POLICY REPORT

December 2025

Convergence of Biotechnologies and Artificial Intelligence

Implications on Biological Security

Julius Cesar Trajano, Jeselyn, and Mely Caballero-Anthony

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

Ponder the Improbable since 1996

Table of Contents

Executive Summary

The rapid convergence of artificial intelligence (AI) and biotechnology presents a profound dual-use challenge. While these advances offer transformative capabilities, they also expand the range and accessibility of tools that could be misused for hostile purposes, including the design of novel pathogens or the circumvention of existing detection systems.

Current governance frameworks for both life sciences and AI often operate in isolation, leaving critical blind spots in governance and accountability. Closing these gaps requires more coordinated action by and among stakeholders in biological sciences and AI to enhance transparency and safeguards in scientific research.

ASEAN can strengthen regional AI-biosecurity governance by leveraging existing institutional platforms, promoting self-regulation, standardising transparency principles, and building capacity across member states. A multi-stakeholder approach involving scientists, the business sector, ethicists, and civil society will be essential to building trust and mitigating AI-related biological risks.

Introduction

The 50th anniversary of the entry into force of the Biological Weapons Convention has renewed global attention on the rapidly changing landscape of biological security, with it being the only global treaty outlawing the development and use of biological weapons.[1] Organised by the United Nations, the commemorative conference in March 2025 highlighted how advances in biotechnology (e.g., synthetic biology, genetic engineering, DNA synthesis)—increasingly shaped by artificial intelligence (AI)—comes with greater security risks.[2]

This technological convergence offers major benefits, from accelerated vaccine development, improved diagnostics and public health responses, to the identification of emerging threats. However, the dual-use nature of AI-powered biotechnologies also heightens the risk of deliberate or accidental release of harmful biological agents. As biosecurity experts emphasise, vigilance is essential to ensure that scientific progress benefits society rather than threatens international peace and security.[3]

This risk is further underscored by warnings from the industry. OpenAI, the developer of Chat GPT, recently stated in its Preparedness Framework Statement that upcoming AI models are expected to attain "high" capability levels in biology.[4] This raises concerns that such technologies can be exploited to develop biological threats even by individuals with limited subject expertise. The statement highlights the core challenge: while AI and biotechnologies hold promise for accelerating scientific progress, they also present significant risks if safeguards against misuse are not adequately enforced.

Against this backdrop, this policy report examines the dual nature of AI in biotechnological applications and its implications for biosecurity. We contend that the integration of AI unlocks significant scientific opportunities while simultaneously heightening security risks and revealing major gaps in existing oversight. As a result, there is an urgent need for safeguards to manage these tools and to enhance ASEAN-led regional cooperation to future-proof biosecurity governance in Southeast Asia.

AI's Growing Role in the Life Sciences

In an era of unprecedented technological convergence, AI is accelerating breakthroughs in biological research, offering hope for curing diseases, optimising bio-manufacturing, and detecting pandemics early. This could transform the way the world respond to disease outbreaks. By analysing large datasets, AI can help identify

[1] United Nations, "50th Anniversary of the Biological Weapons Convention," last accessed 3 June 2025, https://disarmament.unoda.org/50th-anniversary-of-the-biological-weapons-convention/.
[2] Izumi Nakamitsu, Opening remarks at the commemorative event to mark the 50th anniversary of the Biological Weapons Convention, Geneva Switzerland, 26 March 2025
[3] https://www.nti.org/analysis/articles/statement-on-biosecurity-risks-at-the-convergence-of-ai-and-the-life-sciences/.
[4] Open AI, "Preparing for future AI capabilities in biology," 18 June 2025, https://openai.com/index/preparing-for-future-ai-capabilities-in-biology/.

promising vaccine targets, forecast vaccine efficacy, and detect potential outbreaks—strengthening disease surveillance and early warning systems.[5]

