

RSIS Commentary is a platform to provide timely and, where appropriate, policy-relevant commentary and analysis of topical and contemporary issues. The authors' views are their own and do not represent the official position of the S. Rajaratnam School of International Studies (RSIS), NTU. These commentaries may be reproduced with prior permission from RSIS and due credit to the author(s) and RSIS. Please email to Editor RSIS Commentary at RSISPublications@ntu.edu.sg.

Biosecurity in the Age of AI: Risks and Opportunities

By Julius Cesar Trajano and Jeselyn

SYNOPSIS

Biosecurity has become more complex with the emergence of artificial intelligence-powered biotechnologies. The biotechnology-AI nexus can potentially strengthen biosecurity but amplify biological risks if misused. There is an urgent need for integrated governance frameworks to manage the dual-use nature of AI-powered biotechnology tools and regional cooperation through ASEAN to future-proof biosecurity governance in Southeast Asia.

COMMENTARY

The United Nations recently organised a [commemorative conference](#) to celebrate the 50th anniversary of the entry into force of the Biological Weapons Convention (BWC), a key global treaty outlawing the development and use of biological weapons. The commemorative conference highlights the rising security risk of the intersection between advances in biotechnology (e.g., synthetic biology, genetic engineering, DNA synthesis) and emerging technologies, particularly artificial intelligence (AI). This notwithstanding, biosecurity experts have repeatedly emphasised that we should be vigilant and ensure that the rapid advances in science and technology benefit society rather than threaten peace and international security.

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 harness AI to exploit biotechnologies for the development of biological weapons. The swift progress in bioscience and biotechnology, coupled with their interaction with AI, presents both challenges and opportunities for the BWC. These advancements are giving rise to novel biological risks while offering innovative ways to mitigate those risks through a modernised, 21st-century approach to transparency.

AI as a Biosecurity Enabler

With Southeast Asia's dense population, rapidly advancing biotechnology sector, and history of disease outbreaks, [AI offers](#) a valuable tool for disease surveillance in the region. For instance, Singapore's [National Environment Agency](#) has already employed AI-driven data analysis and predictive modelling to monitor and anticipate dengue fever outbreaks.

[AI-powered biological design tools](#) (BDTs) now provide a range of capabilities to biologists, driving innovative applications across life sciences research and development, agriculture, sustainability, pollution mitigation, energy security, public health, and national defence. These AI-enabled biotechnology tools facilitate the engineering of biological systems, including viruses and living organisms. In particular, BDTs can potentially drive progress in developing new medicines and vaccines to address emerging and re-emerging diseases.

Several [research laboratories](#) and [institutes](#) in Southeast Asia have begun utilising AI tools to boost pandemic and epidemic preparedness research, secure high-consequence pathogens inside laboratories, and fast-track healthcare and biotechnology innovation. AI tools are now used to enhance laboratory biosecurity by improving access control and preventing unauthorised access to sensitive biological materials and research facilities in several Southeast Asian biolabs.

Additionally, AI can support safer management of [Dual-Use Research of Concern](#) (DURC) by helping researchers assess the risks and benefits of certain studies before they proceed. This is particularly important for Southeast Asia, where biosafety and biosecurity standards, particularly in DURC, are still developing and vary widely across countries.

AI as a Biosecurity Risk Amplifier

In the absence of policy guardrails and regulatory oversight, AI-powered BDTs – akin to large language models (LLMs) for biologists – are making sophisticated bioengineering knowledge more accessible, even to individuals with limited formal scientific training and with malicious intent. The rapid advancement of AI-driven BDTs, such as protein-design technology, also presents serious risks of misuse, making it easier to design and synthesise dangerous pathogens that can spread more easily among human populations or cause more severe health damage.

AI-enabled DURC might also cause massive harm if used to make viruses with worrying new properties. The accessibility of AI-driven bioengineering tools lowers barriers to designing synthetic pathogens with potentially enhanced virulence or resistance to existing medical countermeasures. With the dual-use nature of both AI tools and life sciences, detecting deliberate misuse reliably is challenging.

When it comes to laboratory operations, AI-driven lab operations can potentially increase the risk of biosecurity breaches, either through cyber vulnerabilities or insider threats. As research labs and high-containment laboratories in Southeast Asia have increasingly relied on AI-enabled cybersecurity systems for operation, research and

security, it is imperative to develop a strong cyberbiosecurity culture among laboratory staff and researchers.

Integrated Biosecurity-AI Governance: Considerations for Southeast Asia

Establishing policy guardrails containing safeguards and risk reduction measures for dual-use AI-powered biotechnologies would be essential to promote responsible innovation. As the international community has yet to develop such guardrails for AI and biotechnologies, strengthening collaboration between governments, AI developers, and biosafety and biosecurity experts is critical for anticipating potential risks and identifying adequate safeguards.

The UN is encouraging BWC States Parties to agree to set up a new scientific advisory mechanism for the convention as soon as possible. It is also important that researchers and students fully understand the significant power – and potential dangers – of the dual-use technologies they engage with.

Promoting responsible use of AI and biotechnologies is critical to leverage the benefits of such technologies and prevent weaponisation risks. The dual-use nature of AI in biotechnology underscores the delicate balance between fostering innovation and implementing safeguards. In the absence of tight government oversight frameworks for the biotechnology industry and AI-powered biological tools, self-regulation, which essentially entails voluntary adoption of guidelines and principles, by scientists and industry players, has been the default framework.

The scientific community is one of the most important stakeholders in this regard. For instance, the “[Tianjin Biosecurity Guidelines](#) for Codes of Conduct for Scientists” are a set of 10 guiding principles and standards of conduct designed to promote responsible science practice and strengthen biosecurity governance at the national and institutional levels.

In Southeast Asia, several national biorisk and life science associations have developed voluntary guidelines on the use of emerging technologies in the life sciences. [Singapore's Biorisk Code](#) of Conduct for Life Sciences Industry and Professionals is an important document that seeks to prevent the potential misuse of the life sciences by promoting a culture of responsibility. In 2024, national biorisk associations from the Philippines, Indonesia and Malaysia launched [their joint project on establishing a knowledge-sharing network](#), fostering the exchange of best practices on safeguarding critical biotechnologies and AI tools and preventing deliberate misuse.

State and non-state stakeholders need to prioritise the development of comprehensive AI governance frameworks that clearly define the ethical use of AI in biological research and biotechnology. This can be achieved by enhancing multisectoral collaboration, bringing together expertise from diverse fields to collectively develop and implement feasible regulations and guidelines.

Conclusion: Future-Proofing ASEAN Biosecurity

Regional cooperation through ASEAN networks and capacity-building projects is

essential to developing consistent, cross-border policies addressing AI's potential to enhance biotech research and development and disrupt biosecurity in the region.

This collaboration could involve establishing regional AI-bioethics committees and working groups that would coordinate efforts on AI-related biosecurity threats, facilitate the exchange of best practices, and implement joint monitoring initiatives.

This effort could serve as an extension or programme within the upcoming ASEAN Biosafety and Biosecurity Network, which is set to be established in the near future. It would strengthen regional cooperation and ensure cohesive biosecurity governance across Southeast Asia.

Julius Cesar Trajano and Jeselyn are, respectively, Research Fellow and Research Analyst with the Centre for Non-Traditional Security Studies (NTS Centre) at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

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