PROCEEDINGS
OF
LONDON INTERNATIONAL CONFERENCES

eISSN 2977-1870

Examining Dual-Use Risks in Biotechnological Supply Chains: The Contribution of Empathic AI in Reducing Threats Posed by Pathogens with Increased Pandemic Potential

Christina Schabasser*

Abstract

This research investigates the dual-use dilemma in technology supply chains and how empathic AI can address such a dilemma. The literature reviewed for this study revealed that AI has the potential to enhance supply chain management by clarifying and early detecting anomalies in biotechnology development and adoption. Over 90 percent of this research's survey respondents agreed that AI can play a major role in securing biotechnology adoption through early detection, with them considering traceability a top priority in the process. Experts interviewed by the researcher believed that dual-use risks of biotechnology development revolve around the misuse of research findings, uncontrolled pathogen modification, and ethical concerns that may lead to societal backlash. In this context, they proposed empathic AI as a potential solution due to its ability to provide early detection, monitoring measures, and ethical guidance for biotechnology adoption, offering actionable insights into how policymakers and stakeholders should develop AI to mitigate the risks.

Keywords: biotech supply chains, AI, dual-use research, empathic AI, biosecurity

https://doi.org/10.31039/plic.2025.14.335

* University of Sopron, Hungary christina.schabasser@live.at

Introduction

The anthrax attacks in the United States in 2001 demonstrated that dual-use is not merely an abstract danger. This historically-documented example of the misuse of biological agents indicated how serious the threat of bioterrorism can be. The bioterror attacks occurred shortly after the attacks of September 11, 2001 in the midst of increased nationwide fear and uncertainty. The first case occurred on October 4, 2001, after a photo editor at a Florida media outlet was diagnosed with pulmonary anthrax. Letters containing anthrax were sent to various media outlets and the offices of U.S. senators. By late November 2001, the outbreak appeared to have subsided, with no additional contaminated letters detected. Overall, 22 people became infected, either with cutaneous or pulmonary anthrax, and five of the pulmonary cases resulted in death. Contamination was found in media offices, postal facilities, and congressional buildings. Government offices and postal services were disrupted, and some buildings were closed for over a year. The cost of cleanup and decontamination amounted to tens of millions of dollars. Fears of bioterrorism through the postal system increased public concern (Center for Counterproliferation Research, 2002).

This tension between benefits and risks associated with biotechnological products is often referred to as the "dual-use dilemma." Today, life scientists face such a dilemma; on one hand, advances in biotechnology can yield significant medical benefits, while on the other hand, they pose the risk of misuse for creating biological weapons. Unlike nuclear physics development which is inaccessible to most people, thus allowing innovations like nuclear fission to be used for both peaceful purposes (e.g., energy, medicine) and the development of weapons of mass destruction, biological research results are openly accessible, increasing the likelihood of misuse. Biological weapons are less costly to produce, with the estimated costs of causing civilian casualties being approximately one dollar per square kilometer, compared to 800 and 2,000 dollars per square kilometer for nuclear and conventional weapons, respectively. They also involve less technical complexity than nuclear weapons. Predicting or preventing a bioterrorism attack is difficult, but the likelihood of an attack should not be underestimated. Therefore, investment in defense should be warranted. What makes biological weapons so insidious is that the effects of an attack are not immediately noticeable. However, immediate treatment of the victims is crucial for their survival (Selgelid, 2009; Saunders-Hastings, 2014).

One question arises in the field of global biotechnological supply chains, where high complexity is derived from various global participants worldwide: How can safety concerns be effectively addressed? All actors involved in the supply chain must be vigilant in addressing biosecurity risks. They include, for example, providers and equipment manufacturers, who should strengthen cyber and informational security measures to protect intellectual property and customer information. Some of the cybersecurity measures they may consider include customer screening processes, prevention of unauthorized access or manipulation of equipment, and integration of screening capabilities for sequences of concern into their devices (Adamson & Allen, 2025). They also need to monitor the supply chain of the dual-use biotechnology products from the manufacturer to the end user (Samundeswari et al., 2023).

It becomes increasingly evident that artificial intelligence, as a dual-use technology, can both enhance and threaten the security of biotechnological supply chains at the same time. This duality highlights the critical need for robust safeguards to maximize benefits while minimizing the risks of misuse.

This study investigates how artificial intelligence (AI) can enhance transparency, traceability, and security in biotech supply chains while minimizing misuse risks. It also discusses AI-enabled security concerns. The study includes a literature review, presents the research methodology involving expert and public surveys, analyzes the results, and concludes with a discussion.

Literature

Biotechnology has advanced significantly due to laboratory automation, increased access to data, and progress in computational biology (Schabacker et al., 2019).