Southeast Asia stands to benefit considerably from these developments. The region's dense populations, expanding biotechnology sector, and recurrent disease outbreaks make timely detection and response particularly critical. For instance, Singapore's National Environment Agency employs AI-driven data analysis and predictive modelling to monitor and anticipate dengue fever outbreaks.[6] More broadly, AI is increasingly employed across three critical phases of pandemic management: prevention, detection, and response. In the prevention phase, AI systems analyse vast datasets to identify potential hotspots, predict outbreak patterns, and inform early interventions. During detection and response, it supports real-time diagnostics, accelerates contact tracing, and optimises resource allocation, thereby enhancing the speed and effectiveness of public health measures.[7]

Beyond public health surveillance, AI-powered biological design tools (BDTs) are reshaping the possibilities in biotechnology research. They are expanding the capabilities available to biologists, driving innovative applications across life sciences research and development, agriculture, sustainability, pollution control, energy security, public health, and national defence. Other than facilitating the engineering of biological systems (e.g. viruses and living organisms), BDTs can potentially advance the development of new medicines and vaccines to address emerging and re-emerging diseases.[8] Currently, one of the most widely developed types of BDTs are AI-powered protein design platforms.

Several research laboratories and institutes in Southeast Asia have also begun utilising AI tools to boost pandemic and epidemic preparedness, secure high-consequence pathogens, and fast-track healthcare and biotechnology innovation.[9] Furthermore, AI is increasingly integrated into laboratory biosecurity systems to prevent unauthorised access to sensitive materials or facilities.[10]

Additionally, AI can support safer management of Dual-Use Research of Concern (DURC) by helping researchers assess the risks and benefits of certain studies

---

[5] James Revill, Clarissa Rios, and Louison Mazeaud, "What will be the impact of AI on the bioweapons treaty?", *Bulletin of the Atomic Scientists*, 16 November 2024, https://thebulletin.org/2024/11/what-will-be-the-impact-of-ai-on-the-bioweapons-treaty/?utm_source=chatgpt.com.

[6] YCP, "Partner Expertise: How AI is Revolutionizing Early Detection of Diseases", 7 December 2023, https://ycp.com/insights/article/artifical-intelligence-healthcare-southeast-asia#:~:text=In%20another%20interesting%20example%20of,the%20outbreak%20of%20dengue%20fever.

[7] University of Oxford, "New study shows how AI can help prepare the world for the next pandemic", 20 February 2025, https://www.ox.ac.uk/news/2025-02-20-new-study-shows-how-ai-can-help-prepare-world-next-pandemic.

[8] Sarah R. Carter, Nicole E. Wheeler, Christopher R. Isaac, and Jaime Yassif, "Developing Guardrails for AI Biodesign Tools", *NTI Paper*, November 2024, https://www.nti.org/wp-content/uploads/2024/11/NTIBio_Paper_Developing-Guardrails-for-AI-Biodesign-Tools_FINAL.pdf.

[9] Universitas Gadjah Mada, "Artificial Intelligence for Pandemic and Epidemic Preparedness (AI4PEP)" ,last accessed 3 June 2025, https://centertropmed-ugm.org/project/ai4pep/.

[10] Anel Azel Dimaano, "RITM, Germany strengthen health research efforts; launches Project BUKLOD", Research Institute for Tropical Medicine (Department of Health of the Philippines), 3 March 2023, https://ritm.gov.ph/projectbuklodaiml/; Jones Lang LaSalle (JLL) , "From wet to dry: How AI is shaking up laboratory design", 11 December 2024, https://www.jll.co.th/en/trends-and-insights/investor/from-wet-to-dry-how-ai-is-shaking-up-laboratory-design.

before they proceed. This is particularly important for Southeast Asia, where biosafety and biosecurity standards for DURC are still nascent and vary widely across countries.[11]

The Dual-Use Dilemma: Biosecurity Risks in AI-Biotech

The potential of AI in biotechonoloy presents a profound dual-use dilemma: the same tools that can generate life-saving innovations can also be misused to develop biological weapons (see Table 1). The rapid advances have significantly transformed the global biosecurity landscape, presenting new types of threats and capabilities.

