Science and Technology Advisory Mechanism for the Biological Weapons Convention

A Proof-of-Concept Exercise

1 Background

1.1 Scientific experts from all five UN regional groups simulated a meeting of a science and technology advisory mechanism for the Biological Weapons Convention (BWC). The meeting took place in Trieste, Italy on 27-28 February 2024. This proof of concept exercise considered the subject *Exploring Benefits and Risks of Artificial Intelligence on Biosecurity and International Cooperation in the Context of the Biological Weapons Convention* as a way to foresee how such a mechanism might operate. The implementer of the meeting was the InterAcademy Partnership (IAP), a network of 150 academies of science, engineering and medicine in over 100 countries globally, that worked in coordination with the U.S. National Academies of Sciences, Engineering, and Medicine (NASEM). Thirty-eight participants from 32 countries and 20 online observers were invited to the meeting. The meeting included diversity in geography, subject matter expertise, age, and gender.

1.2 This in-person meeting was the second of two activities to simulate the “hybrid”\(^1\) science and technology advisory mechanism currently under consideration by States Parties of the BWC.\(^2\) The hybrid model would consist of a body open to experts from all States Parties to gather and discuss information on a possible topic, which would then be considered further by a limited-size body of experts. The first IAP activity was held virtually in an open-ended working group format on 14 November 2023.\(^3\) The November event intended to focus the questions to be considered in the second meeting in Trieste by a smaller group of technical experts. Both the virtual meeting in November and the in-person meeting in February were by invitation only and were held under the Chatham House Rule.

1.3 The February meeting in Trieste was chaired by Dr. Peter McGrath (IAP), assisted by Vice-Chairs Dr. Peter Ahabwe (Emergency Health Operations Centre, Uganda), Professor Neela Badrie (Caribbean Academy of Sciences, Trinidad & Tobago), Dr. Kavita Berger (NASEM), and Dr. Cedric Invernizzi (Spiez Laboratory, Switzerland). The meeting was further supported by Rapporteurs Dr. Kayhan Azadmanesh (Pasteur Institute of Iran) and Dr. Maria J. Espona (Information Quality, Argentina), and Dr. Jonathan Forman (Pacific Northwest National Laboratory, USA), who contributed as the “Science Advisor” in the proof-of-concept simulation. The list of participants and the meeting agenda are provided in Annexes 1 and 2 of this report. After brief introductions, participants were asked to consider artificial intelligence (AI) and its potential impacts on biosecurity and international cooperation in the context of the BWC in a general discussion and in two breakout groups. Participants informally endorsed this report of the simulation exercise, which did not attempt to formulate recommendations.

---

2 Overview

2.1 The meeting began with three briefings addressing AI and biosecurity, followed by guided discussions and breakout sessions. The briefings included a presentation on AI in the BWC context by Dr. Gunnar Jeremias (University of Hamburg, Germany), followed by more technically focused presentations on the anticipated impact of AI on both biosecurity and international cooperation from Professors Vukosi Marivate (University of Pretoria, South Africa) and Nicole Wheeler (University of Birmingham, United Kingdom).

2.2 Dr. Jeremias discussed the wide variety of applications of AI technologies in life sciences and other scientific disciplines. He provided an overview of the norms of the BWC and open questions that AI has generated regarding challenges and benefits to the Convention (including biosecurity, verification, forensics attribution). He also noted that a scientific advisory body could bolster the BWC confidence building measures. His presentation included perspectives on trends in the field of AI, weaknesses in our understanding of AI tools and their capabilities, and perspectives on AI governance. In this regard, he noted that the recent EU Directive and the U.S. Executive Order were unspecific, and that there were few regulations worldwide.

2.3 Professor Marivate noted that AI has been around in various forms for decades and we engage with it in our everyday lives, for example in algorithms in our internet search engines and mobile devices. Today, AI development cycles are faster, investments for developing new AI capabilities have increased, and widespread adoption of AI has occurred across many industries and sectors. Professor Marivate’s presentation highlighted the use of AI tools in South Africa for monitoring pests, including through use of computer vision to analyze digital images, and disease management through compiling and visualizing data from across public health resources.