The following figures show the strong growth characterizing the biotechnology market: according to estimates, the global biotechnology market size was USD 1.55 trillion in 2023 and is forecast to reach USD 3.88 trillion by 2030 (Grand View Research, 2023).

Biotechnology enables precise modification of genetic material for medical and agricultural purposes (Shinomiya & Tanaka, n.d.). Biotechnology encompasses the application of technological approaches to engineering. It also manipulates and monitors living systems, including genome sequencing, DNA synthesis, recombinant protein production, plant and animal breeding, alternative protein development, and biofuel generation. Biological technology enables the transformation of different aspects of human life, introducing unprecedented changes (Nature Biotechnology, 2021).

Pathogens with Increased Pandemic Potential are particularly noteworthy, as research in this area also affects the global population (Eyal, Leshabari, & Sarker, 2024). These kinds of pathogens, modified through laboratory experiments, may lead to widespread and uncontrolled transmission with an increased risk of moderate to severe illness and/or death in humans (Gillum, 2024). One recommendation in this regard is to include global populations and their representatives in consultation and decision-making processes (Eyal, Leshabari, & Sarker, 2024).

In addition to the positive aspects of biotechnology, it is also prone to considerable safety concerns (Schabacker et al., 2019). However, it is crucial to clarify the purpose of biotechnology, mainly because the techniques to create a bioweapon are similar to those for legitimate research (Baillie, Dyson, & Simpson, 2012).

For example, the increasing prevalence of biological research in the digital environment also increases the potential for its misuse. Therefore, evolving risks must be managed effectively. Innovations in genetic engineering (e.g., CRISPR-Cas9 systems), as well as the convergence of laboratory automation, computational biology, and access to publicly accessible genome databases, pose risks. The combination of publicly available genome databases, biofactories, laboratory automation, and computational biology can increase the risk of misuse in the production of highly dangerous biological agents and toxins. Physical samples are no longer required for their design and production. The prohibited production of new, highly dangerous biological agents and toxins is also conceivable (Schabacker et al., 2019).

There are currently no guaranteed technical safeguards for genome editing. The ability to alter life at the genomic level is raising increasing concern about the consequences of genome editing. There are concerns about the potential for eugenic practices and possible consequences for the descendants of individuals with edited genomes. Although the editing of fertilized human embryos has not yet been approved anywhere, genome editing is currently undergoing laboratory testing around the world (Shinomiya & Tanaka, n.d.).

The new risks in biotechnology cannot be addressed with existing methods, such as background checks and registration by institutions (Schabacker et al., 2019).

In research on pathogens with increased pandemic potential, it was recommended that the upstream phase of such high-risk research should address the question of whether the research should be conducted at all. Ethical guidelines, such as the Nuremberg Code and the Belmont Report, provide fundamental principles for such decisions. The midstream phase clarifies how the research should be conducted to ensure that the research meets the highest standards of biosafety and biosecurity. Collaboration between scientists, biosafety and biosecurity experts, policymakers, ethicists, and the public is essential for research in the field of pathogens with increased pandemic potential in a safe manner while simultaneously enabling scientific innovation. The downstream phase clarifies how the research results should be used. An additional problem lies in the inconsistency of the relevant guidelines of the leading scientific journal (Gillum, 2024).

The dual-use nature of biotechnology is also evident in the reactions and publications of countries. In 2004, the so-called 'Fink Report' of the US National Academies of Science was published. It emphasizes social responsibility in biotechnology research and oversees a special responsibility not only on behalf of researchers and research institutions, but also publishers, governments, and funding organizations. In 2005, the IAP Statement on Biosecurity was published by the InterAcademy Panel, which contains a code of conduct for scientists consisting of the five aspects: (1) awareness, (2) safety and security, (3) education and information, (4) accountability, and (5) oversight. With its strategic biotechnology program, China is trying not only to protect itself against potential biological risks but also to increasing its own technological development. At the same time, China emphasizes the importance of biotechnology for military use. In 2024, the European Commission released the report "Building the Future with Nature: Boosting Biotechnology and Biomanufacturing in the EU", highlighting biotechnology as one of ten technological fields particularly relevant to the security of the European economy (Shinomiya & Tanaka, n.d.). It is often argued that scientists have a moral obligation to prevent the misuse of their research since they best facilitate the inherent potential for abuse (Baillie, Dyson, & Simpson, 2012).

However, the risks and safety concerns are not limited to the laboratory environment. The growing complexity of pharmaceutical supply chains, including those for biotechnology products, makes them vulnerable to threats such as contamination, counterfeiting, and sabotage (Youvan, 2024).

