Panelists' Recommendations

Panelist 1: Cassidy Nelson

I recommend that States Parties not only adopt Annex III to establish the Science and Technology Advisory Mechanism, but explicitly mandate that its first 'Broad Theme' for review—as per Appendix I, Paragraph 2—be the convergence of Artificial Intelligence and the Life Sciences.

Why? Because AI model updates happen in weeks, while our diplomatic cycles take years. We cannot afford to establish this mechanism and then wait another year to decide what it should look at. Areas the Advisory Mechanism could potentially help address:

1. The "Digital" Verification Exercise (Annex I, Section D)

- Paragraph 26 of Section D encourages States Parties to organize "trial/practice application of compliance and verification measures". However, historically, these have been physical exercises (e.g., mock on-site inspections).
- Recommendation: Regarding Paragraph 26 of Section D on 'trial/practice application', I recommend that the Working Group explicitly encourages a digital verification exercise. States Parties should trial the use of AI-driven open-source intelligence (OSINT) and trade data analysis to detect simulated non-compliance. This would test the utility of AI as a verification tool without the logistical burden of a physical inspection, directly supporting the mandate of the new Open-Ended Working Group.

2. "Compute" as Article X Assistance (Annex II)

- Annex II (ICA Mechanism) focuses on the exchange of "equipment, materials and scientific... information". In 2025, "equipment" is increasingly interpreted as physical hardware (pipettes, sequencers). The "Hardware Gap" (lack of GPUs) is a major barrier to equity.
- Recommendation: In operationalising Annex II, specifically under Appendix I, Paragraph 3(c) regarding the exchange of 'equipment', we should explicitly clarify that 'cloud computing resources' and 'secure API access credits' constitute a form of material assistance. Providing access to secure, high-performance compute is the most effective way to democratise modern biology without the proliferation risks of shipping physical hardware or open-sourcing sensitive model weights.

3. Expanding "Codes of Conduct" to the Tech Sector (Annex I, Section B)

- Paragraphs 8 & 9 promote a "culture of responsibility" and welcome the *Tianjin Biosecurity Guidelines*. These guidelines are excellent but heavily oriented towards wet-lab scientists. A major source of risk is now computer scientists and AI engineers who lack biosecurity training.

- Recommendation: Regarding Paragraph 8 on 'developing or updating voluntary codes of conduct', I recommend adding specific language to include 'professionals in artificial intelligence and computational biology'.

The BWC needs to signal that biosecurity norms must extend beyond the laboratory to the server room. We should encourage States Parties to engage their domestic AI sectors to adopt codes of conduct analogous to the Tianjin Guidelines, specifically for the training and release of biological foundation models.

Panelist 2: Geoffrey Otim

My recommendation is for States Parties to consider establishing a BWC-aligned ‘AI-Biodesign Safety Framework’. This would harmonize safety filters, risk-tiered access models, red-zone definitions, developer responsibility guidelines, and audit expectations for AI-biodesign systems. Importantly, it should embed equity and capacity-building to ensure that Global South regions can access safeguarded, beneficial AI tools while collectively reducing the global risk of misuse.

Panelist 3: Sana Zakaria

States Parties are encouraged to ensure that the Science and Technology Advisory Mechanism’s monitoring, assessment and reporting of emerging and converging technologies relevant to the Convention, including developments in AI-enabled biodesign tools, are made available in a timely and transparent manner to inform voluntary cooperation and assistance under Article X. Such information may assist States Parties, upon their request, in identifying and addressing potential security-related gaps or vulnerabilities within their national implementation systems at an early stage, thereby helping to proactively mitigate possible biological security loopholes and strengthen the effective implementation of the Convention.

Role of Regional Cooperation and Bodies in Cyberbiosecurity: The Case of Southeast Asia

Julius Cesar Trajano, Research Fellow, S Rajaratnam School of International Studies, Nanyang Technological University, Singapore

Key Recommendations:

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.