2.4 Professor Wheeler presented the results of a 2023 report that addressed the governance of AI-bio capabilities and the biosecurity implications of AI developments. She highlighted examples of AI to predict the structures of highly toxic chemicals and discussed capabilities and limitations of current AI systems. AI tools can be used to efficiently collate technical information and summarize it in plain language for non-experts, and to help with experimental design and programming. She noted that when AI tools are not developed by domain experts they can fall short of providing benefits to researchers in that field. Professor Wheeler provided further insights into the capabilities and limitations of large language models (LLMs), biological design tools, and automation of laboratory processes.

2.5 Following the three presentations, Vice-Chair Dr. Berger moderated a guided discussion on the points raised by the speakers. Key issues from this discussion included:
(a) AI is a collective term referring to several major areas: machine learning, reasoning, natural language, computer vision, and robotics. Although there is no official definition of AI, for some it encompasses algorithms, data systems, and computer hardware working together to achieve intelligent behavior. These information technologies might have transformational impacts on the life sciences and biosecurity. In the context of the BWC, AI tools such as biological design software and LLMs capable of analyzing vast amounts of biological data

7 For a recent definition of AI system by the OECD see “What is AI? Can you make a clear distinction between AI and non-AI Systems?” Marko Grobelnik, Karine Perset, Stuart Russell, March 6, 2024, https://oecd.ai/en/wonk/definition
have generated both enthusiasm and concern, highlighting the need for multidisciplinary
teams of science and technology subject matter experts.

(b) AI tools produce digital, not physical outputs. Producing physical outputs such as a biological
material or substance (including biological weapons) requires laboratories, production
equipment, and technically proficient personnel.

(c) Generating meaningful outputs with AI requires “good questions” and reliable high-quality
data that minimize inaccuracies and, critically, bias. This necessitates having methods to
validate, protect, and secure the data used with AI tools. For these reasons, cyber security,
blockchain, and other technologies that protect and ensure data integrity also warrant
consideration in discussions about ensuring responsible use of AI with biological data.

(d) Understanding limitations of AI tools is necessary to ensure meaningful outputs. General
limitations include a lack of good quality datasets, uncertainty quantification in AI, and the
inability of current models to use reason to develop research questions and hypotheses. AI
models can introduce bias, errors, and “hallucinations” with no indication of which outputs
are accurate. The transfer learning (a technique in machine learning where a model developed
for a task is re-used in another task) of AI models between datasets is another possible
limitation.

(e) Limitations of biological design tools include narrow search space and protein design tools
not scaling to higher complexity systems such as viruses and microbes.

(f) AI tools can also be integrated into larger systems that include:

- Data collection capabilities: these might involve sensors that gather information from
  the environment.
- Hardware components controlled by AI: these could include unmanned vehicles or
  robotic laboratory systems that the AI commands to perform specific functions based
  on its analysis of data inputs. AI tools combined with biological data enable the
  advancement of knowledge and research in the life sciences.

(g) AI tools allow for faster processing of information and may aid in decision making processes.
They also provide capabilities to search large biological and clinical datasets, combine and
synthesize information, and recognize patterns from across the input data sources for enhanced
prediction of biologically relevant information such as drug targets, protein, peptides and other
biological macromolecular structures, and physiological effects. These capabilities have led
to increasingly more capable biological design tools.

(h) For biosecurity, some experts view AI as a potential game-changer that could have severe
negative consequences. This perspective is driven by concerns related to easier, faster, and
cheaper creation of biological weapons. AI driven peptide and protein design tools, in
particular, have elicited security concerns about their potential use in designing biological
toxins and/or infectious proteins (e.g., prions). Thus, AI-enabled protein design and synthesis
was recognized by meeting participants as a capability with immediate relevance to the BWC.
Participants noted that an assessment of these and similar developments for the BWC could
benefit from further deliberations through a temporary working group of suitable subject
matter experts.

---

8 Hallucinations are false or misleading results generated by an AI model. These errors can result from a variety of reasons, including insufficient
or biased training data and erroneous assumptions in a model.