The vulnerabilities that exist in the pharmaceutical supply chain also apply to the biotechnology supply chain, which is particularly vulnerable due to product sensitivity. For example, supply chain vulnerabilities could arise in the areas of manufacturing, packaging, and distribution. The precise control and monitoring required for the manufacture of complex biotech products, for example, cannot be met if part of the process is outsourced to facilities in countries with less stringent regulatory frameworks. One of the most common risks includes incorrect labeling or packaging errors, which may lead to dangerous situations. This risk particularly applies to sensitive biotechnology products that require precise handling and storage conditions. The distribution stage of the supply chain also carries risks. Products are distributed to customers through a network of wholesalers, distributors, and retailers, making them vulnerable to theft, diversion, and the introduction of counterfeit products. Counterfeit products typically enter legitimate supply chains via rogue distributors or poorly regulated markets. The elaborate nature of distribution networks, especially in developing countries, poses difficulties for authorities to inspect the integrity of every shipment (Youvan, 2024).

The biotech supply chain is not immune to manipulation in the development and production of biological processes, such as cyberattacks. It is therefore also exposed to digital threats. Attackers may corrupt important data, which would have negative consequences for the integrity and quality of biological products. Sabotage of security systems could result in physical or digital security vulnerabilities that could destabilize the entire biotech supply chain (Murch et al., 2018).

Despite the creation of regulatory frameworks for greater security, security gaps remain. For example, the US regulatory system for synthetic biology focuses on how the products are used, not how they are manufactured, because overly strict regulations on the manufacturing process could hinder trade and research. Unfortunately, these rules may not prevent those seeking to misuse the technology from obtaining the necessary materials. Further gaps in the supply chain could be exploited to the detriment of safety. Some organisms are exempt from EPA (Environmental Protection Agency) regulatory rules, which require commercial producers of microorganisms to obtain special permits for certain activities. These regulatory exemptions can provide a loophole for misuse: a manufacturer could take an organism exempt from regulation, insert a synthetic DNA segment, and create a threat. Furthermore, it is highly risky if laboratories fail to do so. In addition, the rapid development of new technologies opens the door to uncertainty through the creation of many microbes and modified products, as well as incomplete monitoring by authorities. Rules are in place for screening synthetic DNA, but they only address basic rules. Many companies lack the ability to find all dangerous sequences, and adhering to the rules is not mandatory. Moreover, manufacturers are typically unaware of how the supply chain works, thus increasing safety risks. (Frazar et al., 2017).

Pathogen genome sequencing (PGS), a sub-field of biotechnology, is widely used in disease surveillance and control, global and local disease control programs, as well as the monitoring of resistant pathogens. The PGS supply chain comprises four groups of actors: (1) Laboratories (e.g., national health laboratories, academic institutions, research centers), (2) Distributors and logistics intermediaries (including freight carriers, forwarders, and clearing agents), (3) Manufacturers – produce the required PGS materials and equipment, and (4) partners who play a facilitating role in the PGS ecosystem, such as donor agencies and external laboratories that have supported the setup of PGS facilities and the procurement of materials. The sustainable functioning of PGS laboratories depends on reliable supply chains for reagents and equipment. PGS supply chains in low-income countries often remain underdeveloped. Pathogen genomic sequencing labs are often immature in terms of their supply chain management (SCM), and they assign a low priority to SCM. Challenges that may arise in PGS supply chains (some of which are more likely in low-income or resource-limited regions) include: (1) Compliance with cold chain requirements throughout the supply chain during customs-related processes, which is complex and may lead to increased costs as well as the need for investment in the cold chain infrastructure; (2) Variable and often long lead times for PGS materials which increase the risk of product expiration or damage and can result in stock shortages; (3) Lengthy and inconsistent customs clearance procedures which extend delivery times and jeopardize the integrity of the cold chain; (4) Technical issues with PGS equipment and platforms which include malfunctions, installation and repair requirements, and concerns regarding maintenance and service agreement; and (5) PGS laboratories which have limited, uncertain, and unsustainable budgets and often rely on external support, affecting the resilience and reliability of their supply chains (Bam et al., 2023).

The value chain of potentially dangerous microbes spans collection, transport, laboratory handling, testing procedures, waste disposal, and storage in biobanks. The pathogen value chain involves inherent risks and demands rigorous analysis and robust mitigation strategies to avert spillover (e.g., transmission of pathogens to humans). Inherent risks can result from insufficient biosafety and biosecurity measures in both field collection and research laboratory settings.

