RSIS COMMENTARY

12 August 2025

Strengthening Transparency at the AI-Biotech Nexus

Julius Cesar Trajano, Jeselyn, and Mely Caballero-Anthony

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

Ponder the Improbable since 1996

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

RSIS COMMENTARY

www.rsis.edu.sg No. 173 – 12 August 2025

Strengthening Transparency at the AI-Biotech Nexus

By Julius Cesar Trajano, Jeselyn, and Mely Caballero-Anthony

SYNOPSIS

Rapid advancements in artificial intelligence increasingly shape rising biosecurity concerns. To prevent the misuse of emerging biotechnologies and AI for hostile purposes, greater transparency in both life sciences and AI development is essential. At the same time, when applied responsibly, AI-driven tools and biotechnologies have significant potential for detecting and responding to emerging biological threats, thereby reinforcing international peace and security.

COMMENTARY

In June 2025, OpenAI, the developer of Chat GPT, warned that future AI models are likely to reach "High" capability levels in biology under its "Preparedness Framework". This means that individuals with basic training might obtain AI tools capable of creating biological or chemical threats. It also warned that these AI models raise an important dual-use consideration: enabling scientific advancement while safeguarding against harmful misuse.

In an era of unprecedented technological convergence, AI is accelerating breakthroughs in biological research, offering hope against diseases, optimising bio-manufacturing, and enabling early detection of pandemics. However, with this potential comes a serious dual-use dilemma: the same research outputs that generate lifesaving innovations can also be misused to develop biological weapons.

Against rapid advances in biological and AI research, the landscape of global security has been transformed significantly, presenting new types of threats and capabilities. Enhancing transparency in the life sciences and AI development is therefore crucial to mitigate the threat of frontier technologies being weaponised, which could threaten

peace and security. However, when used responsibly, AI-enabled biotechnologies and AI models can also be employed to detect and counter emerging biosecurity threats.

Transparency Under Threat

Large-language models (LLMs) such as GPT-4 and 4o have achieved transformational growth in dual-use capabilities, including supporting the design and implementation of biological and chemical research and testing protocols. LLMs have the potential to be utilised in accessing biological AI models to perform complex scientific tasks. This means that in the near future, AI will likely reduce the cost of biological innovations and help less experienced researchers utilise increasingly complex and powerful biological tools.

The same underlying capabilities that drive progress, such as analysing biological data, predicting chemical reactions, or guiding laboratory experiments, could also be misused to enable people with minimal expertise to recreate biological threats or assist highly skilled actors in developing bioweapons.

Recent evaluations by OpenAI and others indicate that frontier AI systems may soon enable novice actors to replicate known biothreats. The growing "novice uplift" risk highlights a critical gap in current biosecurity governance – a lack of transparency in how AI tools intersect with sensitive biological knowledge and capabilities. This lack of national regulatory oversight undermines trust and transparency, particularly as private AI labs, startups, or universities conduct powerful research outside government oversight.

Without transparency, the bio-AI field becomes opaque, trust declines, and regulatory blind spots expand. A key concern is the lack of clear responsibility and accountability for AI companies regarding the dual-use potential of their technologies, especially in the context of biological research. The question arises: What share of responsibility should AI developers bear relative to the scientists using AI models in their research?

An indication of this growing concern is the proliferation of cloud labs. These are automated laboratories operated remotely through cloud-based platforms, enabling researchers to conduct and oversee experiments using robots without being physically present. They offer benefits such as increased flexibility, lower costs, and scalable operations. However, these facilities also carry potential risks, including the capacity to produce harmful pathogens.

How AI Can Help Boost Transparency in Biological Research

Although AI presents certain risks, it also offers significant opportunities to strengthen biological arms control and reduce biological threats. Since the Biological Weapons Convention (BWC) lacks a formal verification mechanism, AI and other emerging capabilities could help develop innovative measures to ensure compliance by 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 cases of BWC violations and help to reduce the impact of any use of biological weapons.

AI tools can be utilised in several ways to identify and react to biological threats:

• AI applications could include the mapping and analysing of terrorist networks, patterns, social media, and travel to predict and disrupt biologically related activities and attacks.

• AI-enabled capabilities could be utilised to analyse data, images, and overhead satellite imagery to help differentiate between legitimate biological research and suspicious, weapons-related activities.

• AI can be used to identify and disrupt illicit procurement networks that attempt to bypass export control measures and acquire dual-use biological materials.

• AI applications can support attribution efforts by identifying unique signatures of biological samples or incidents, helping to trace their origins or the responsible parties.

AI could, therefore, enable more effective and targeted policy responses and could deter the development or usage of biological weapons.

ASEAN's Role in Enhancing AI Transparency for Biological Arms Control

Without a verification mechanism under the BWC, regional transparency measures are vital for building trust and ensuring compliance. As AI becomes more integrated into biotechnology and disease surveillance, there is a growing need for mechanisms that ensure the transparent and responsible use of AI, especially in its dual-use applications. There are cogent reasons why ASEAN, as a regional organisation with a long-standing focus on confidence-building, dialogue, and non-traditional security cooperation, is well-positioned to support efforts that promote AI transparency in the biological domain.

Firstly, ASEAN's institutional platforms, such as the soon-to-be-established ASEAN Biosafety and Biosecurity Network (ABBN) and the ASEAN Health Cluster 2 on "Responding to All Hazards and Emerging Threats", can serve as platforms for dialogue on responsible AI development and application in biotechnology. These platforms have already facilitated discussions on other emerging technologies and regional security concerns. They can be expanded to include structured dialogues on AI-related risks, norms, and transparency practices, particularly in relation to biological threat mitigation.

Secondly, ASEAN member states could consider establishing a regional voluntary reporting mechanism or transparency initiative focused on the AI-biotech nexus. While formal verification under the BWC remains out of reach, such voluntary measures, including the sharing of national AI-biosecurity policies, oversight frameworks, and ethical guidelines, can foster regional confidence and demonstrate collective commitment to non-proliferation and responsible innovation. These transparency efforts could be integrated into the future ABBN, which is currently under development.

Thirdly, 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.

Fourthly, ASEAN's emphasis on capacity-building and narrowing of development gaps across 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 them to participate meaningfully in regional transparency initiatives. Tailored technical assistance, knowledge-sharing platforms, and public-private dialogues on AI in biosciences could contribute to a more balanced and inclusive regional approach to transparency.

Fifthly, ASEAN can advocate for greater involvement of scientists, ethicists, 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.

Conclusion

By emphasising transparency over verification, ASEAN can carve out a pragmatic and constructive role in supporting the BWC's objectives in the age of AI. In doing so, ASEAN helps to bridge the gap between developed and developing countries, between innovation and regulation, and between security and scientific openness – ensuring that AI is not only protected against misuse but actively harnessed to strengthen the global biological security regime.

Julius Cesar Trajano and Jeselyn are respectively Research Fellow and Research Analyst at the Centre for Non-Traditional Security Studies (NTS Centre) at the S. Rajaratnam School of International Studies (RSIS). Mely Caballero-Anthony is Professor and Head of the NTS Centre, as well as the Biosecurity and International Security Lead of the Asia Centre for Health Security.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798

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