliance reviews. It should also require shared screening standards for nucleotide orders, including customer screening and a continuously updated sequences-of-concern database. For outbreak prevention and response, signatories should share lab-safety best practices and pathogen genomic data, with protocols for disclosing credible information on disease origins.

Compliance should be verified through cross-audits and limited scientific access to relevant biological lab procedures. Because bioweapons create mutual catastrophic risk that crosses borders, the treaty should frame cooperation as reciprocal risk reduction and not a concession to strategic rivals.

4.1.4 Technical Standards as an Enforcement Framework

Technical standards can be another framework for enforcing biosecurity safeguards in AI models. Standards can turn desired safety goals into technical requirements that can be mandated by governments, private regulators, or insurance companies.

Several standards bodies and independent evaluators are already working toward responsible AI governance. For example, Model Evaluation and Threat Research (METR) compares frontier AI safety policies against a range of criteria, including capability thresholds for biological misuse, conditions for halting deployment, model-weight security, and accountability [141]. ISO/IEC JTC 1/SC 42 is developing standards for artificial intelligence, and other bodies can similarly define the technical rules that later could be incorporated into biosecurity risk mitigation requirements [142].

This framework has several advantages. Standards can be more technical and easier to update than congressional mandates. They also rely on existing technical expertise outside government, which is useful when agencies lack enough specialized personnel to regulate frontier AI systems directly. Standards can also transcend national borders more easily than domestic statutes, making them useful for international AI-biosecurity coordination [143].

However, entrenchment may occur because established firms can devote more resources to influencing and drafting technical standards [144]. Furthermore, premature standardization before risks are well understood can result in standards that are too weak to address biosecurity concerns or so stringent that they create barriers to entry for less-resourced firms [145].

As a result, technical standards should not be used alone as a regulatory mechanism. Instead, they can be incorporated into other regimes to address gaps where technical specificity is required to legally enforce requirements.

The United States should fund NIST and CAISI to develop AI-biosecurity technical standards that can be used by government agencies, private regulators, and insurers. The federal government should also tie procurement eligibility and limited liability protections to certified compliance with those standards. Finally, the United States should compete for leadership in international standards bodies to ensure that global AI standards reflect biosecurity priorities over private interests.

4.2 Frameworks for Regulating the Biotechnology and Synthesis Industry

The regulatory goal is to reduce the risk of biological harm while minimizing disruption to legitimate research and commercial biotechnology. A practical framework should strengthen oversight of the access points that make pathogen construction feasible, including ordering sequence synthesis and acquisition of specialized laboratory equipment.

4.2.1 Nucleotide Screening Regulations

Finding the right balance between protective measures against emerging biotechnology risk and disruption of the sector's innovation is critical. Private biotechnology companies still require nucleotide sequences for research and development. In 2024, the nucleotide market exceeded \$900 million, with projections of the market size rising above \$1.5 billion by 2030 [146].

Congress should adopt the core provisions of the Biosecurity Modernization and Innovation Act of 2026 to extend synthetic nucleic acid order oversight beyond federally funded research and require screening for all nucleotide sequence orders longer than 50 nucleotides, irrespective of their federal or private funding. The 2023 HHS framework discussed in Section 3.2 mandates NIH-funded labs to order from providers abiding by screening protocols, while the private sector and third-party orders remain unregulated. This gap creates an operational risk where different seemingly unrelated customers can order nucleotide sequences that, once assembled, can lead to pathogen generation. These measures would reduce the likelihood that a novel pathogen could be produced in-house by non-state or rogue state actors.

According to the 2023 framework, sequence compatibility with an SOC still allows customers to procure the desired nucleotide sequence as long as their legitimacy is verified and customers track the use of their equipment. In the event the legitimacy requirement is not fulfilled, the providers should deny the order and contact agencies, such as the DOC and the Federal Bureau of Investigation (FBI). The government should deploy a centralized tracking system using AI to evaluate if 50-nucleotide sequences fit into a longer SOC, then cross-check other orders for other portions of the SOC.

However, this framework is limited to the Federal Select Agent Regulations, which regulate a subset of microbial organisms and toxins determined to have the potential to pose a severe threat to public health and safety, animal health, plant health, animal or plant products, or the environment [117]. It does not have regulatory oversight over what could be an emerging gain-of-function *de novo* pathogen sequence obtained from AIxBio predictive tools (see Section 2.2). The government should closely oversee advancements in open-source or easy-to-access LLMs with predictive ability for the effects of many classes of genomic changes or intelligent *de novo* design of new biological systems [14].

AIxBio tools, such as *Evo 2*, could accelerate translational medicine, but they could also give malicious actors dangerous capabilities [147]. The technology readiness level of the AIxBio-validation interface needs to be continuously monitored by government agencies and biosecurity experts.

The same predictive capacity that creates dual-use risk can also give the United States a defensive advantage by enabling early detection of hazardous biological designs. In the foreseeable future, AI agents are likely to become more integrated with biological research tools, enabling laboratories to automate the analysis of increasingly complex biological datasets [72]. A second-generation genome language model could emerge, reducing the need for lab-based *in vitro* testing and model validation, and removing human review from the loop. The government should track advances in AIxBio validation and partner with private or nonprofit organizations to develop a secure AI-based biosecurity screening platform. The United States should further invest in technology to use AI to model the potential human-cell effects of novel genetic sequences, then mandate synthesis providers to screen orders for credible biosecurity risks before fulfillment.

AIxBio's predictive features should be integrated into the HHS guidelines for protective measures during nucleic acid order screening. This requirement will close the gap between the sequences currently included in the U.S. government's Federal Select Agent Program list and newly designed pathogenic sequences. Such agentic AI integration should proceed incrementally, with validation checkpoints assessing whether the platform can reliably flag novel, potentially harmful sequences. The framework should also establish procedures for customers to provide evidence of legitimate, benign use and for providers to track the ordered biomaterial.

4.2.2 Laboratory Equipment Licensing Regulations

A federal licensing regime should prevent malicious actors outside legitimate laboratory settings from acquiring equipment capable of enabling biological weapons development by requiring buyer verification and pre-purchase approval, while mandating registration of ownership and transfers. These sensitive AIxBio tools should include advanced cell-analysis systems, nucleic acid synthesis machines and software, bioreactors, and gene-editing platforms used to analyze, design, modify, test, or scale biological agents. Similar regulatory definitions already exist for export compliance and can be extended to domestic production.

Since 1996, 15 C.F.R. § 742.2 has restricted exports and reexports of listed chemical and biological items by requiring licenses and directing denial when an export could make a “material contribution to the design, development, production, stockpiling or use of chemical or biological weapons” [148]. In 2021, the Biden Administration imposed export controls on software for nucleic acid assemblers and synthesizers on biological-weapons nonproliferation grounds [44]. Then, before leaving office in 2025, President Biden expanded the list once more to include additional laboratory equipment and related technology, such as high-parameter flow cytometers, which can rapidly measure cell characteristics to generate datasets that can help design AI-enabled bioweapons [36].

American equipment producers cannot freely export covered laboratory equipment and related technology to most non-allied, unstable, and terrorism-linked destinations, yet comparable domestic purchase and possession remain largely uncontrolled. Extending export-control concepts to domestic licensing would close this gap by strengthening oversight of acquisition and ownership inside the United States.