Safe management of infectious waste remains critical along the pathogen value chain, as improper disposal can compromise biocontainment measures. Standardized procedures for handling, treatment, and disposal of pathogens significantly reduce this risk. Throughout the pathogen value chain, infectious waste management remains an ongoing concern, as improper disposal increases the risk of breaching biocontainment. Thorough protocols covering pathogen segregation, packaging, treatment, validation, and disposal reduce related risks. A strategic and all-encompassing approach aimed at detecting risks accompanying the complete pathogen value chain should enhance safety and protective measures at every stage, including the collection and testing of samples in the field as well as the transportation, laboratory handling, waste disposal, and management of biorepositories. Strengthening monitoring, biosafety, and biosecurity measures along the value chain requires innovative protocols, global cooperation, transparency, and governance. Enhanced tamper-proof tracking, remote monitoring, and integrated communication systems improve the security of the pathogen supply chain, while backup cold storage, authorized personnel access, and routine audits strengthen the protection of archived bioprobes (Karlsson et al., 2024).

After reviewing the risks and safety concerns regarding biotechnology and its supply chains, the question arises of how artificial intelligence (AI) can leverage AI to enhance safety in biotech supply chains.

Researchers have been promoting the adoption of AI to enhance supply chain resilience by enabling adaptation to and recovery from disruptions, thereby maintaining its functionality, including encouraging the use of AI technologies (e.g., Machine Learning (ML), predictive analytics, automation, and robotics). An example of such adaptation is the use of AI technologies (e.g., AI-powered scenario planning and simulation models) in the recovery process, which may facilitate post-disruption analysis and contingency planning to enable supply chain recovery measures (Saad Al-Naimi, 2025).

The Biological Weapons Convention (BWC) aims to prevent the development and use of biological weapons by addressing the dual-use nature of certain biotechnologies. Implementation is carried out through commitments and voluntary information-sharing by member states. Unfortunately, this framework still lacks a formal inspection or verification mechanism, leaving it vulnerable to violations, as exemplified by the Soviet Union's covert biological weapons program. Future international AI agreements in the field of biotechnology, thus, should draw lessons from existing security treaties such as the BWC, particularly regarding verification mechanisms, governance structures, technical expertise, and strategies to prevent non-compliance (Wasil et al., 2024). For instance, AI in biorisk management and biosecurity can assess the safety and protective measures of research activities as well as evaluate the probability of accidental release of organisms (De Haro, 2024).

The adoption of AI technologies, particularly through simulations, enables the evaluation of the effectiveness of different response strategies. For example, AI could support the design of medical countermeasures to defend against bioterror attacks (Cohen & Tang, 2024).

Bioterrorism is considered a realistic risk scenario that can cause significant disruptions in the supply chain. AI serves as a tool to predict potential disruptions and enhance the resilience of supply chains against crises such as pandemics or bioterrorism (Abbas & Badi, 2024).

For instance, when a small U.S. drug company employed a machine learning model to identify molecules that could potentially be suitable for treating rare diseases, it trained the program to filter out toxic molecules. As part of an experiment for an international security conference, the company changed the rules with appropriate safety measures. The computer was tasked with identifying harmful molecules instead of filtering them out. The result was astonishing: within six hours, the computer generated 40,000 candidates. While some of these were already known chemical warfare agents, others appeared to be even more dangerous. For policymakers, AI may serve both as an opportunity and as a potential disaster maker (Irving, 2024).

The benefits of using AI in supply chains are frequently highlighted (e.g., optimized inventory management and prevention of stockouts, or increased productivity through automation of repetitive tasks and real-time analysis of large datasets) as it is revolutionizing supply chain management (Edwards, 2025).

Research on the potential of AI for preventing sabotage in biotechnology supply chains is relatively limited. The available literature predominantly frames AI as a potential threat to the security and integrity of these supply chains rather than as a protective tool.

It turns out that the use of AI in biotechnology supply chains is a double-edged sword. Ultimately, the question remains how to manage the inherent dual-use nature of AI in order to prevent security risks within biotechnology supply chains. While AI currently has only a minimal impact on biological threats, the regulatory gaps regarding its adoption are concerning. Legally mandated monitoring, red-teaming, and stricter oversight of production and supply chains could help reduce risks and hinder the development of bioweapons (Morgan, 2024).

Methodology

The research methodology comprised two core components. First, data were collected through a questionnaire consisting of nine Likert-scale questions, designed to measure participants' attitudes, concerns, and perceptions regarding biotechnology and its potential risks. A total of 103 individuals participated in this survey.

Second, experts in the fields of biotechnology, artificial intelligence, biosecurity, epidemiology, and supply chain management were identified and contacted via LinkedIn. Keywords such as "Biosecurity Expert," "Dual-Use Research," and "Biotech Supply Chain" were used to locate relevant professionals for inclusion in the study.