Table 1: Examples of AI Bio Tools/Models with Dual-Use Implications[12]

Tool/Model	Main Beneficial Use	Dual-Use Concerns
AlphaFold (DeepMind)	Rapidly and affordably predicts protein structures which hold transformative potential for vaccine development, drug design, and other public health applications	Could enable weaponising of genetic insights, allowing bad actors to design new bioweapons that can target individuals with specific genetic traits
CRISPR AI Design Tools (e.g., Benchling, CRISPR RGEN Tools)	Redefines biotechnology, significantly amplifying the impact of CRISPR genome editing in medicine, agriculture, and climate actions	Could be misused to develop harmful pathogens and edit dangerous organisms for nefarious purposes
Moremi Bioagent	Positioned as a transformative tool for drug discovery and vaccine design	Could be used to design a novel protein as bioweapon, with higher toxicity than Sarin, one of them most volatile nerve agents
Text-to-Biology Models (e.g., GPT-like models	Could become very effective laboratory assistants which might be able to provide step-by-step instructions for experiments and guidance for	Provide knowledge with dual-use potential and security sensitive information and thus remove some barriers

[11] World Health Organization, "What is dual-use research of concern?", 13 December 2020, https://www.who.int/news-room/questions-and-answers/item/what-is-dual-use-research-of-concern.
[12] Sterling Sawaya, Taner Kuru and Thomas Campbell, "The Potential for Dual-Use of Protein-Folding Prediction", UNICRI, 2021, https://unicri.org/sites/default/files/2021-12/21_dual_use.pdf; Google DeepMind, "AlphaFold", last accessed 18 August 2025, https://deepmind.google/science/alphafold/;Jennifer Doudna, "Combining AI and Crispr Will Be Transformational", *Wired*, 26 November 2024, https://www.wired.com/story/combining-ai-and-crispr-will-be-transformational/?utm_source=chatgpt.com; Gertrude Hattoh, et al., "Can Large Language Models Design Biological Weapons? Evaluating Moremi Bio", ArXiv, May 2025, DOI:10.48550/arXiv.2505.17154; Jonas Sandbrink, "Artificial intelligence and biological misuse: Differentiating risks of language models and biological design tools", arXiv; 2023. doi:10.48550/arXiv.2306.13952; Nicole Wheeler, "Responsible AI in biotechnology: balancing discovery, innovation and biosecurity risks", *Frontier in Bioengineering and Biotechnology* Vol 13, 2025, https://doi.org/10.3389/fbioe.2025.1537471; Institute for Protein Design, "RoseTTAFold: Accurate proteinstructure prediction accessible to all", University of Washington, 15 July 2021, https://www.ipd.uw.edu/2021/07/rosettafold-accurate-protein-structure-prediction-accessible-to-all/.

trained on bio literature)	troubleshooting pathogen and biotech experiments	encountered by historical biological weapons efforts, in particular lowering barriers to biological misuse
AI Protein Design Platforms (e.g., RosettaFold, ProGen)	Build models of complex biological assemblies in a fraction of the time previously required, generate structures directly relevant to human health, industrial applications, and combating antimicrobial resistance	Could streamline the development of effective bioweapons by enabling the design of proteins with tailored properties

The Problem of Novice Uplift

Growing concerns about biosecurity risks are being intensified by recent trends in AI development. One major issue is "novice uplift," where AI systems could enable people with only basic knowledge in life sciences to design, manipulate, or engineer hazardous biological materials.

The Global Risks Report 2025 by the World Economic Forum warns that advances in AI-driven biotech will make biological weapons easier and cheaper to develop over the next decade. This also raises the risk that non-state actors could develop such weapons, increasing the severity of future terrorist attacks. While the misuse of AI by novice cybercriminals is already a growing concern, an even more alarming threat is the potential for nefarious non-state actors to exploit biotechnologies for the development of biological weapons.