4.3 Frameworks for Early Outbreak Detection and Response

Early outbreak policy should reduce the time between biological anomaly detection and coordinated public health action. A practical framework should integrate emerging technology to detect and communicate biological threats early enough for targeted containment and rapid response.

4.3.1 Proactive Outbreak Monitoring

Epidemic intelligence is the process of detecting, verifying, and analyzing public health threats to enable timely responses [149]. Despite increased AI capabilities in outbreak detection as demonstrated during the COVID-19 pandemic, remaining challenges include real-time adaptability, multilingual data handling, misinformation, and public health policy alignment [150].

The National Syndromic Surveillance Program helps gather and provide syndromic data from collaborations with state and local health departments and others [151]. The One CDC Data Platform is a unified platform aiding in preparation, early detection, and response to public health threats through data sharing between the CDC and its partners [152]. Advancements in AI's large language models and natural language processing applied to the existing NSSP and One CDC Data Platform would enable improved real-time analytics and sharing [151, 152]. Development of a cohesive AI-based epidemic intelligence system would upgrade multilingual surveillance, employ predictive analytics for early outbreak forecasting, and optimization algorithms for health care resource management [152].

CDC launched the National Wastewater Surveillance System (NWSS) in 2020 to coordinate national wastewater monitoring of SARS-CoV-2. The system has since expanded beyond COVID-19 to include influenza A, SARS-CoV-2, respiratory syncytial virus, measles, avian influenza A(H5), and monkeypox [153, 154]. Simultaneously, its bioaerosol counterpart, the DHS's BioWatch, is operating in 30 major metropolitan areas across the United States with the highest population density and greatest potential consequences of an attack [155].

Additionally, early outbreak detection could rely on real-time sequencing information through the CDC's Advanced Molecular Detection Program. To date, genomic sequencing of patients' data remains subject to regulatory hurdles due to patient and genomic data privacy and cost-effective scale-up [156]. While genomic sequencing becomes easier and faster technologically, data integration into a structured bioinformatics database for near real-time analysis and early detection remains costly. Leveraging interoperability between the fragmented bioinformatics platforms, cloud storage, and analytic pipelines is key to ensuring a thorough assessment of an emerging biological threat [156].

Recent advances in viral detection through metagenomic sequencing of air samples could significantly expand the ease of early detection for transmissible viruses and airborne diseases [157]. The U.S. government should invest through BARDA funding in upgrading the existing detection platform for bioaerosol monitoring on a larger scale. Secondly, the government should actively deploy an AI-assisted interoperable system for proactive monitoring of wastewater streams and bioaerosol infectious loads in rural areas as well as large metropolitan areas.

The United States should develop a coordinated system that tracks viruses in both wastewater and air, all feeding into a shared CDC data platform. This strategy would help officials determine the emergence point and act faster to curb outbreaks. It would enable earlier decisions on measures, like isolation or preventive treatment, reducing the risk of wider spread.

4.3.2 Outbreak Responses

Rapid advances in genomic surveillance, wastewater monitoring, and AI-enabled anomaly detection improve early outbreak identification, but not prevention and response [158, 159]. The lessons from the COVID-19 pandemic and analysis of the emerging biotechnology field highlight policymaking strategies to be implemented for both early outbreak response and longer-term epidemic control.

4.3.2.1 Metagenomic Next-Generation Sequencing for Proactive Emerging Threat Diagnostics

Infectious disease diagnostics are expected to enable simultaneous, hypothesis-free detection of a wide array of pathogens, including viral infections,

through the use of metagenomic next-generation sequencing. mNGS operates by comprehensively sequencing all genetic material in a sample and computationally matching those sequences to known organisms, enabling pathogen identification without requiring prior assumptions about the cause of infection [160].

Despite advancements in mNGS, notable limitations include standardization of the methods, bioinformatics, and databases used in practice [67]. To date, no FDA-approved mNGS platforms exist for infectious disease monitoring, but some have been granted the breakthrough device designation [161]. To close the gap between early outbreak detection and rapid response, the government should prioritize standardizing mNGS platforms. This effort should follow Clinical Laboratory Improvement Amendments requirements and be supported by CDC guidance and FDA oversight.

Epidemic risk depends heavily on transmissibility and population susceptibility: if exposure can infect nearly anyone, containment becomes harder. According to the CDC's definition, an outbreak is defined as an aggregation of cases with a higher number than expected for a given time, within a specific location, and for a target population [162]. Precautions for preventing the transmission of infectious diseases from infected to healthy individuals are outlined in the CDC's guideline for isolation policies [163]. However, even with a robust framework for combating an outbreak, parameters, such as transmissivity and severity of illness, are contingent upon the emerging infectious threat.

As demonstrated by the COVID-19 pandemic, mNGS data sampled from symptomatic patients, asymptomatic patients, and contacts would provide relevant information on viral incubation time [161]. Additionally, mNGS is key in identifying the circulating viral strains and tracking the evolutionary course of the epidemic [164]. The government should invest in supporting the emerging mNGS platforms for widespread implementation. The government should also approve their clinical use for novel infections, with epidemiological data fed into the integrated One CDC Platform for early outbreak response and to generate knowledge about epidemiological risk. A reliable assessment of the transmissivity and viral incubation time would assist policymakers in implementing isolation strategies and travel restrictions appropriately.

4.3.2.2 Vaccine Platform Acquisition for Efficient Epidemic Response

There is no universally accepted best vaccine platform for rapid viral response. Although live attenuated vaccines are potent and do not typically cause disease, they require more careful handling and storage and may be problematic for immunocompromised patients. On the other hand, inactivated vaccines, while easier to handle and unable to revert to an active virus, often require boosters for a prolonged immunogenic response in patients [165].

As demonstrated with the COVID-19 pandemic, the mRNA vaccine manufacturing platform benefits from numerous attributes, such as flexibility, high potency, safety, and efficacy, coupled with the ability for rapid clinical development, scalability, and cost-effectiveness in manufacturing [166]. However, like any vaccine, it requires the viral sequence and identification of an immunogenic target. That was the case for the Pfizer and Moderna mRNA vaccines against the SARS-CoV-2 spike protein [167]. The success of the vaccine came from targeting a highly conserved biomarker, such as the spike protein, critical for host infection and conserved across strains despite newly acquired mutations [168].

Therefore, the mRNA vaccine platform is expected to show similar therapeutic results in the context of future viral epidemics and possible emerging pandemics. Moderna's current vaccine pipeline for viral infections and ongoing clinical trials for potential anticancer vaccines highlight the therapeutic benefit of deploying a flexible, scalable, and efficient mRNA vaccine platform in the future [169]. For major outbreak threats, the government should use an Operation Warp Speed-style model to fund private companies, like Moderna, for both R&D and clinical trials [170]. The government should secure a flexible and scalable mRNA vaccine manufacturing platform for future transmissible viral outbreaks. A government-owned platform should emerge through an incentivized partnership with the private-sector leaders who established the manufacturing pipeline.

5. Conclusion

AIxBio makes the next biological crisis harder to imagine and harder to contain. The danger is no longer limited to pathogens that emerge by chance. It now includes biological threats accelerated by models, data, and manufacturing systems that move faster than public institutions can govern.