The two questions posed to the experts were:

In your view, what are the most critical dual-use risks currently present in global biotechnological supply chains, especially in light of emerging pathogen threats?

How do you see the role of empathic or ethically-informed AI in detecting or mitigating these risks, particularly in early-warning or decision-support systems?

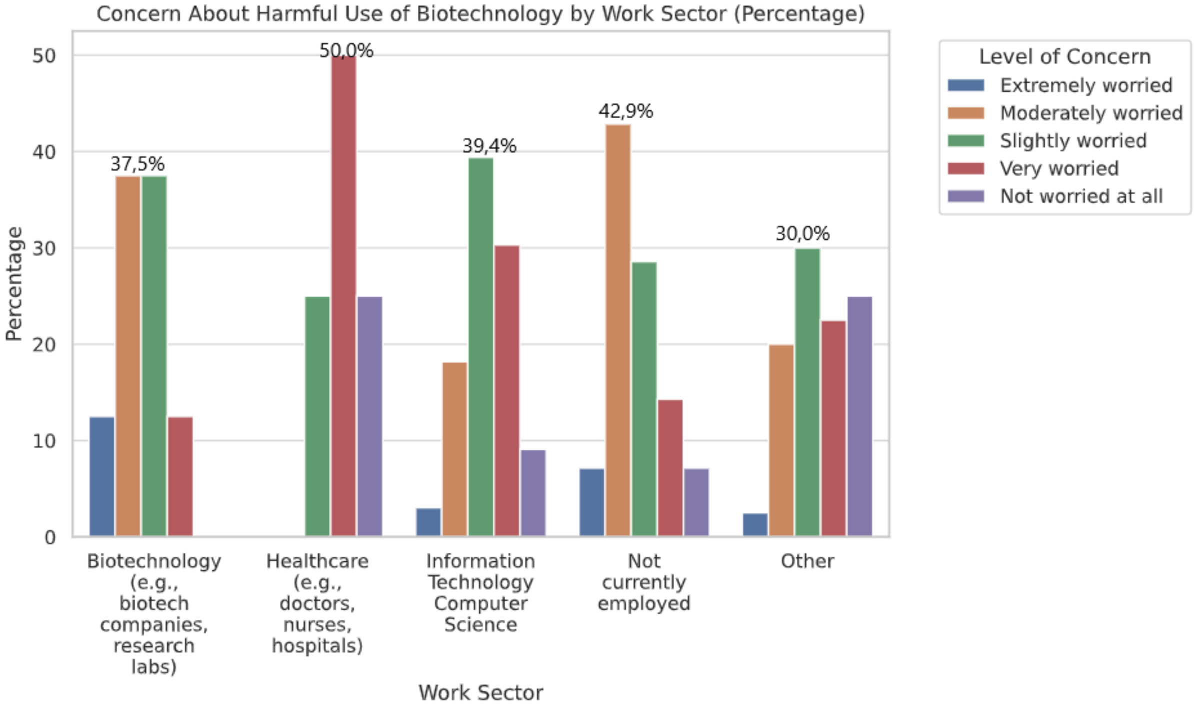
The data collection activity combined an initial survey of the general public with qualitative interviews of experts, capturing both broad perceptions and in-depth insights into dual-use risks in biotechnological supply chains. Using LinkedIn for expert recruitment allowed access to a diverse, interdisciplinary pool, while the focused, open-ended questions provided nuanced perspectives on the role of AI in mitigating these risks.

Results and Discussion

The survey of 103 individuals regarding their attitudes, concerns, and perceptions of biotechnology and its potential risks yielded the following notable insights.

Figure 1 shows the sector-specific concerns over the misuse of biotechnology. Biotechnology professionals demonstrated high levels of concern, indicating that they are strongly aware of potential risks within the field. Academics also expressed a significant degree of concern, likely due to their deeper understanding of the dual-use nature of biotechnology. Individuals from non-technical sectors, such as media, business, and the public sector, showed more varied responses, suggesting differing levels of awareness or perceptions of risk. The response "not at all worried" was rarely selected. Overall, concerns about the misuse of biotechnology were widespread across all sectors (see figure 1).