A key enabler of this heightened risk is the transformational growth in dual-use capabilities demonstrated by existing Large-language models (LLMs) such as GPT-4 and 4o, which are increasingly proficient in supporting the design and implementation of biological and chemical research and testing protocols.[13] LLMs have the potential to be utilised in accessing biological AI models to perform complex scientific tasks. Crucially, the very same underlying capabilities driving this scientific progress, such as reasoning over biological data, predicting chemical reactions, or guiding lab experiments, could be misused to assist highly skilled actors in creating bioweapons.

Recent evaluations show that frontier AI systems may soon meaningfully assist even novice actors in replicating known biothreats. The growing “novice uplift” effect highlights a critical gap in current biosecurity governance: a lack of transparency in how AI tools intersect with sensitive biological knowledge and capabilities.[14]

[13] Jaspreet Pannu, et. al., “Dual-use capabilities of concern of biological AI models”, *PLoS Computational Biology* 21, no. 5, May 2025, https://journals.plos.org/ploscompbiol/article?id=10.1371/journal.pcbi.1012975.
[14] Nikki Teran, “ChatGPT Agent Setting Industry Leading Example for Biosecurity Safeguards”, NTI bio, last accessed 13 August 2025, https://www.nti.org/risky-business/chatgpt-agent-setting-industry-leading-example-for-biosecurity-safeguards/.

The Governance Blind Spot

This governance gap is exacerbated by the current lack of national regulatory oversight on emerging technologies and life sciences, a situation that undermines trust and transparency, particularly as private AI labs, startups, or universities conduct powerful research outside government control.

Mitigating these risks requires action across three key domains: (i) transparency, (ii) responsibility and accountability, and (iii) security culture.

> **(i) Transparency**: Transparency is the cornerstone of responsible innovation in both AI and life sciences. Without it, the bio-AI space becomes opaque, eroding public trust and widening regulatory blind spots.
>
> **(ii) Responsibility and Accountability**: A key concern is the lack of clear responsibility/accountability for AI companies regarding the dual-use potential of their technologies, especially in advancing biological research. This raises a critical question: how much responsibility should be borne by AI developers relative to the scientists or end-users employing AI models in their research?
>
> **(iii) Security Culture**: AI-driven lab operations can increase the risk of biosecurity breaches, either through cyber vulnerabilities or insider threats. As research labs and high-containment laboratories in Southeast Asia increasingly rely on AI-enabled cybersecurity systems, it is imperative to develop a strong cyberbiosecurity culture among laboratory staff and researchers.

A robust cyberbiosecurity culture should, ideally, encompass a set of values, practices, and behaviours aimed at preventing: (i) unauthorised access to or loss of bioinformation; (ii) the discontinuation of operations due to cyberattacks; (iii) insider threats and unauthorised digital access to networked laboratory equipment; (iv) the sabotage of laboratory security system; (v) theft, misuse or sabotage of information on sensitive biological agents; and (vi) espionage pertaining to biosecurity-relevant information.

Leveraging AI to Strengthen Biological Security

While the "novice uplift" and governance challenges outlined above highlight the potential dangers of dual-use AI, it is crucial to recognise that the technology also offers considerable opportunities to strengthen biological arms control and counter biological threats.

Given that the Biological Weapons Convention (BWC) lacks a formal verification mechanism, AI and other emerging technologies could support the development of innovative measures to strengthen compliance of state and non-state actors. AI's ability to analyse large volumes of data to identify trends could significantly enhance disease surveillance, enable early warning systems, and accelerate response efforts. When harnessed effectively, these capabilities could improve cross-border assistance in response to a BWC violation and help mitigate the impact of any use of biological weapons.

Building on this potential, countries could further operationalise AI tools in several concrete ways to actively detect and respond to biological threats from both state and non-state actors. Possible AI applications in this area include mapping and analysing terrorist networks, behavioural patterns, social media activity, and travel routes to anticipate and disrupt potential plans or attacks.[15] AI-enabled systems can also analyse data, images, and overhead satellite imagery to help distinguish between legitimate biological research and suspicious, weapons-related activities. Furthermore, AI can be leveraged to identify and disrupt illicit procurement networks seeking to bypass export control measures and acquire dual-use biological materials.