The United States should first close its own governance gaps. It needs enforceable safeguards for frontier models, universal DNA synthesis screening, control over sensitive laboratory equipment, and faster outbreak detection. But governance must be precise. Overregulation would slow the AI and biotechnology sectors that give the United States its strategic edge. Underregulation would leave the country exposed to biological misuse. National security requires both innovation and model safety, because unsafe systems can erase the gains technological leadership was meant to secure.

Then, the United States should lead the adoption of universal international safeguards. AIxBio risk cannot be treated only as another arena of great power competition. Biological threats spill across borders regardless of who created them, making risk reduction not a zero-sum game. The United States should align incentives by making verification and transparency serve every state's interest in avoiding engineered biological crises. Cooperation that reduces biological risk is a way for all sides to preserve lives, resources, and strategic capacity, not a concession.

Endnotes

- [1] Jake Sullivan, "Remarks by National Security Advisor Jake Sullivan on Artificial Intelligence and National Security at the National Defense University," speech transcript, The American Presidency Project, October 24, 2024, <https://www.presidency.ucsb.edu/documents/remarks-national-security-advisor-jake-sullivan-artificial-intelligence-and-national>.
- [2] Executive Order No. 14,110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," 88 Fed. Reg. 75,191-75,226 (November 1, 2023), <https://www.federalregister.gov/d/2023-24283>.
- [3] Jaskaran Preet Singh Saini, Ankita Thakur, and Deepak Yadav, "AI-Driven Innovations in Pharmaceuticals: Optimizing Drug Discovery and Industry Operations," *RSC Pharmaceutics* 2 (2025): 437-454, <https://doi.org/10.1039/d4pm00323c>.
- [4] D. B. Catacutan, J. Alexander, A. Arnold, et al., "Machine Learning in Preclinical Drug Discovery," *Nature Chemical Biology* 20 (2024): 960-973.
- [5] J. Kim, S. Lee, H. Park, and Y. Choi, "Artificial Intelligence in CRISPR-Cas9 Genome Editing: Design, Optimization, and Applications," *Experimental & Molecular Medicine* 57 (2025): 1419-1431.
- [6] Kavita Gupta, "Neural Networks Layers Explained," Medium, accessed August 2026, https://medium.com/@kavita_gupta/neural-networks-layers-explained-098da06e1b98.
- [7] InfoDiagram, "Predictive AI Model Development Process Diagram," accessed August 2026, <https://www.infodiagram.com/slides/predictive-ai-model-development-process-diagram/>.
- [8] H. Zhang, H. Liu, Y. Xu, H. Huang, Y. Liu, J. Wang, Y. Qin, H. Wang, L. Ma, Z. Xun, X. Hou, T. K. Lu, and J. Cao, "Deep Generative Models Design mRNA Sequences with Enhanced Translational Capacity and Stability," *Science* 390 (2025): eadr8470, <https://doi.org/10.1126/science.adr8470>.
- [9] Christopher M. Bishop, *Pattern Recognition and Machine Learning* (New York: Springer, 2006).
- [10] Ian Goodfellow, Yoshua Bengio, and Aaron Courville, *Deep Learning* (Cambridge, MA: MIT Press, 2016).
- [11] U.S. Food and Drug Administration, *Considerations for the Use of Artificial Intelligence to Support Regulatory Decision-Making for Drug and Biological Products: Guidance for Industry and Other Interested Parties* (Silver Spring, MD: U.S. Food and Drug Administration, 2025), <https://www.fda.gov/media/184830/download>.
- [12] Guy Durant, Fergus Boyles, Kristian Birchall, and Charlotte M. Deane, "The Future of Machine Learning for Small-Molecule Drug Discovery Will Be Driven by Data," *Nature Computational Science* 4, no. 10 (2024): 735-743, <https://doi.org/10.1038/s43588-024-00699-0>.
- [13] J. Abramson, J. Adler, J. Dunger, R. Evans, T. Green, A. Pritzel, O. Ronneberger, et al., "Accurate Structure Prediction of Biomolecular Interactions with AlphaFold 3," *Nature* 630 (2024): 493-500, <https://doi.org/10.1038/s41586-024-07487-w>.
- [14] G. Bixi, N. K. Schaefer, P. K. Koo, et al., "Genome Modelling and Design across All Domains of Life with Evo 2," *Nature* (2026), <https://doi.org/10.1038/s41586-026-10176-5>.
- [15] U.S. Food and Drug Administration, "Step 2: Preclinical Research," *The Drug Development Process*, archived November 29, 2014, Internet Archive, <https://web.archive.org/web/20141129071644/http://www.fda.gov/ForPatients/Approvals/Drugs/ucm405658.htm>.
- [16] U.S. Food and Drug Administration, "Step 3: Clinical Research," *The Drug Development Process*, archived November 22, 2014, Internet Archive, <https://web.archive.org/web/20141122080847/http://www.fda.gov/ForPatients/Approvals/Drugs/ucm405622.htm>.
- [17] C. Cinti, M. G. Trivella, M. Joulie, H. Ayoub, and M. Frenzel, "The Roadmap toward Personalized Medicine: Challenges and Opportunities," *Journal of Personalized Medicine* 14 (2024): 546, <https://doi.org/10.3390/jpm14060546>.
- [18] Tolulope O. Olorunsogo, Obe Destiny Balogun, Oluwatoyin Ayo-Farai, Oluwatosin Ogundairo, Chinedu O. Maduka, and Chika C. Okongwu, "Bioinformatics and Personalized Medicine in the U.S.: A Comprehensive Review: Scrutinizing the Advancements in Genomics and Their Potential to Revolutionize Healthcare Delivery," *World Journal of Advanced Research and Reviews* 21, no. 1 (2024): 335-351, <https://doi.org/10.30574/wjarr.2024.21.1.0016>.
- [19] Francis S. Collins and Harold Varmus, "A New Initiative on Precision Medicine," *New England Journal of Medicine* 372 (2015): 793-795, <https://www.nejm.org/doi/pdf/10.1056/NEJMp1500523>.
- [20] The All of Us Research Program Genomics Investigators, "Genomic Data in the All of Us Research Program," *Nature* 627 (2024): 340-346, <https://doi.org/10.1038/s41586-023-06957-x>.
- [21] National Human Genome Research Institute, "Pharmacogenomics," [genome.gov](https://www.genome.gov/genetics-glossary/Pharmacogenomics), accessed August 2026, <https://www.genome.gov/genetics-glossary/Pharmacogenomics>.
- [22] National Institutes of Health, "All of Us Research Program," accessed August 2026, <https://www.joinallfous.org/>.
- [23] Mary V. Relling and William E. Evans, "Pharmacogenomics in the Clinic," *Nature* 526 (2015): 343-350, <https://doi.org/10.1038/nature15817>.
- [24] HIPAA Journal, "6.9 Million 23andMe Users Affected by Data Breach," accessed August 2026, <https://www.hipaajournal.com/6-9-million-23andme-users-affected-by-data-breach/>.