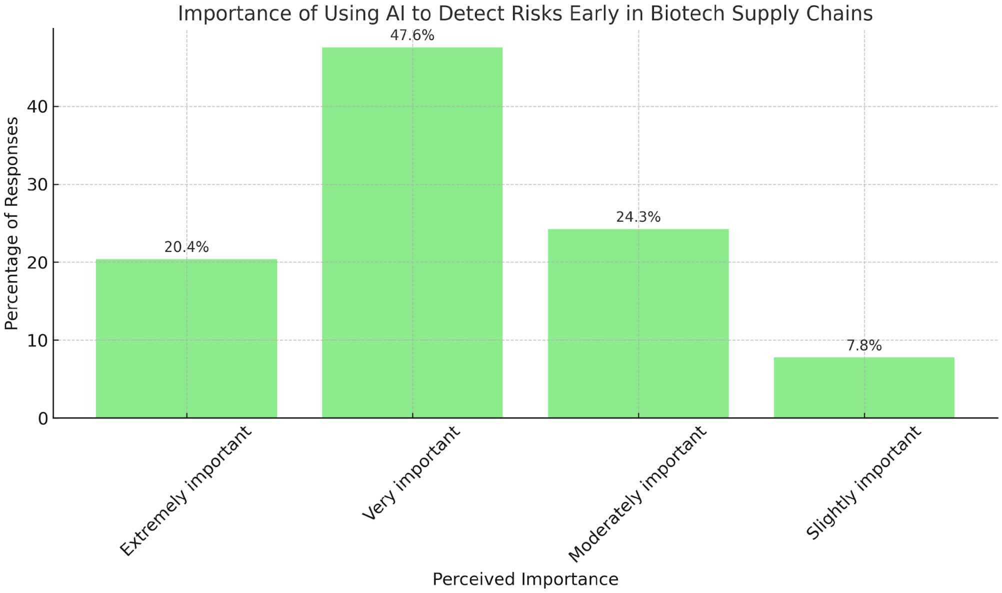
Figure 1. Sector-Specific Concerns Over the Misuse of Biotechnology



Source: own figure

The majority of respondents considered the use of AI in biotech supply chains to be either "extremely important" or "moderately important." Overall, there is strong support, with over 90% of participants believing that AI plays a meaningful role in early risk detection (see figure 2). Only a small fraction of respondents viewed AI as "slightly important" or "not at all important," indicating very few are indifferent or opposed. These results reflect a strong public awareness of AI's value in ensuring safety within the biotech sector.

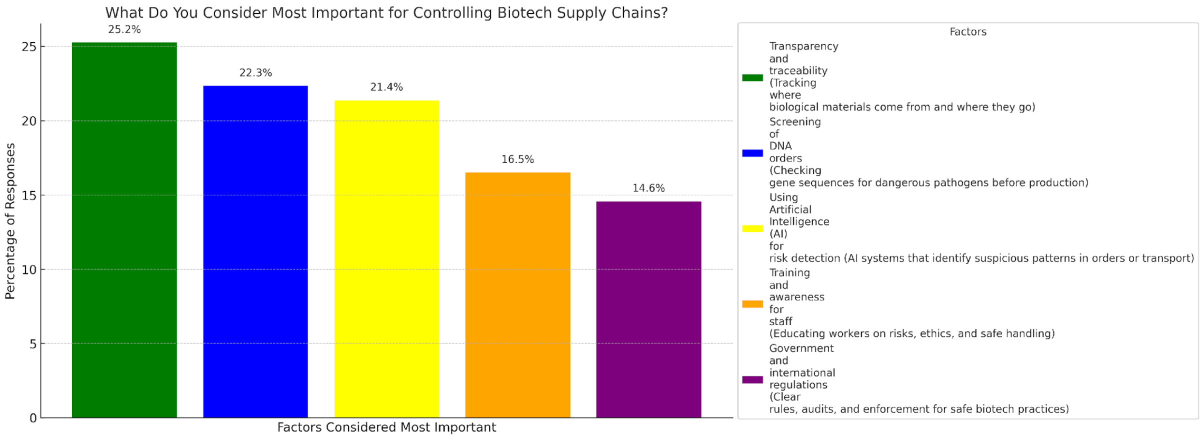
Figure 2. Importance of AI in Ensuring Biotech Supply Chain Safety



Source: own figure

Most respondents believed traceability of biotechnology adoption is essential to track biotech materials clearly and reliably (see Figure 3). Cybersecurity and transparency were also considered very important for maintaining safe supply chains. While monitoring and inspections remain significant, they were ranked slightly lower than digital tools and traceability measures. Overall, trust in data and systems significantly shaped people's perceptions on the risks of biotechnology.