9 “AI tools” use various techniques, for example, machine learning (one neural network) or deep learning (layered neural networks), to develop
large language models, generative pre-trained transformers (GPT), natural language processing, speech processing, computer vision, and other
models. For general information on AI and its current trends, see: (1) N. Maslej, L. Fattorini, E. Brynjolfsson, J. Etchemendy, K. Ligett, T.
Steering Committee, Institute for Human-Centered AI, Stanford University, Stanford, CA, April 2023; https://aiindex.stanford.edu/report; (2)

10 Temporary working groups are time-limited groups of experts guided and overseen by members of a scientific advisory body composed of some
members from the advisory body and outside experts who bring additional, focused expertise to the deliberations. Such groups, which have been
(i) Similarly, AI tools that can be used to study microbial systems might guide modification and engineering of known pathogens and/or creation of novel pathogens.\(^1\) AI tools can also be exploited to spread misinformation and disinformation that may adversely influence decision-making around response to biological threats or compliance with the obligations set by the BWC.

(j) Automation of scientific processes with AI tools can be limited by challenges of scale, and it comes with the need for expertise in maintaining and sustaining robotic systems. While robotic systems are sometimes seen as “deskilling” the scientist from bench work, keeping robotic systems operating requires workers with engineering and programming skills and is therefore “reskilling” some scientists.

(k) AI technologies continue to evolve and therefore some current limitations including lack of creativity in scientific hypothesis generation may become less constraining over time.

(l) Significant opportunities for AI tools in research and biotechnology exist, while their role in the BWC context has yet to be fully explored. Although potential nefarious uses have been discussed, concrete examples of attempts to develop AI-enabled (or designed) bioweapons have not been reported.

(m) Possible benefits to the BWC that can come from using AI include: tools that can enhance confidence in compliance with BWC obligations; forensics and attribution applications for investigations; screening of DNA sequences purchase orders to prevent the creation of pathogenic organisms; biosurveillance and detection; early disease warning; compilation of health data and outcomes; pandemic preparedness; vaccine and drug development; and research and/or information-sharing and collaboration. Sectors taking advantage of these benefits may use different definitions of biosecurity\(^12\) and all these capabilities come with the challenge of explainability and validation, especially when AI tools are used to inform decision-making.

(n) Given the abundance of potential opportunities for using AI systems, building “sandboxes” across organizations that make use of AI systems would be beneficial. Topics and data sets could be explored, predictive and diagnostic power of the AI tools evaluated, and the technology demystified to allow practical ways to understand it and use it could be helpful in assessing relevance to the BWC.

(o) With increasingly free access to information and unrestricted use of electronic resources, AI systems and the data they use can be stored in the cloud, eliminating the need for a physical location. The transnational nature of open access of data and open-source AI tools raises several policy and legal questions nationally and internationally.

(p) AI governance to guardrail the safety and ethical use of AI tools is receiving increased attention and will require collaboration across governments, organizations, and other stakeholders.

(q) AI governance discussions have generated concerns that over-regulation might harm rather than help biosecurity. Conversely, more cautious and controlled access approaches to mitigate risk might be seen as potentially limiting international cooperation and limiting access to AI tools for beneficial uses.

\(^1\) This concern was raised when synthetic biology emerged some 20 years ago and synthetic biologists and security experts learned how much we don’t know about structure-function. In addition, the synthetic/engineering biology community has faced significant challenges in developing truly novel organisms that are stable.

\(^12\) “Biosecurity” in the BWC context is most commonly used to refer to mechanisms to establish and maintain the security and oversight of pathogenic microorganisms, toxins and relevant resources, as discussed during the 2003 meetings of the Convention. See “Biosafety and Biosecurity,” submitted by the Information Support Unit, Meeting of Experts, Geneva, 1-5 December 2008, BWC/MSP/2008/MX/INF.1, digitallibrary.un.org/record/636795?ln=en8v=pdf.
3 Plenary Discussion

In the general discussion following the three briefings, the following main points were discussed:

3.1 AI is having impacts across all aspects of society, including how science is practiced. There is much hype over the risks and benefits alike, and diverse views exist on how to think about and provide practical guidance on AI and its adoption.
   (a) Meeting participants emphasized the importance of establishing a process for the continuous review of trends in AI, particularly its use in biology relevant to the BWC. This process should include ongoing discourse about the positive and negative implications for the BWC, facilitating further discussions on AI topics and the sharing of practical insights. This will ultimately inform the BWC community on emerging AI-related issues within its forums. It could serve as a standing agenda item for a BWC scientific advisory mechanism.
   (b) Development of a primer for the BWC States Parties that provides definitions and examples of the breadth of AI tools, their use with biological data, their capabilities and limitations, and their demonstrated applications in the life sciences could enrich discussions within the BWC about their positive and negative implications. This primer could include general considerations on issues such as data, computing, technical knowledge, and other needs for transforming AI designs from the digital to the physical world. The science and technology advisory mechanism could facilitate the development of such a primer.

3.2 For the BWC, LLMs and biological design tools were seen as having high relevance. AI is a rapidly evolving set of technologies and is regarded as a potential game-changer. Understanding the full impact of any AI capability or prediction would also need to consider the conversion of AI outputs from the digital to the physical world.

3.3 As an enabling technology, AI could be used to facilitate beneficial and harmful developments. Predicting the overall broad impact on the BWC is difficult, but exploring the influence would be helpful. AI enabled protein design and synthesis is an area with immediate relevance that has received attention in BWC forums. The ability to rapidly design and produce proteins as drugs may also be misused to design and produce highly toxic proteins and/or infectious proteins (e.g., prions). Additionally, AI might be used to redesign existing known pathogens to enable cross-over between species. Meeting participants noted that assessment of these developments for the BWC could benefit from further deliberations through a temporary working group of experts in virology, microbiology, biochemistry, AI models, and those at the interface of life-science and AI.

3.4 A BWC scientific advisory body, if created, could engage across AI-focused scientific and industrial communities (both within and outside the life sciences, and from across regional groups) and report on current trends and capabilities and relevance and implications on the BWC. Topics and issues identified as priorities could further considered by the scientific advisory body.

3.5 Other topics on AI and biosecurity that a BWC scientific advisory body might consider for further deliberation and/or future working groups could include:
   (a) The BWC relevant biological datasets used with AI tools and considering issues of validation, reliability, data access and protection, and data sharing and transfer of these data.
   (b) The potential role of AI tools in facilitating international cooperation and understanding the potential resource and model compatibility limitations.
   (c) The process and requirements of translating BWC relevant biological information and AI outputs from digital into physical space.
   (d) Development of codes of conduct and ethics to implement responsible AI practices, including equity of access and benefits by all regions, increase transparency in AI systems, and build “explainable” AI tools in the context of BWC.
4 Breakout sessions

4.1 Participants were divided into two breakout groups. Each group discussed the following four thematic questions:

1. How could AI contribute positively to advancing biotechnology and international cooperation in the BWC context?
2. How could AI negatively affect biotechnology and international cooperation in the BWC context?
3. How could AI contribute positively to strengthening security in the BWC context?
4. How could AI negatively affect security in the BWC context?

4.2 The groups were facilitated by Vice-Chair Dr. Ahabwe and Rapporteur Dr. Azadmanesh (Group 1) or Vice-Chair Professor Badrie and Rapporteur Dr. Espona (Group 2). At the conclusion of the breakout sessions, the participants reconvened in a plenary to report on the discussions.

4.3 The breakout session discussions raised many of the same issues and diversity of perspectives as were observed during the virtual open-ended working group format meeting held in November 2023, indicating the breadth and complexity of potential impacts of AI in the BWC context. Some responses applied to both positive and negative consequences. The points raised in the paragraphs that follow highlight key themes from the in-person discussion and represent issues that participants viewed as likely to remain relevant through at least the next five years.

4.4 Regarding the thematic question (1), *How could AI contribute positively to advancing biotechnology and international cooperation in the BWC context?*, the following points were raised:

(a) AI tools can monitor attempts to create a new pathogen, or to build a known high-risk pathogen, allowing controls to be put in place for biotechnology oversight.

(b) AI tools can monitor biotechnology activities and to verify and validate information, ensuring safety and beneficial outcomes from biotechnology and pharmaceutical research and development.