- [25] U.S. Department of Health and Human Services, Office for Civil Rights, “Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,” 2024, <https://ocrportal.hhs.gov>.
- [26] Wilkins MR et al., “Progress with proteome projects: why all proteins expressed by a genome should be identified and how to do it,” *Biotechnology & Genetic Engineering Reviews*. (1996).
- [27] Henry Rodriguez, Jean Claude Zenklusen, Louis M. Staudt, James H. Doroshow, and Douglas R. Lowy, “The Next Horizon in Precision Oncology: Proteogenomics to Inform Cancer Diagnosis and Treatment,” *Cell* 184, no. 7 (2021): 1661-1670, <https://doi.org/10.1016/j.cell.2021.02.055>.
- [28] Ruedi Aebersold and Matthias Mann, “Mass Spectrometry-Based Proteomics,” *Nature* 422 (2003): 198-207.
- [29] Torsten Hubertus, “An Overview on Major Affinity Proteomics Methods,” *Journal of Data Mining in Genomics & Proteomics* 15, no. 4 (2024): 364, <https://doi.org/10.4172/2153-0602.24.15.364>.
- [30] Centers for Disease Control and Prevention, “Genetic Disorders,” *Genomics and Your Health*, May 15, 2024, <https://www.cdc.gov/genomics-and-health/about/genetic-disorders.html>.
- [31] National Human Genome Research Institute, “Genetic Disorders,” last updated May 18, 2018, <https://www.genome.gov/For-Patients-and-Families/Genetic-Disorders>.
- [32] American College of Obstetricians and Gynecologists, “Carrier Screening for Genetic Conditions,” Committee Opinion No. 691, March 2017, <https://www.acog.org/clinical/clinical-guidance/committee-opinion/articles/2017/03/carrier-screening-for-genetic-conditions>.
- [33] U.S. Food and Drug Administration, “KYMRIAH,” cellular and gene therapy product information, accessed August 2026, <https://www.fda.gov/vaccines-blood-biologics/cellular-gene-therapy-products/kymriah>.
- [34] Milena Falcaro, Alejandra Castañón, Busani Ndlela, et al., “The Effects of the National HPV Vaccination Programme in England, UK, on Cervical Cancer and Grade 3 Cervical Intraepithelial Neoplasia Incidence: A Register-Based Observational Study,” *The Lancet* 398, no. 10316 (2021): 2084-2092, [https://doi.org/10.1016/S0140-6736\(21\)02178-4](https://doi.org/10.1016/S0140-6736(21)02178-4).
- [35] K. Tao, J. Zhou, Y. Getaneh, et al., “GenBank2PubMed: Bridging Viral Genomic Data and the Scientific Literature with AI-Assisted Curation,” *Scientific Reports* 15 (2025): 45009, <https://doi.org/10.1038/s41598-025-28386-8>.
- [36] Bureau of Industry and Security, “Controls on Certain Laboratory Equipment and Related Technology to Address Dual-Use Concerns about Biotechnology,” *Federal Register* 90, no. 10 (January 16, 2025): 4612-4617, <https://www.federalregister.gov/documents/2025/01/16/2025-00723/controls-on-certain-laboratory-equipment-and-related-technology-to-address-dual-use-concerns-about-biotechnology>.
- [37] Daniel Griffin, Martin Johnson, Nicholas M. Thomson, and Clarence K. Wong, “Continuous Manufacturing of Small Molecule Drug Substances,” *Pharmaceutical Engineering*, July/August 2023, <https://ispe.org/pharmaceutical-engineering/july-august-2023/continuous-manufacturing-small-molecule-drug-substances>.
- [38] Sang Hwan Seo and Man Ki Song, “Advancements and Challenges in Next-Generation mRNA Vaccine Manufacturing Systems,” *Clinical and Experimental Vaccine Research* 14, no. 4 (2025): 299-307, <https://doi.org/10.7774/cevr.2025.14.e40>.
- [39] Coalition for Epidemic Preparedness Innovations, “Pushing mRNA Vaccine Development Timelines to New Speeds,” February 6, 2025, <https://cepi.net/pushing-mrna-vaccine-development-timelines-new-speeds>.
- [40] Coalition for Epidemic Preparedness Innovations, “Project to Explore Speed Up of mRNA Vaccine Production Deployable for Local Outbreaks,” July 22, 2024, <https://cepi.net/project-explore-speed-mrna-vaccine-production-deployable-local-outbreaks>.
- [41] GlobalSpec, “DNA Synthesizers Information,” accessed August 2026, https://www.globalspec.com/learnmore/labware_scientific_instruments/clinical_research_labware/dna_synthesizers.
- [42] Biology Insights, “What Is Enzymatic DNA Synthesis and How Does It Work?,” July 29, 2025, <https://biologyinsights.com/what-is-enzymatic-dna-synthesis-and-how-does-it-work/>.
- [43] Norbert Pardi, Michael J. Hogan, Frederick W. Porter, and Drew Weissman, “mRNA Vaccines - A New Era in Vaccinology,” *Nature Reviews Drug Discovery* 17 (2018): 261-279.
- [44] Bureau of Industry and Security, Department of Commerce, “Commerce Control List: Expansion of Controls on Certain Biological Equipment ‘Software,’” *Federal Register* 86, no. 190 (October 5, 2021): 54,814-54,819, <https://www.federalregister.gov/documents/2021/10/05/2021-21493/commerce-control-list-expansion-of-controls-on-certain-biological-equipment-software>.
- [45] Favour D. Makurvet, “Biologics vs. Small Molecules: Drug Costs and Patient Access,” *Medicine in Drug Discovery* 9 (2021): 100075, <https://doi.org/10.1016/j.medidd.2020.100075>.
- [46] Jack W. Scannell, Alex Blanckley, Helen Boldon, and Brian Warrington, “Diagnosing the Decline in Pharmaceutical R&D Efficiency,” *Nature Reviews Drug Discovery* 11 (2012): 191-200, <https://doi.org/10.1038/nrd3681>.
- [47] Doni Dermawan and Nasser Alotaqi, “From Lab to Clinic: How Artificial Intelligence (AI) Is Reshaping Drug Discovery Timelines and Industry Outcomes,” *Pharmaceuticals* 18, no. 7 (2025): 981, <https://doi.org/10.3390/ph18070981>.
- [48] D. Dermawan and F. Alotaqi, “Applications of Artificial Intelligence in Drug Discovery and Development: A Comprehensive Review,” *Biomolecules* 15, no. 4 (2025): 480, <https://doi.org/10.3390/biom15040480>.