Figure 3. What's Most Important for Biotech Supply Chain Safety



Source: own figure

The key insights derived from the expert questions and their responses are summarized in a table 1:

Table 1. Summary of Expert Perspectives

Expert	Insights
1	- One of the most pressing dual-use dilemma of biotechnological supply chains is their potential negative impacts on human health - The ethical commitment of biotechnological researchers is essential to ensure ethical research and use of biotechnologies - Empathic AI may help relevant stakeholders evaluate the ethical use of biotechnologies by providing actionable insights into their safe use
2	- The proliferation of digitization is the most critical dual-use risk - He perceives misuse of biotechnological research findings as another critical risk - Empathic AI may serve as a reliable reference for predicting and communicating disease outbreaks caused by biotechnologies
3	- Findings of research on biotechnologies can be misused as researchers may use them to create and modify pathogens - Ethical concerns surrounding biotechnologies may lead to societal backlash - Empathic AI may provide data-based analysis and insights into ethical practices surrounding biotechnologies
4	- The potential misuse of biotechnologies in creating new pathogens is a serious risk of biotechnology dual-use - AI can help detect the potential issue inflicted by biotechnology misuse early
5	- The democratization of advanced bioengineering tools may lead to uncontrolled unethical pathogen modification and other unethical practices - Empathic AI can serve as an intelligent safeguard that monitor suspicious use of biotechnologies
6	- Data resulting from biotechnology research can be misused by irresponsible actors - AI can detect unusual patterns in biotech systems - AI can provide insights and recommendations to policymakers
7	- The synthesis of gene and secret development of pathogens may lead to virus bioengineering, which can be misused - AI may enable early detection system which may quickly identify unusual patterns in bioengineering

Source: own table

Conclusion

The results of this research highlight the dual-use dilemma of biotechnology supply chains, especially how they are prone to pathogen misuse and illegal distribution, as well as how AI can help address such a risk. The literature review showcases AI's capability in complementing supply chains. However, it should be noted that these findings did not cover how AI may help prevent the potential misuse of biotechnology, most likely due to the limitation in the number of available references.

The survey conducted in this research indicated a strong public awareness of AI's potential in addressing the dual-use dilemma of biotechnology. The majority of respondents considered traceability as the key to biotechnology development and adoption, as it enables users to track biotech materials properly. Intriguingly, over 90 percent of participants believed AI can play a meaningful role in providing early risk detection of anomalies in biotechnology adoption. Experts highlighted that the biotechnological supply chains are prone to the misuse of research findings, uncontrolled pathogen modifications, and other ethical concerns that may lead to societal backlash. In this context, they proposed that empathic AI can serve as a valuable asset for early detection, monitoring, and ethical guidance of biotechnology development, thus providing actionable insights and recommendations to policymakers and stakeholders to properly mitigate such risks.

The author wishes to express her gratitude to the experts who generously shared their knowledge and perspectives for this study:

- Olal Amos Jerome – Biomedical Engineer, Data Scientist, CEO of SafeMed Technologies, Cofounder of Agrovision Uganda
- Nyeke James Tony – Medical Research Council Unit The Gambia; Social Epidemiology Lab, Germany
- Gilbert Narh Nyavor – KNUST, Ghana; Genetic Engineering enthusiast
- Nana Yaa Adomaa Doku-Amponsah – University of Ghana, BSc Biomedical Engineering, 2025
- Al-Imran – BSc Computer Science & Engineering (Data Science), United International University, Bangladesh
- Daniel Yarboi – Computer Engineering graduate; AI researcher in Cybersecurity & Healthcare
- Simon Anguzu – MSc Molecular Biology student, Makerere University

References

Abbas, N., & Badi, S. (2024). *Enhancing healthcare supply chain security: Strategies for resilience against pandemics and bioterrorism.* https://doi.org/10.13140/RG.2.2.15417.58726

Adamson, G., & Allen, G. C. (2025, August 6). *Opportunities to strengthen U.S. biosecurity from AI-enabled bioterrorism: What policymakers should know.* Center for Strategic and International Studies. https://www.csis.org/analysis/opportunities-strengthen-us-biosecurity-ai-enabled-bioterrorism-what-policymakers-should

Baillie, L., Dyson, H., & Simpson, A. (2012). Dual use of biotechnology. In R. G. Frey & C. H. Wellman (Eds.), *Encyclopedia of applied ethics* (pp. 876–883). Elsevier. https://doi.org/10.1016/B978-0-12-373932-2.00430-0

Bam, L., Breugem, T., Joachim, M., Parsa, I., Van Wassenhove, L. N., & Yadav, P. (2023, December 5). Challenges in pathogen genomic sequencing supply chains in Sub-Saharan Africa: Exploring the role of communities of practice (INSEAD Working Paper No. 2024/02/TOM). INSEAD. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4654811

Center for Counterproliferation Research. (2002). *Anthrax in America: A chronology and analysis of the fall 2001 attacks* (Working Paper). National Defense University. https://wmdcenter.ndu.edu/Publications/Publication-View/Article/626576/anthrax-in-america-a-chronology-and-analysis-of-the-fall-2001-anthrax-attacks/