(c) AI tools can bridge gaps between countries with different resources through information generation, sharing, and analysis. This kind of information sharing could serve to encourage increased participation in the BWC meetings and foster international cooperation. This discussion focused on access to tools and did not consider resources required to maintain and adopt AI tools and systems.

(d) AI tools can guide and control robotic systems that can assist in patient care during routine operations and emergency situations such as pandemics.

(e) AI tools can aid in the discovery and development of effective pharmaceuticals and vaccines used as prophylactics and/or therapeutics.

(f) AI tools can test response capabilities, robustness of oversight mechanisms, and safety of biotechnology products and services.

(g) AI tools in combination with distributed ledger technology (e.g., blockchain), cyber security best practices, and other technologies for tracking and verifying transfers of materials, equipment, and/or digital information can control and secure supply chains from theft and diversion and protect data privacy.

(h) AI analysis of information on research, products, and capabilities in the life sciences could help identify subject matter experts who can address BWC related capability development.
4.5 Regarding the thematic question (2), *How could AI negatively affect biotechnology and international cooperation in the BWC context?*, the following points were raised:

(a) AI tools may allow masking of illicit biotechnology activities.

(b) Given the resources and expertise required to maximize the utility and effectiveness of AI tools, proliferation and adoption of AI technologies brings with it the potential to deepen disparity among countries with differing levels of resources. This point may appear to contradict a perceived benefit (see sub-paragraph 4.4(c) above) which was identified from a discussion that did not consider resource and expertise requirements.

(c) AI tools that enhance misinformation and disinformation can result in increasing distrust and stymie international collaborative efforts.

4.6 Regarding the thematic question (3), *How could AI contribute positively to strengthening security in the BWC context?*, the following points were raised:

(a) AI tools can be used for monitoring and tracking patterns of infectious disease outbreaks, predicting and preventing the spread of disease, and processing and using the information to reduce disease impact and evaluate risks to public health.

(b) AI tools can bolster pandemic preparedness or resilience to the intentional release of an infectious agent. The World Health Organization (WHO) has adopted AI for collecting data and issuing alerts.

(c) AI tools hold immense potential to strengthen biosecurity by predicting and identifying novel pathogens. This could revolutionize our ability to anticipate biological threats and bolster health systems. By pinpointing critical areas for preventive measures, AI can pave the way for swifter and more efficient assistance and response when outbreaks occur. Should a new agent/pathogen be identified (whether designed by AI or not), AI tools could identify key areas in health systems to prevent and support efficient assistance and response to biological threats when required.

(d) AI tools can allow more robust and informative risk assessments on biothreats, and aid in real-time decision-making so that those responding to biothreats can receive the information they need at the speed of relevance. Depending on the data, assumptions and parameters, tools of this kind could also be used for biosafety and risk assessments that can assist in oversight and regulatory approval processes.

(e) AI tools can process and recognize information that can help to identify patterns of illicit and/or clandestine acquisitions, new (and/or disruptive) life-science discoveries, and interesting and potentially concerning publications for further review. Such monitoring, however, would not likely be able to determine intent, and additional follow up and questions would likely be required. This approach may also have undesirable impacts on privacy and human rights.

(f) AI tools may be an enabler for both recognizing and countering misinformation and disinformation targeted at BWC States Parties.

(g) If States Parties were willing to share confidence building measures (CBMs) in a common digital space, AI tools could be employed to help review and summarize information from the CBMs for increased transparency.

4.7 Regarding the thematic question (4), *How could AI negatively affect security in the BWC context?*, the following points were raised:

(a) AI enabled misinformation and disinformation efforts might include research papers with false or manipulated data as a component to further push false perceptions about biothreats that ultimately weaken the effectiveness of decision-making processes. This could hamper prevention and response activities, and possibly attribution and confidence in BWC compliance. Participants recognized targeted disinformation as a tangible challenge to biosecurity.
(b) The AI discussion draws a lot of attention and speculation on biorisk and biothreats, yet the traditional biothreats are still a security concern and may provide easier pathways to access and deploy bioagents. In this regard, uncertainties and concerns about AI in the life sciences might detract attention from preparedness for higher probability biothreats and risks.