- [49] Sarfaraz K. Niazi, "Artificial Intelligence in Small-Molecule Drug Discovery: A Critical Review," *Pharmaceuticals* 18, no. 9 (2025): 1271, <https://doi.org/10.3390/ph18091271>.
- [50] MedlinePlus Genetics, "What Are mRNA Vaccines and How Do They Work?," accessed August 2026, <https://medlineplus.gov/genetics/understanding/therapy/mrnavaccines/>.
- [51] H. Zhang, L. Zhang, A. Lin, C. Xu, Z. Li, K. Liu, B. Liu, et al., "Algorithm for Optimized mRNA Design Improves Stability and Immunogenicity," *Nature* 621 (2023): 396-403, <https://doi.org/10.1038/s41586-023-06127-z>.
- [52] *Nature Chemical Biology*, "AI-Powered Design Accelerates the Development of mRNA Therapeutics," *Nature Chemical Biology* 22 (2026): 15-16, <https://doi.org/10.1038/s41589-025-02074-0>.
- [53] Melody Redman, Andrew King, Caroline Watson, and David King, "What Is CRISPR/Cas9?," *Archives of Disease in Childhood: Education and Practice* 101, no. 4 (2016): 213-215, <https://doi.org/10.1136/archdischild-2016-310459>.
- [54] Vertex Pharmaceuticals Incorporated, CASGEVY (Exagamglogene Autotemcel) Suspension for Intravenous Infusion: Prescribing Information (Silver Spring, MD: U.S. Food and Drug Administration, 2023), <https://www.fda.gov/media/174615/download>.
- [55] National Center for Advancing Translational Sciences, "Cell Therapy," Rare Diseases Registry Program glossary, accessed August 2026, <https://registries.ncats.nih.gov/glossary/cell-therapy/>.
- [56] Ignas Mazelis et al., "Multistep Genomics on Single Cells and Live Cultures in Subnanoliter Capsules," *Science* 391 (2026): 1130-1137, <https://doi.org/10.1126/science.ady7209>.
- [57] Suzanne Day, "Combining Biology and AI to Advance Cell Therapy," Harvard Medical School, February 4, 2026, <https://hms.harvard.edu/news/combining-biology-ai-advance-cell-therapy>.
- [58] Yi Ni, Liwei Zhu, and Shuai Li, "Bio AI Agent: A Multi-Agent Artificial Intelligence System for Autonomous CAR-T Cell Therapy Development with Integrated Target Discovery, Toxicity Prediction, and Rational Molecular Design," *arXiv preprint*, 2025, <https://doi.org/10.48550/arXiv.2511.08649>.
- [59] *J. Clin. Med.*, "CAR-T-Cell-Based Cancer Immunotherapies: Potentials, Limitations, and Perspectives," *Journal of Clinical Medicine* 13, no. 11 (2024): 3202, <https://doi.org/10.3390/jcm13113202>.
- [60] A. S. Colina, V. Shah, R. K. Shah, T. Kozlik, R. K. Dash, S. Terhune, and A. E. Zamora, "Current Advances in Experimental and Computational Approaches to Enhance CAR T Cell Manufacturing Protocols and Improve Clinical Efficacy," *Frontiers in Molecular Medicine* 4 (2024): article 1310002, <https://doi.org/10.3389/fmmed.2024.1310002>.
- [61] Rose Lee, "Metagenomic Next Generation Sequencing: How Does It Work and Is It Coming to Your Clinical Microbiology Lab?," *American Society for Microbiology*, November 4, 2019, <https://asm.org/articles/2019/november/metagenomic-next-generation-sequencing-how-does-it>.
- [62] H. Duan, X. Li, A. Mei, P. Li, Y. Liu, X. Li, et al., "The Diagnostic Value of Metagenomic Next-Generation Sequencing in Infectious Diseases," *BMC Infectious Diseases* 21 (2021): 1-13, <https://doi.org/10.1186/s12879-020-05746-5>.
- [63] M. Morsli, Q. Kerharo, J. Delerce, P. H. Roche, L. Troude, and M. Drancourt, "Haemophilus influenzae Meningitis Direct Diagnosis by Metagenomic Next-Generation Sequencing: A Case Report," *Pathogens* 10 (2021): 461, <https://doi.org/10.3390/pathogens10040461>.
- [64] J. Chen, Y. Zhao, Z. Shang, Z. Lin, G. Xu, B. Bai, et al., "The Clinical Significance of Simultaneous Detection of Pathogens from Bronchoalveolar Lavage Fluid and Blood Samples by Metagenomic Next-Generation Sequencing in Patients with Severe Pneumonia," *Journal of Medical Microbiology* 70 (2021): 001259, <https://doi.org/10.1099/jmm.0.001259>.
- [65] Charles Y. Chiu and Steven A. Miller, "Clinical Metagenomics," *Nature Reviews Genetics* 20 (2019): 341-355, <https://doi.org/10.1038/s41576-019-0113-7>.
- [66] Patrick Benoit, Noah Brazer, Mikael de Lorenzi-Tognon, et al., "Seven-Year Performance of a Clinical Metagenomic Next-Generation Sequencing Test for Diagnosis of Central Nervous System Infections," *Nature Medicine* 30 (2024): 3522-3533, <https://doi.org/10.1038/s41591-024-03275-1>.
- [67] M. Batool and J. Galloway-Peña, "Clinical Metagenomics - Challenges and Future Prospects," *Frontiers in Microbiology* 14 (2023): 1186424, <https://doi.org/10.3389/fmicb.2023.1186424>.
- [68] Ying Yu, Yuanbang Mai, Yuanling Zheng, et al., "Assessing and Mitigating Batch Effects in Large-Scale Omics Studies," *Genome Biology* 25 (2024): 254, <https://doi.org/10.1186/s13059-024-03401-9>.
- [69] Alessandro Barberis, Hugo J. W. L. Aerts, and Francesca M. Buffa, "Robustness and Reproducibility for AI Learning in Biomedical Sciences: RENOIR," *Scientific Reports* 14 (2024): 1933, <https://doi.org/10.1038/s41598-024-51381-4>.
- [70] Timothy Clark, Harry Caufield, Jillian A. Parker, et al., "AI-Readiness for Biomedical Data: Bridge2AI Recommendations," *bioRxiv preprint*, posted October 25, 2024, <https://doi.org/10.1101/2024.10.23.619844>.
- [71] James Revill and Catherine Jefferson, "Tacit Knowledge and the Biological Weapons Regime," *Science and Public Policy* 41, no. 5 (2014): 597-610, <https://doi.org/10.1093/scipol/sct090>.
- [72] N. Teran and J. M. Yassif, *AlxBio Horizon Scan: Winter 2025-2026* (Washington, DC: Nuclear Threat Initiative, March 3, 2026).
- [73] D. Luckey, S. D. Muggy, T. Frey, D. Stebbins, T. Rissman, B. Espinosa, D. Tapia, et al., *Mitigating Risks at the Intersection of Artificial Intelligence and Chemical and Biological Weapons* (Santa Monica, CA: RAND Corporation, 2025).

