Panelists Recommendations

Panelist 1 - Ryan Teo:

"Recognizing that digital sequence information (DSI) has become integral to modern biological research and that certain applications of DSI-enabled technologies could pose risks to the objectives of the Convention, States Parties are encouraged to:

(a) Develop national approaches to assess and, where appropriate, apply biosecurity screening mechanisms to the synthesis of genetic material based on DSI, particularly for sequences encoding known pathogens or toxins listed under the Convention;

(b) Promote the adoption of voluntary biosecurity standards among gene synthesis providers, cloud laboratories, and related service providers operating within their jurisdiction;

(c) Share information on effective practices for balancing biosecurity concerns with the benefits of international scientific cooperation and the exchange of DSI for peaceful purposes consistent with Article X; and

(d) Consider DSI-related risks within the scope of their national implementation measures under Article IV, taking into account relevant developments in science and technology."

Panelist 2 – Julius Cesar Trajano

Establishment of Biological Security Centres of Excellence (CoEs)

The Biological Security Centres of Excellence (CoEs) should expand and institutionalise cyberbiosecurity training programmes tailored for Global South practitioners, with a strong alignment to the objectives of the Biological Weapons Convention (BWC). Such programmes should build technical and governance capacities to manage emerging risks at the intersection of digital and biological systems—including the protection of genomic data, safeguarding automation and AI-enabled laboratory infrastructures, and strengthening cybersecurity protocols across research institutions. By offering accessible, modular training delivered through regional hubs, the CoEs can help bridge capability gaps, promote responsible innovation, and support States Parties in meeting their BWC obligations. Enhanced international cooperation and resource-sharing will further ensure that Global South stakeholders can sustainably adopt cyberbiosecurity best practices and contribute to a more resilient global biosecurity architecture.

Leveraging on Regional Capacity

In Southeast Asia, the Association of Southeast Asian Nation (ASEAN)'s emphasis on capacity-building and reducing development gaps among member states can be directed toward enhancing the BWC implementation, cyberbiosecurity literacy,

technical skills, and regulatory coherence. This includes supporting governments in establishing safeguards against AI and cyber tech misuse in biological research. Through collaboration between UN agencies and ASEAN, tailored technical assistance, knowledge-sharing platforms, and public-private dialogues could foster enhanced cyberbiosecurity measures, practices and norms in the region.

Cybersecurity and Biosecurity Joint Initiatives

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.

Panelist 3 – Dr. Zia Ashraf

I would propose strengthening Annex III of the Draft final report of the Working Group on the Strengthening of the Convention by explicitly mandating the Science and Technology Advisory Mechanism to conduct: “Regular assessments of cyberbiosecurity risks and opportunities arising from the convergence of biological science with artificial intelligence, digital infrastructure, and automated laboratory systems.” This recommendation would not create additional legal obligations. Instead, it would improve transparency, enhance confidence, and help States Parties anticipate emerging challenges such as vulnerabilities in automated laboratory equipment, cyberattacks on genomic databases, or misuse of AI-enabled biological design tools