(c) AI tools have raised concerns about enabling the development of novel (and potentially lethal) bioagents that may be difficult to detect without advanced capabilities, and about lowering barriers to access of toxic and/or pathogenic agents by both State and Non-State actors.

(d) AI tools can be used to identify gaps and vulnerabilities in healthcare and threat response systems that can be exploited by adversaries.

(e) AI tools are dynamic and rapidly evolving, and therefore, identifying the most effective approaches for oversight and regulation remains unclear. Any approach is unlikely to keep pace with new advances and the emergence of new capabilities.

(f) As new technologies emerge, their integration with AI enabling information processing capabilities will continue to raise additional concerns of potential risks. In this context, neurochips were identified as a potential BWC relevant emerging risk that could be used to generate AI datasets.

4.8 Following the read-outs and discussion of the breakout sessions, Vice-Chair Dr. Invernizzi moderated a general discussion on items that would require further consideration. Issues raised in this discussion included:

(a) The topic of AI is highly complex. To fully understand how these AI tools work and what they are capable of requires transdisciplinary approaches and diverse subject matter expertise.

(b) Data sources, accessibility, and quality are fundamental issues in understanding and evaluating AI capabilities and uses. Guidelines that can inform policy makers and enhance technical literacy of AI tools could be beneficial.

(c) The topic of data accessibility is also highly complex. Arguments have been made for making data open for reasons of transparency and verifying suitability for use in AI models, while at the same time arguments exist for protecting sensitive information and ensuring that critical data used in AI models are not manipulated or compromised.

(d) Many beneficial applications of AI (including those with relevance to the BWC) can be realized within the life sciences and for countering/reducing biological risks and threats. Despite these opportunities, discussions around AI tend to drift toward areas of concern. The focus on risks appears to highlight the presence or apparent presence of randomness and variability in data or in the outcomes of the use of AI tools, how comfortable users are with trusting the outcomes, and the unknowns related to future implications of use of AI.

(e) Together with technical and scientific questions, meeting participants discussed non-technical issues such as regulatory, data privacy, and others.

(f) Meeting participants generally agreed that a technical discussion in a temporary working group on selected benefits and risks of AI and some prioritization of AI issues relevant to both individual BWC articles and overall implementation of the BWC might be a useful approach.

(g) One critical and complex aspect of considering AI implications for the BWC is the question of what a bioweapon looks like. With traditional military technologies (such as a bomb or missile), recognizing and understanding what a multi-use technology is and what constitutes a weapon component are relatively easy. AI is an enabling tool, not a weapon component in the traditional sense, and coupling enabling technologies with life-science research (which can have multi-use implications) serves to create greater levels of uncertainty on intent and applications of the research efforts.
5 Acceptance of the Report

5.1 Following a brief discussion led by Dr. Forman regarding who the science advice is intended for (e.g., the BWC States Parties) and what it might be used for, the participants reviewed the key points from their deliberations and considered how these could be helpful for the BWC community to be made aware of.

5.2 The meeting participants reviewed and discussed a draft report, provided additional comments and edits, and accepted a preliminary version as an accurate record of the meeting discussions. Participants were informed that after incorporating the additional edits and comments, the report will be shared with participants in correspondence.

5.3 The implementers found that the two meetings succeeded in serving the purpose of the proof of concept of an advisory body, both in terms of simulating the process of convening such a scientific advisory body and of simulating the deliberations of such a body. Much of the success of this activity could be owed to the networks of the IAP and NASEM as neutral convenors of global talent. The implementers aim to prepare a report that summarizes their views and impressions related to the process of the proof-of-concept exercise.

5.4 The Chair thanked the IAP for organizing the meeting and for making the participation of experts from all regions possible. He also thanked the presenters and participants for fruitful discussions, and expressed his appreciation to the Vice-Chairs, Rapporteurs, and Science Advisor for their contributions and engagement in the simulation.

5.5 The Chair closed the proof-of-concept meeting on 28 February 2024.

1 Integrated circuit chips that can record signals from neural activity signals from an animal (or human) brain in real time. Some research in this field combines the ability to capture and digitalize neural activity with biosensor components.