- [74] Nuclear Threat Initiative, *The Convergence of Artificial Intelligence and the Life Sciences* (Washington, DC: Nuclear Threat Initiative, 2023), <https://www.nti.org/analysis/articles/the-convergence-of-artificial-intelligence-and-the-life-sciences/>.
- [75] Nuclear Threat Initiative, “Statement on Biosecurity Risks at the Convergence of AI and the Life Sciences,” July 17, 2025, <https://www.nti.org/analysis/articles/statement-on-biosecurity-risks-at-the-convergence-of-ai-and-the-life-sciences/>.
- [76] R. D. Arroyo-Olarte, R. Bravo Rodríguez, and E. Morales-Ríos, “Genome Editing in Bacteria: CRISPR-Cas and Beyond,” *Microorganisms* 9, no. 4 (2021): 844, <https://doi.org/10.3390/microorganisms9040844>.
- [77] H. Boubakri, “CRISPR-Cas9-Mediated Genome Editing in Fungi: Applications, Challenges, and Future Directions,” *Journal of Applied Microbiology* 137, no. 3 (2026): ixag046, <https://doi.org/10.1093/jambio/ixag046>.
- [78] S. H. King, C. L. Driscoll, D. B. Li, D. Guo, A. T. Merchant, G. Brix, M. E. Wilkinson, and B. L. Hie, “Generative Design of Novel Bacteriophages with Genome Language Models,” *bioRxiv preprint*, 2025, <https://doi.org/10.1101/2025.09.12.675911>.
- [79] A. J. Leikas, S. Ylä-Herttuala, and J. E. K. Hartikainen, “Adenoviral Gene Therapy Vectors in Clinical Use: Basic Aspects with a Special Reference to Replication-Competent Adenovirus Formation and Its Impact on Clinical Safety,” *International Journal of Molecular Sciences* 24, no. 22 (2023): 16519, <https://doi.org/10.3390/ijms242216519>.
- [80] U.S. Food and Drug Administration, Center for Biologics Evaluation and Research, *Design and Analysis of Shedding Studies for Virus or Bacteria-Based Gene Therapy and Oncolytic Products: Guidance for Industry* (Silver Spring, MD: U.S. Food and Drug Administration, August 2015).
- [81] K. Zhao, Y. Yan, X.-K. Jin, T. Pan, S.-M. Zhang, C.-H. Yang, Z.-Y. Rao, and X.-Z. Zhang, “An Orally Administered Gene Editing Nanoparticle Boosts Chemo-Immunotherapy in Colorectal Cancer,” *Nature Nanotechnology* 20 (2025): 935-946, <https://doi.org/10.1038/s41565-025-01904-5>.
- [82] National Academies of Sciences, Engineering, and Medicine, “Related Developments That May Impact the Ability to Effect an Attack Using a Synthetic Biology-Enabled Weapon,” in *Biodefense in the Age of Synthetic Biology* (Washington, DC: National Academies Press, 2018), 85-94, <https://doi.org/10.17226/24890>.
- [83] National Institute of Standards and Technology, “Biosecurity for Synthetic Nucleic Acid Sequences,” July 30, 2025, <https://www.nist.gov/programs-projects/biosecurity-synthetic-nucleic-acid-sequences>.
- [84] World Health Organization, *Health Emergency Preparedness, Response and Resilience: Draft Report* (Geneva: World Health Organization, June 30, 2024), https://cdn.who.int/media/docs/default-source/emergency-preparedness/who_hepr_june30draftforconsult.pdf?sfvrsn=e6117d2c_4&download=true.
- [85] F. Xu et al., “Emerging and Reemerging Infectious Diseases: Global Trends and New Strategies,” *Signal Transduction and Targeted Therapy* 9 (2024): 223, <https://doi.org/10.1038/s41392-024-01917-x>.
- [86] World Health Organization, “Prioritizing Diseases for Research and Development in Emergency Contexts,” accessed August 2026, <https://www.who.int/activities/prioritizing-diseases-for-research-and-development-in-emergency-contexts>.
- [87] World Health Organization, “2018 Annual Review of Diseases Prioritized under the Research and Development Blueprint,” event page, February 6-7, 2018, <https://www.who.int/news-room/events/detail/2018/02/06/default-calendar/2018-annual-review-of-diseases-prioritized-under-the-research-and-development-blueprint>.
- [88] World Health Organization, “WHO’s Response to Hantavirus Cases Linked to a Cruise Ship,” note for media, May 7, 2026, <https://www.who.int/news/item/07-05-2026-who-s-response-to-hantavirus-cases-linked-to-a-cruise-ship>.
- [89] John A. Lednicky, “Hantavirus, Explained,” University of Florida College of Public Health and Health Professions, May 8, 2026, <https://phhp.ufl.edu/2026/05/08/hantavirus-explained/>.
- [90] MSN, “Hantavirus Cruise Passengers Will Be Evacuated Soon, Report Says: Latest Updates,” accessed August 2026, <https://www.msn.com/en-us/travel/news/hantavirus-cruise-passengers-will-be-evacuated-soon-report-says-latest-updates/ar-AA22rrN8>.
- [91] Centers for Disease Control and Prevention, “About Andes Virus,” accessed August 2026, <https://www.cdc.gov/hantavirus/about/andesvirus.html>.
- [92] European Centre for Disease Prevention and Control, “ECDC Publishes Guidance for Management of Passengers Linked to Andes Hantavirus Outbreak on Cruise,” accessed August 2026, <https://www.ecdc.europa.eu/en/news-events/ecdc-publishes-guidance-management-passengers-linked-andes-hantavirus-outbreak-cruise>.
- [93] David Chisompola, Emmanuel Luwaya, John Nzobokela, Phinnoty Mwansa, and Martin Chakulya, “AI-Powered Analysis of Viral Metagenomic Sequencing Data for Rapid Outbreak Investigation and Novel Pathogen Discovery,” *Frontiers in Microbiology* 16 (2026): 1717859, <https://doi.org/10.3389/fmicb.2025.1717859>.
- [94] Google Cloud, “Retrieval-Augmented Generation,” accessed August 2026, <https://cloud.google.com/use-cases/retrieval-augmented-generation>.
- [95] Administration for Strategic Preparedness and Response, “Biosafety Level Requirements,” accessed August 2026, <https://aspr.hhs.gov/S3/Pages/Biosafety-Level-Requirements.aspx>.

