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

RSIS COMMENTARY

www.rsis.edu.sg No. 156 – 17 October 2024

Cyberbiosecurity: Adapting to Emerging Threats in the Biosecurity Landscape

By Jeselyn and Julius Cesar Trajano

SYNOPSIS

Cyberbiosecurity is a growing area of concern. However, it remains poorly addressed and underappreciated, especially in Southeast Asia. A comprehensive approach incorporating cyber and biosecurity strategies such as raising awareness, capacity-building and engaging the biotechnology sector is needed.

COMMENTARY

In the recently concluded Annual Biorisk Conference on Strengthening Global Partnerships on Biosafety and Biosecurity, biosecurity experts in the Asia-Pacific highlighted an existential biological risk that demands urgent attention: cyberbiosecurity.

Cyberbiosecurity is an emerging field that addresses the vulnerabilities and risks at the intersection of cybersecurity and biosecurity. It has become critical with the rapid advancement of biotechnology and the cyber challenges associated with it. For instance, synthetic biology is now driving toward digitisation and automation, generating both biosecurity and cybersecurity risks.

Why Cyberbiosecurity Matters

The World Health Organisation (WHO) Laboratory Biosecurity Guidance issued in 2024, highlights potential cyber threats to bioscience laboratories and facilities.

These cyberbiosecurity threats include unauthorised access to or loss of information (e.g., research data, sensitive unpublished research, genetic DNA sequence data, information about sensitive biological agents); discontinuation of operations due to cyberattacks; unauthorised digital access to networked laboratory equipment;

sabotage of laboratory security system; theft, misuse or sabotage of information on sensitive biological agents; and espionage pertaining to biosecurity-relevant information.

As biotechnology becomes increasingly digitised, with massive amounts of genetic data, research outcomes, and even synthetic biology information/data being stored and processed in digital formats, the need to secure these assets against cyberattacks is critical.

Moreover, life science and bioscience laboratories and facilities have been steadily adopting advanced information technologies and operational technologies to enhance their critical scientific functions that support prevention, detection, response and recovery to catastrophic biosecurity events, including pandemics and deliberate use of biological weapons.

Several high-containment laboratories, for instance, in Southeast Asia have been working with biological agents or living microorganisms which are used for purposes such as medical, therapeutic, diagnostic or research, contributing to the advancement of health security as well as biotechnological and biomedical innovations.

Working with large volumes of biological agents can significantly increase risks. Biological operations in laboratories and related facilities are increasingly computer-based and utilise cloud-based systems.

Cyberattacks on these laboratories can effectively compromise the security of biological agents. Compounding this challenge is the advancement of Artificial Intelligence (AI) and its widespread use in cloud computing. This has significantly amplified the risk to facilities handling biological materials, as AI-enabled cyber threats are expected driving a rapid increase in security vulnerabilities.

As advancements in biological science technologies continue, AI-enabled cyberattacks are poised to become a growing threat to biosecurity. For instance, cybersecurity vulnerabilities in laboratory machines like DNA synthesisers could be exploited to introduce malware, alter design specifications, record DNA sequences, disrupt laboratory biosecurity protocols, or grant unauthorised access to sensitive data.

The Need for Cyberbiosecurity in Southeast Asia

The importance of enhancing cyberbiosecurity is paramount, especially in Southeast Asia, given the increasing use of digital applications in biotechnology. Countries like Singapore, Thailand, Malaysia, Indonesia, and the Philippines have adopted national cybersecurity strategies and national biosecurity policy frameworks, whether through a comprehensive law or various government regulations.

However, a significant challenge across the region is the lack of a cohesive policy framework that directly addresses cyberbiosecurity. Existing regulations are often fragmented, as cybersecurity and biosecurity are typically treated in isolation, leading to gaps in comprehensive protection.

Relatedly, the region's biosecurity experts have pointed out that cyberbiosecurity issues remain poorly addressed and underappreciated in the life science and biotechnology communities in Southeast Asia.

There is a lack of awareness and understanding of the potential cybersecurity risks and threats associated with digital lab data and digital information about biological samples inside laboratories. They suggest that organisations must adopt a new mindset and strategy on enhancing cybersecurity measures to protect identity-related attacks on data and remote control of facilities handling biological materials.

Way Forward for Cyberbiosecurity

The unique intersection between cyberphysical systems and biological systems in bioscience laboratories and facilities accentuates the critical need for enhanced cyberbiosecurity measures.

It is therefore important for biosecurity risk management experts and cybersecurity professionals to collaborate and jointly create standards, technical guidance, and best practices related to the enhancement of cyberbiosecurity in tandem with existing biorisk management practices in life science-related facilities.

There should be national efforts to develop cyber training environments that simulate the processes of biosecurity-related facilities. Cyberbiosecurity assessments should include not only relevant Information Technology/Operational Technology infrastructure but also regulatory information systems.

Furthermore, raising awareness is critical given the lack of understanding of the potential cybersecurity risks and threats associated with digital lab data and digital information about biological samples inside laboratories.

Regional and national networks of biorisk practitioners have a critical role to play in strengthening cyberbiosecurity within the bioscience and biotechnology community. National biosecurity associations in several Southeast Asian countries have begun introducing cyberbiosecurity as part of their national training programmes for their members.

The Asia-Pacific Biosafety Association had included cyberbiosecurity workshops in its recent biorisk conference, helping biosecurity experts, practitioners and stakeholders across the Asia-Pacific understand new threats and cyberbiosecurity measures.

Capacity building is also essential for developing a skilled workforce capable of addressing the complex challenges of cyberbiosecurity. Governments, academic institutions, and industry stakeholders should collaborate to offer specialized training programs, workshops, and certifications in cyberbiosecurity.

This regional training programme may take the form of cyberbiosecurity-focused workshops. One notable example is the Toxin and Venom Research Laboratory Biosecurity and Cyberbiosecurity Workshop, held in May 2023, involving organizations such as Health Security Partners (HSP), the Malaysian Society of Toxicology

(MySOT), and the Biosecurity Engagement Program (BEP) which brought together researchers from Malaysia, Thailand, and Singapore.

Finally, the role of the biotechnology sector is vital for advancing cyberbiosecurity initiatives. The biotechnology sector is predominantly driven by private industry, and governments must engage with these stakeholders to develop innovative solutions and share resources. Collaborative efforts between the public and private sectors can lead to the development of cutting-edge technologies, technical guidance and good practices that enhance cyberbiosecurity across the region.

Conclusion

Cyberbiosecurity must become a key priority for life science and biotechnology, ensuring that both cybersecurity and biosecurity are addressed in an integrated and comprehensive manner.

To address the complex challenges posed by cyberbiosecurity threats, Southeast Asia must develop a comprehensive approach that incorporates cyber and biosecurity strategies, including raising awareness, capacity building and engaging the biotechnology sector. Currently, the fragmented approach leaves critical cyberbiosecurity vulnerabilities that could be exploited by malicious actors.

Jeselyn and Julius Cesar Trajano are, respectively, Research Analyst and Research Fellow with the Centre for Non-Traditional Security Studies (NTS Centre) at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. They recently participated in the Asia-Pacific Biosafety Association's Annual Biorisk Conference held in the Philippines from 3 to 6 September 2024.

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