AI applications can also support attribution efforts by identifying unique signatures of biological samples or incidents, helping to trace their origins and the actors involved. This would enable more targeted policy responses and may deter further development or use of biological weapons.

Safeguards for Reducing Risks: Policy Considerations for Southeast Asia

The realisation of these defensive benefits, however, is contingent upon effective governance; therefore, the capabilities discussed above must be paired with clear policy action to mitigate risk. Establishing guardrails containing safeguards and transparency measures for dual-use AI-powered biotechnologies is essential to promoting responsible innovation.

As the international community has yet to develop such measures, strengthening collaboration between governments, AI-biotech developers and users, and biosafety and biosecurity experts is critical for anticipating emerging challenges and identifying appropriate safeguards. Relevant stakeholders in Southeast Asian countries and ASEAN can enhance biological security through several modalities:

(i) Leveraging ASEAN Institutional Platforms: Platforms such as the soon-to-be established ASEAN Biosafety and Biosecurity Network (ABBN)[16] and the ASEAN Health Cluster 2 on Responding to All Hazards and Emerging Threats[17] can play a vital role in fostering dialogue on responsible AI development and application in biotechnology. Having begun discussions on emerging technologies and regional security concerns, these platforms can be expanded to include structured dialogues on AI-related risks, norms, and transparency practices, particularly in relation to biological threat mitigation.

[15] David Luckey, et. al., "Mitigating Risks at the Intersection of Artificial Intelligence and Chemical and Biological Weapons", RAND, 28 January 2025, https://www.rand.org/pubs/research_reports/RRA2990-1.html.
[16] ASEAN, "ASEAN Leaders' Declaration on Strengthening Regional Biosafety and Biosecurity", 9 October 2024, https://asean.org/asean-leaders-declaration-on-strengthening-regional-biosafety-and-biosecurity/.
[17] ASEAN, "Health: Overview", last accessed 13 August 2025, https://asean.org/our-communities/asean-socio-cultural-community/health/.

(ii) Promoting Industry Self-Regulation: In the absence of tight government oversight frameworks, self-regulation, which entails the voluntary adoption of guidelines and principles by scientists and industry players, has been the default approach. The scientific community plays a central role in this effort. In Southeast Asia, national biorisk and life science associations have developed guidelines governing the use of emerging technologies. For instance, the Biorisk Association of Singapore's Biorisk Code of Conduct for Life Sciences Industry and Professionals is designed to prevent the misuse of life sciences by promoting a culture of responsibility.[18]

(iii) Standardising Governance Principles: ASEAN can promote the standardisation of AI governance principles related to biological security, such as accountability, auditability, and traceability. Given that AI systems used in biosurveillance and data analysis may involve opaque or proprietary algorithms, a regional framework that encourages transparency about the sources, methods, and limitations of AI tools can help reduce misperceptions and build mutual trust, especially in sensitive areas such as attribution or threat detection.

(iv) Enhancing Regional Capacity: ASEAN's emphasis on capacity-building and reducing development gaps among member states can be directed toward enhancing AI literacy, technical skills, and regulatory coherence. This includes supporting national governments in establishing safeguards against AI misuse in biological research and enabling meaningful participation in regional transparency initiatives. Tailored technical assistance, knowledge-sharing platforms, and public-private dialogues could foster a more balanced and inclusive approach to regional transparency.

(v) Fostering Multi-Stakeholder Involvement: ASEAN can advocate for greater involvement of scientists, ethicists, the business sector, and civil society in regional AI-biosecurity governance, fostering a multi-stakeholder model that enhances transparency and legitimacy. Science diplomacy, long promoted within ASEAN, can be expanded to encompass the AI-biotech frontier, encouraging cooperative research and peer exchanges that promote openness and collaboration in the biological sciences.

[18] Biorisk Association of Singapore, "Singapore Biorisk Code of Conduct for Life Sciences Industry and Professionals", last modified 2022, Singapore BRAS.