- [96] Garanord MD, "The Role of International Laws and Treaties in Controlling Biological Weapons," accessed August 10, 2026, <https://garanord.md/the-role-of-international-laws-and-treaties-in-controlling-biological-weapons/>.
- [97] Y. Bengio, G. Hinton, A. Yao, D. Song, P. Abbeel, A. Darrell, Y. N. Harari, et al., "Managing Extreme AI Risks amid Rapid Progress," *Science* 384, no. 6698 (2024): 842-845, <https://doi.org/10.1126/science.adn0117>.
- [98] C. Autio, R. Schwartz, J. Dunietz, S. Jain, M. Stanley, E. Tabassi, P. Hall, and K. Roberts, *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile*, NIST AI 600-1 (Gaithersburg, MD: National Institute of Standards and Technology, 2024), <https://doi.org/10.6028/NIST.AI.600-1>.
- [99] OpenAI, *Preparedness Framework, Version 2* (San Francisco: OpenAI, April 15, 2025).
- [100] S. Nevo, D. Lahav, A. Karpur, Y. Bar-On, H. A. Bradley, and J. Alstott, *Securing AI Model Weights: Preventing Theft and Misuse of Frontier Models*, RR-A2849-1 (Santa Monica, CA: RAND Corporation, 2024), <https://doi.org/10.7249/RR-A2849-1>.
- [101] C. Bullock, S. Van Arsdale, M. Arnold, M. Maas, and C. Winter, *Existing Authorities for Oversight of Frontier AI Models* (Institute for Law & AI, July 2024), <https://law-ai.org/existing-authorities-for-oversight>.
- [102] U.S. Government Accountability Office, *Artificial Intelligence: Federal Efforts Guided by Requirements and Advisory Groups*, GAO-25-107933 (Washington, DC: U.S. Government Accountability Office, September 2025).
- [103] D. E. Walters and H. J. Wiseman, "Self-Regulation in Emerging and Innovative Industries," *Houston Law Review* 62, no. 3 (2025): 543-610, <https://houstonlawreview.org/article/129432-self-regulation-in-emerging-and-innovative-industries>.
- [104] Gillian K. Hadfield and Jack Clark, "Regulatory Markets: The Future of AI Governance," *Jurimetrics* 65, no. 2 (2026): 195-240.
- [105] Anthropic, *Responsible Scaling Policy, Version 3.1* (San Francisco: Anthropic, April 2, 2026).
- [106] Executive Order No. 14,148, "Initial Rescissions of Harmful Executive Orders and Actions," 90 Fed. Reg. 8,237 (January 28, 2025), <https://www.federalregister.gov/documents/2025/01/28/2025-01901/initial-rescissions-of-harmful-executive-orders-and-actions>.
- [107] Executive Order No. 14,179, "Removing Barriers to American Leadership in Artificial Intelligence," 90 Fed. Reg. 8,741-8,742 (January 31, 2025), <https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence>.
- [108] The White House, *America's AI Action Plan* (Washington, DC: The White House, July 2025), <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf>.
- [109] Executive Order No. 14,365, "Ensuring a National Policy Framework for Artificial Intelligence," 90 Fed. Reg. 58,499 (December 16, 2025).
- [110] *Transparency in Frontier Artificial Intelligence Act*, S.B. 53, 2025-2026 Reg. Sess., ch. 138 (Cal. 2025), https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=202502060SB53.
- [111] *Responsible AI Safety and Education Act*, S. 6953-B, 2025-2026 Leg. Sess., ch. 699 (N.Y. 2025), <https://www.nysenate.gov/legislation/bills/2025/S6953/amendment/B>.
- [112] Executive Order No. 14,409, "Promoting Advanced Artificial Intelligence Innovation and Security," signed June 2, 2026, <https://www.whitehouse.gov/presidential-actions/2026/06/promoting-advanced-artificial-intelligence-innovation-and-security/>.
- [113] *Artificial Intelligence and Biosecurity Risk Assessment Act*, S. 2399, 118th Cong. (2023).
- [114] *Strategy for Public Health Preparedness and Response to Artificial Intelligence Threats Act*, S. 2346, 118th Cong. (2023).
- [115] *Strategy for Public Health Preparedness and Response to Artificial Intelligence Threats Act*, S. 501, 119th Cong. (2025), <https://www.govinfo.gov/content/pkg/BILLS-119s501is/pdf/BILLS-119s501is.pdf>.
- [116] *Generative AI Terrorism Risk Assessment Act*, H.R. 1736, 119th Cong. (2025), U.S. Government Publishing Office, November 12, 2025.
- [117] U.S. Department of Health and Human Services, *Administration for Strategic Preparedness and Response, Screening Framework Guidance for Providers and Users of Synthetic Nucleic Acids* (Washington, DC: U.S. Department of Health and Human Services, October 2023), <https://aspr.hhs.gov/S3/Documents/SynNA-Guidance-2023.pdf>.
- [118] Alexander Graf, "How to Extract the Spike Sequence of the Omicron Variant from Uploaded Samples at GISAID?," Bay-VOC, November 30, 2021, https://bay-voc.lgl.bayern.de/faq/sarsCov2_spike.xhtml.
- [119] National Science and Technology Council, *Framework for Nucleic Acid Synthesis Screening* (Washington, DC: Office of Science and Technology Policy, April 29, 2024).
- [120] National Institutes of Health, "4.1.25 Public Health Security," in *NIH Grants Policy Statement* (Bethesda, MD: National Institutes of Health, March 2026), https://grants.nih.gov/grants/policy/nihgps/HTML5/section_4/4.1.25_public_health_security.htm.
- [121] Office of Science and Technology Policy, *United States Government Policy for Oversight of Dual Use Research of Concern and Pathogens with Enhanced Pandemic Potential* (Washington, DC: Office of Science and Technology Policy, May 6, 2024).

- [122] Executive Order No. 14,292, “Improving the Safety and Security of Biological Research,” 90 Fed. Reg. 19,611 (2025).
- [123] National Defense Authorization Act for Fiscal Year 2026, Pub. L. No. 119-60, § 851 (2025).
- [124] Biosecurity Modernization and Innovation Act of 2026, S. 3741, 119th Cong. (2026).
- [125] Securing Gene Synthesis Act, H.R. 4702, 118th Cong. (2023).
- [126] Nucleic Acid Standards for Biosecurity Act, H.R. 3029, 119th Cong. (2025).
- [127] Imai N, et al., Report 2: Estimating the potential total number of novel Coronavirus (2019-nCoV) cases in Wuhan City, China. (2020).
- [128] Qun Li et al., “Early Transmission Dynamics in Wuhan, China, of Novel Coronavirus-Infected Pneumonia,” *New England Journal of Medicine* 382 (2020): 1199-1207, <https://doi.org/10.1056/NEJMoa2001316>.
- [129] Natsuko Imai, Ilaria Dorigatti, Anne Cori, Steven Riley, and Neil M. Ferguson, Report 2: Estimating the Potential Total Number of Novel Coronavirus Cases in Wuhan City, China (London: Imperial College London, January 22, 2020), <https://www.imperial.ac.uk/media/imperial-college/medicine/sph/ide/gida-fellowships/Imperial-College-COVID19-update-epidemic-size-22-01-2020.pdf>.
- [130] Donald J. Trump, “Declaring a National Emergency Concerning the Novel Coronavirus Disease (COVID-19) Outbreak,” proclamation, March 13, 2020, <https://trumpwhitehouse.archives.gov/presidential-actions/proclamation-declaring-national-emergency-concerning-novel-coronavirus-disease-covid-19-outbreak/>.
- [131] International Trade Administration, “I-94 Arrivals: Historical Data,” accessed August 2026, <https://www.trade.gov/i-94-arrivals-historical-data>.
- [132] Centers for Disease Control and Prevention, “Policy and Standards,” Data Modernization Initiative, accessed August 2026, <https://www.cdc.gov/data-modernization/php/policy-standards/index.html>.
- [133] M. Wang, Z. Zhang, A. S. Bedi, A. Velasquez, S. Guerra, S. Lin-Gibson, L. Cong, et al., “A Call for Built-In Biosecurity Safeguards for Generative AI Tools,” *Nature Biotechnology* 43 (2025): 845-847, <https://doi.org/10.1038/s41587-025-02650-8>.
- [134] Andreessen Horowitz, “David Sacks: AI, crypto, China, Dems, and SF [Audio podcast episode],” In The a16z Show. (2025).
- [135] G. Weil, M. Pistillo, S. Van Arsdale, J. Ikegami, K. Onuma, M. Okawa, and M. A. Osborne, Insuring Emerging Risks from AI (Oxford Martin AI Governance Initiative; Institute for Law & AI; Aioi R&D Lab Ltd.; Aioi Nissay Dowa Insurance Co. Ltd.; Touro University Jacob D. Fuchsberg Law Center, November 14, 2024).
- [136] R. Henson, “Government-Backed Insurance for Artificial Intelligence Technologies,” *Georgia State University Law Review* 41 (2025): 559.
- [137] Munich Re, Generating Content with AI: An IP-Infringement Minefield (Munich: Munich Re, 2024).
- [138] Armilla AI, “AI Insurance - Lloyd’s Coverholder,” accessed August 2026, <https://armilla.ai/>.
- [139] G. Smith, “Licensing Frontier AI Development: Legal Considerations and Best Practices,” *Lawfare*, January 3, 2024, <https://www.lawfaremedia.org/article/licensing-frontier-ai-development-legal-considerations-and-best-practices>.
- [140] Allison Berke, Risk-Based Categorization and Governance of Biological Data in AI Systems (Baltimore: Johns Hopkins Bloomberg School of Public Health, Center for Health Security, March 2026).
- [141] METR, Common Elements of Frontier AI Safety Policies (Berkeley, CA: METR, 2025).
- [142] International Organization for Standardization, “ISO/IEC JTC 1/SC 42: Artificial Intelligence,” accessed August 2026.
- [143] L. Galante and T. Feldman, “Technical Standards: America’s Forgotten Tool of Statecraft,” *Lawfare*, October 23, 2025.
- [144] S. Nyman, Standards and Competition (Washington, DC: World Bank Group, 2025).
- [145] A. Garcia-Herrero, M. Krystianczuk, N. Poitiers, and P. Weil, Standard Setting in the Field of Emerging Digital Technologies (Washington, DC: German Marshall Fund of the United States, 2023).
- [146] Grand View Research, “Nucleotides Market Size, Share and Trends Analysis Report,” accessed August 2026, <https://www.grandviewresearch.com/industry-analysis/nucleotides-market>.
- [147] Arc Institute, “Evo 2,” accessed August 2026, <https://arcinstitute.org/>.
- [148] Bureau of Industry and Security, Department of Commerce, “Proliferation of Chemical and Biological Weapons,” 15 C.F.R. § 742.2 (May 1, 2026), <https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-742/section-742.2>.
- [149] ASSET, “Epidemic Intelligence,” 2015, <https://www.asset-scienceinsociety.eu/pages/epidemic-intelligence>.
- [150] J. Kaur and Z. A. Butt, “AI-Driven Epidemic Intelligence: The Future of Outbreak Detection and Response,” *Frontiers in Artificial Intelligence* 8 (2025): 1645467, <https://doi.org/10.3389/frai.2025.1645467>.
- [151] Centers for Disease Control and Prevention, “National Syndromic Surveillance Program,” accessed August 2026, <https://www.cdc.gov/nssp/index.html>.
- [152] Centers for Disease Control and Prevention, “One CDC Data Platform,” accessed August 2026, <https://www.cdc.gov/data-modernization/php/one-cdc-data-platform/index.html>.