Cohen, M. C., & Tang, C. S. (2024, February 5). The role of AI in developing resilient supply chains. *Georgetown Journal of International Affairs.* https://gjia.georgetown.edu/2024/02/05/the-role-of-ai-in-developing-resilient-supply-chains/

De Haro, L. P. (2024). Biosecurity risk assessment for the use of artificial intelligence in synthetic biology. *Applied Biosafety, 29*(2). https://doi.org/10.1089/apb.2023.0031

Edwards, J. (2025, March 3). AI-driven productivity gains: Transforming pharma supply chain efficiency. *Pharma IQ.* https://www.pharma-iq.com/manufacturing/articles/ai-driven-productivity-gains-transforming-pharma-supply-chain-efficiency

Eyal, N., Leshabari, M., & Sarker, M. (2024). Dual-use research and research using enhanced pathogens in high-income countries: Whose business? *mSphere, 9*(7). https://doi.org/10.1128/msphere.00168-24

Frazar, S., Hund, G., Bonheyo, G., Diggans, J., Bartholomew, R., Gehrig, L., & Greaves, M. (2017). Defining the synthetic biology supply chain. *Health Security, 15*(4), 375–386. https://doi.org/10.1089/hs.2016.0083

Gillum, D. R. (2024). Balancing innovation and safety: Frameworks and considerations for the governance of dual-use research of concern and potential pandemic pathogens. *Applied Biosafety, 29*(2), 1–10. https://doi.org/10.1089/apb.2024.0033

Grand View Research. (2023, August). *Biotechnology market size and share | Industry report, 2030.* https://www.grandviewresearch.com/industry-analysis/biotechnology-market

Irving, D. (2024, March 21). Artificial intelligence and biotechnology: Risks and opportunities. *RAND Corporation.* https://www.rand.org/pubs/articles/2024/artificial-intelligence-and-biotechnology-risks-and.html

Karlsson, E. A., Blacksell, S. D., Carroll, D., Harper, D. R., Morzaria, S., & Claes, F. (2024). We need a global framework for promoting safe handling of high consequence pathogens. *BMJ, 386*, q1855. https://doi.org/10.1136/bmj.q1855

Morgan, S. (2024, November 15). The double-edged sword: Opportunities and risks of AI in biosecurity. *Georgetown Security Studies Review.* https://georgetownsecuritystudiesreview.org/2024/11/15/the-double-edged-sword-opportunities-and-risks-of-ai-in-biosecurity/

Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy. *Frontiers in Bioengineering and Biotechnology, 6*, 39. https://doi.org/10.3389/fbioe.2018.00039

Nature Biotechnology. (2021). The next 25 years. *Nature Biotechnology, 39*, 249. https://doi.org/10.1038/s41587-021-00849-7

Saad Al-Naimi, D. M. (2025). The impact of AI in supply chain resilience: A systematic mapping review. *Gateway Journal for Modern Studies and Research, 2*(1). https://doi.org/10.61856/nrcn3x58

Samundeswari, S., Lalitha, V., Kavitha, V., Harini, M., Dharshini, T., & Srinithi, S. (2023). Supply chain management of dual-use drugs using blockchain. *Procedia Computer Science, 230*, 388–397. https://doi.org/10.1016/j.procs.2023.12.094

Saunders-Hastings, P. (2020). Securitization theory and biological weapons: Assessing threats in global health security. *Journal of Security Studies, 15*(3), 210–230. https://doi.org/10.1234/jss.v15i3.5678

Schabacker, D. S., Levy, L.-A., Evans, N. J., Fowler, J. M., & Dickey, E. A. (2019). Assessing cyberbiosecurity vulnerabilities and infrastructure resilience. *Frontiers in Bioengineering and Biotechnology, 7*, Article 61. https://doi.org/10.3389/fbioe.2019.00061

Selgelid, M. J. (2009). Governance of dual-use research: An ethical dilemma. *Bulletin of the World Health Organization, 87*(9), 720–723. https://doi.org/10.2471/blt.08.051383

Shinomiya, N., & Tanaka, K. (n.d.). The security implications of developments in biotechnology. *National Institute of Infectious Diseases; Toyo Eiwa University; Temple University, Japan.*

Wasil, A., Barnett, P., Gerovitch, M., Hauksson, R., Reed, T., & Miller, J. (2024, September 4). Governing dual-use technologies: Case studies of international security agreements and lessons for AI governance. *SSRN.* https://doi.org/10.2139/ssrn.4946527

Youvan, D. C. (2024, September). The hidden risks in pharmaceuticals: Examining vulnerabilities in global supply chains and potential for sabotage. https://doi.org/10.13140/RG.2.2.19217.03689