Conclusion

The convergence of AI and biotechnology poses a profound dual-use challenge, amplifying biological security risks, notably the threat of 'novice uplift', and highlighting governance gaps in transparency and accountability. To effectively manage these risks, ASEAN must move toward substantive safeguards by strengthening institutional dialogue, standardising principles like accountability and traceability, and promoting self-regulation across the scientific and industrial sectors. Finally, by emphasising transparency over verification, ASEAN can forge a pragmatic, constructive role in supporting the BWC's objectives. This proactive stance ensures AI is not merely protected against misuse but is actively harnessed to strengthen global biological security and bridge divides between innovation and regulation.

About the Authors

Mr Julius Cesar Trajano is Research Fellow at the Centre for Non-Traditional Security Studies (NTS Centre), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU) Singapore. He is part of the NTS Centre's Biosecurity and International Security programme and coordinates the Centre's nuclear security research programme. He has co-authored policy reports, commentaries and articles on biosecurity and biotechnology governance, nuclear security and climate security in Southeast Asia. He is among the co-organisers of the recently convened Study Group on Biosecurity and Health Security in the Asia-Pacific under the Council for Security Cooperation in the Asia Pacific (CSCAP). His latest publications include Emerging Biosecurity Landscape in Southeast Asia (RSIS, 2025) and "Biosecurity in the Changing Global Order: The Case of Southeast Asia" (Asia Policy, 2025). He is currently the Chair of the Asia-Pacific Regional Group of the International Nuclear Security Education Network.

Ms Jeselyn is a Research Analyst at the Centre for Non-Traditional Security Studies (NTS Centre), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU) Singapore. She is involved in the NTS Centre's Biosecurity and International Security programme. She conducts policy analysis on the emerging biosecurity landscape in the Asia-Pacific, the impact of emerging technologies such as artificial intelligence (AI) on biosecurity, and the nexus of climate, peace and security. She holds a Master of Science (MSc) in Asian Studies from RSIS, and a Bachelor of Arts in International Relations from Tokyo International University.

Professor Mely Caballero-Anthony holds the President's Chair for International Relations and Security Studies at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU) Singapore, where she also serves as the Head of the RSIS Centre for Non-Traditional Security Studies (NTS Centre) and Associate Dean (International Engagement). She leads the Biosecurity and International Security focus area at the Asia Centre for Health Security (ACHS). Her research focuses on regionalism and multilateralism in the Asia-Pacific, non-traditional security, human security, nuclear security, peacebuilding, and global governance. She has led several global and regional research projects on international security and global governance, and has held key leadership roles in major international networks and institutions, including as Secretary-General of the Consortium on Non-Traditional Security Studies in Asia since 2008 and a member of the World Economic Forum's Global Council on Nature and Security and the International Climate Security Expert Network.

About the Centre for Non-Traditional Security (NTS) Studies

Mission: To conduct rigorous research aimed at advancing the study of Non-Traditional Security, strengthening regional capacity to address current and emerging NTS risks and challenges, and providing a platform to engage scholars and policymakers in Asia and beyond.

Vision: To be a leading, global-oriented centre for NTS studies and an authoritative source of academic and policy analysis, contributing sustainable and inclusive solution to NTS risks and challenges.

About the S. Rajaratnam School of International Studies

The S. Rajaratnam School of International Studies (RSIS) is a global graduate school and think tank focusing on strategic studies and security affairs. Its five Research Centres and three Research Programmes, led by the Office of the Executive Deputy Chairman, and assisted by the Dean on the academic side, drive the School's research, education and networking activities.

The graduate school offers Master of Science Programmes in Strategic Studies, International Relations, International Political Economy and Asian Studies. As a school, RSIS fosters a nurturing environment to develop students into first-class scholars and practitioners.

As a think tank, RSIS conducts policy-relevant and forward-looking research in both national and international security, science and technology, society and economic and environmental sustainability. RSIS also produces academic research on security and international affairs. It publishes scholarly research in top-tier academic journals and leading university presses, and distributes policy research in a timely manner to a wide range of readers.

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.