- [153] Carly Adams, Megan Bias, Rory M. Welsh, Jenna Webb, Heather Reese, Stephen Delgado, John Person, Rachel West, Soo Shin, and Amy Kirby, "The National Wastewater Surveillance System (NWSS): From Inception to Widespread Coverage, 2020-2022, United States," *Science of the Total Environment* 926 (2024): 171566, <https://doi.org/10.1016/j.scitotenv.2024.171566>.
- [154] Centers for Disease Control and Prevention, "About Wastewater Data," *Wastewater Monitoring*, last updated April 10, 2026, <https://www.cdc.gov/wastewater/about-data/index.html>.
- [155] LegalClarity.org, "DHS BioWatch Program: Purpose, Scope, and Legal Authority," accessed August 2026, <https://legalclarity.org/dhs-biowatch-program-purpose-scope-and-legal-authority/>.
- [156] Global Biodefense, "Genomics and U.S. Public Health Surveillance," August 29, 2025, <https://globalbiodefense.com/2025/08/29/genomics-us-public-health-surveillance/>.
- [157] N. R. Minor, M. D. Ramuta, M. R. Stauss, et al., "Metagenomic Sequencing Detects Human Respiratory and Enteric Viruses in Air Samples Collected from Congregate Settings," *Scientific Reports* 13 (2023): 21398, <https://doi.org/10.1038/s41598-023-48352-6>.
- [158] X. Zhuang, V. Vo, M. A. Moshi, et al., "Early Detection of Emerging SARS-CoV-2 Variants from Wastewater through Genome Sequencing and Machine Learning," *Nature Communications* 16 (2025): 6272, <https://doi.org/10.1038/s41467-025-61280-5>.
- [159] Clinical Lab Products, "Wastewater Surveillance Backed by AI Can Enhance Detection of Emerging Viruses," accessed August 2026, <https://clpmag.com/disease-states/infectious-diseases/wastewater-surveillance-backed-by-ai-can-enhance-detection-of-emerging-viruses/>.
- [160] Hin Fung Tsang, "Metagenomic Next-Generation Sequencing in Infectious Diseases: Clinical Applications, Translational Challenges, and Future Directions," *Diagnostics* 15, no. 16 (2025): 1991, <https://doi.org/10.3390/diagnostics15161991>.
- [161] J. K. Tan, V. Servellita, D. Stryke, et al., "Laboratory Validation of a Clinical Metagenomic Next-Generation Sequencing Assay for Respiratory Virus Detection and Discovery," *Nature Communications* 15 (2024): 9016, <https://doi.org/10.1038/s41467-024-51470-y>.
- [162] Centers for Disease Control and Prevention, "Outbreak Case Definitions," accessed August 2026, <https://www.cdc.gov/urdo/php/surveillance/outbreak-case-definitions.html>.
- [163] Centers for Disease Control and Prevention, *Guideline for Isolation Precautions: Preventing Transmission of Infectious Agents in Healthcare Settings* (Atlanta: Centers for Disease Control and Prevention), <https://www.cdc.gov/infection-control/media/pdfs/Guideline-Isolation-H.pdf>.
- [164] European Society for Clinical Virology Network on Next-Generation Sequencing, "Recommendations for the Introduction of Metagenomic High-Throughput Sequencing in Clinical Virology, Part I: Wet Lab Procedure," *Journal of Clinical Virology* 141 (2021): 104908, <https://doi.org/10.1016/j.jcv.2021.104908>.
- [165] Health Centre, "Advantages and Disadvantages of Inactivated Vaccines," accessed August 2026, <https://www.healthcentre.org.uk/vaccine/advantages-disadvantages-inactivated-vaccines.html>.
- [166] Kai Yuan Leong, Seng Kong Tham, and Chit Laa Poh, "Revolutionizing Immunization: A Comprehensive Review of mRNA Vaccine Technology and Applications," *Virology Journal* 22 (2025): 71, <https://doi.org/10.1186/s12985-025-02645-6>.
- [167] Centers for Disease Control and Prevention, "How COVID-19 Vaccines Work," accessed August 2026, <https://www.cdc.gov/covid/vaccines/how-they-work.html>.
- [168] C. Markosian et al., "Genetic and Structural Analysis of SARS-CoV-2 Spike Protein for Universal Epitope Discovery," *Molecular Biology and Evolution* 39, no. 5 (2022): msac091, <https://doi.org/10.1093/molbev/msac091>.
- [169] Moderna, "Product Pipeline," accessed August 2026, <https://www.modernatx.com/en-US/research/product-pipeline>.
- [170] National Institutes of Health, "Statement from NIH, BARDA, and FDA on Emergency Use Authorization of the Moderna COVID-19 Vaccine," news release, December 18, 2020, <https://www.nih.gov/news-events/news-releases/statement-nih-barda-fda-emergency-use-authorization-moderna-covid-19-vaccine>.



Belfer Center for Science and International Affairs

Harvard Kennedy School

79 JFK Street

Cambridge, MA 02138

www.belfercenter.org



HARVARD Kennedy School
BELFER CENTER

50 YEARS
OF RESEARCH, POLICY,
AND LEADERSHIP