UNIDIR

Funded by the European Union

Cyberbiosecurity: A Matter of International Peace and Security?

LOUISON MAZEAUD • ANDRAZ KASTELIC

Acknowledgements

Support from UNIDIR's funders provides the foundation for all of the Institute's activities. This study was produced by UNIDIR's Weapons of Mass Destruction Programme (WMD) and Security and Technology Programme (SECTEC).

This publication was funded by the European Union as part of the UNIDIR project: 'Science and Technology Watchtower: Monitoring Innovation for Disarmament.'

Gratitude is extended to James Revill (UNIDIR), Giacomo Persi Paoli (UNIDIR), Samuele Dominioni (UNIDIR) and Beyza Unal (UNODA) for providing their thoughts on this paper.

About UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

Note

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

Citation

Louison Mazeaud and Andraz Kastelic, "Cyberbiosecurity: A Matter of International Peace and Security?" (Geneva: UNIDIR, 2025), **https://doi.org/10.37559/WMD/25/CBW/02**

Authors

Louison Mazeaud is an Associate Researcher in the WMD Programme at UNIDIR where she focuses on the nexus between emerging technologies and weapons of mass destruction.

Andraz Kastelic is a Senior Researcher and Coordinator of the SECTEC's Cyber Resilience Workstream at UNIDIR.

Cover image: Futuristic DNA strand (generated with AI). Credit: Adobe Stock / vivekFx.

Contents

Executive Summary

The global bioeconomy is growing rapidly notably aided by the convergence of biotechnology with advanced and powerful information and communication technologies (ICT). This nexus between the **digital and biological domains** brings numerous benefits to a wide range of sectors from agriculture to medicine. Concomitantly, the number of biological research and development facilities is also growing worldwide.

This convergence introduces new and potentially significant risks. They include possible attacks on biological research and development facilities, targeting the **confidentiality, integrity and accessibility** of information. In the context of international peace and security, ICT incidents present a spectrum of consequences, from minor to significant. For example, a minor event could involve a malicious actor spoofing an agricultural facility's sensors to transmit false data to owner, impacting the annual production of crops. Conversely, a significant event could involve a malicious actor infiltrating the ICT systems of a biological research and development facility, to interfere with an automated production system, remotely altering the compounds, thus rendering its product ineffective, or worse, harmful.

Various scholars and practitioners have attempted to name and define a concept recognizing the unique characteristics of the infrastructure, data, vectors, and risk implications at this nexus. **Cyberbiosecurity** refers to a collection of practices aimed at addressing the potential ICT threats to those systems at the intersection of the digital and biological domains. More specifically, it includes methods, procedures and measures to tackle ICT threats to biosafety and biosecurity.

To better understand the nexus between ICT and the biological field, this paper begins with an outline of some of the benefits introduced by the integration of advanced ICT in biological research and development. It then introduces the above definition of the concept of 'cyberbiosecurity' and proceeds to outline some of the key risks at this nexus.

The **New Agenda for Peace** launched by the Secretary-General in 2023 highlights the need for Member States to prevent the weaponization of emerging domains and promote responsible innovation (Action 11). The 2024 **Summit of the Future** was an opportunity for Member States to reaffirm their commitment to the prevention of biorisks and misuse of emerging technologies. This was particularly reflected in the **Pact for the Future**, specifically in Action 26 (to uphold disarmament obligations and commitments) and Action 27 (to seize opportunities associated with new and emerging technologies and address potential risks posed by their misuse).[1] Cyberbiosecurity appears at the junction of these two goals.

This notions has however received tangential attention in the multilateral discussion on international ICT security, specifically the General Assembly subsidiary bodies the Groups of Governmental Experts from 2004 to 2021 and Open-ended Working Groups since 2019. In the context of the **Biological and Toxin Weapons Convention** (BWC), limited attention has been given to cyberbiosecurity related issues. There are however cyber-related elements mentioned in documents and statements of the last 10 years.

---

[1] United Nations. (September 2024). Pact for the Future, Global Digital Compact, and Declaration on Future Generations. https://www.un.org/sites/un2.un.org/files/sotf-pact_for_the_future_adopted.pdf

Finally, in the **United Nations Security Council**, several States have expressed concern over the increase in cyber operations targeting critical infrastructure, including in the health sector, particularly during the COVID-19 pandemic. While not encompassing all aspects of this issue, these discussions can help in sensitizing the international community and practitioners on the need for better measures.

One way forward could be to clarify the breadth of the concept of cyberbiosecurity through exchanges with relevant communities, and considering cyberbiosecurity in the context of the ongoing **BWC Working Group**, notably in discussions on scientific and technological developments. This approach could allow for an exchange of views and good practices in the cyber domain and their applicability to biological research and development facilities.

Ninth Review Conference of the BTWC, Geneva, 2022. Credit: UN photo / Violaine Martin.

Researcher looking through a microscope in a laboratory (generated with AI). Credit: Adobe Stock / Jin Kansa.

1. Introduction

The global bioeconomy[2] is growing rapidly, creating new possibilities to address societal challenges through biotechnology. Such new biotechnological solutions are aided by the convergence of biotechnology with increasingly advanced and powerful information and communication technologies (ICT).[3] While this expanding interaction between the biological and digital domains has the potential to lead to great benefits, it could also unlock a range of new and potentially significant risks. The recent COVID-19 pandemic illustrated some of these risks, with critical healthcare infrastructures and pharmaceutical research organizations among the entities most targeted by malicious cyber actors in recent years.[4] This challenge has been recognized in United Nations forums, as the Deputy Permanent Representative of Costa Rica to the United Nations stated, "[we] must take immediate and decisive action to prevent and stop cyberattacks that target hospitals, healthcare, and research organizations".[5]

---

2 "The bioeconomy means using renewable biological resources from land and sea, like crops, forests, fish, animals and micro-organisms to produce food, materials and energy". European Commission. Accessed 18 November 2024. https://research-and-innovation.ec.europa.eu/research-area/environment/bioeconomy_en

3 Petersen, I., Kollek, R., Brüninghaus, A., Döring, M. (2015). Systems Biology, Information Technology, and Cancer Research. In: *Contextualizing Systems Biology*. Springer. https://doi.org/10.1007/978-3-319-17106-7_4

4 INTERPOL. (4 August 2020). "INTERPOL Report Shows Alarming Rate of Cyberattacks during COVID-19". https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19; Fouad, N. S., (2024). "Cyberbiosecurity in the New Normal: Cyberbio Risks, Pre-Emptive Security, and the Global Governance of Bioinformation". *European Journal of International Security*, 9(4). https://doi.org/10.1017/eis.2024.19

5 Costa Rica, Permanent Mission to the United Nations. (26 August 2020) "Statement at the Security Council Arria Formula: Cyber Attacks Against Critical Infrastructure". New York, p. 1.

The risks arising from the convergence of biotechnology and ICT are multifaceted and potentially significant. They include possible attacks on connected networks and information systems that are crucial for the confidentiality, integrity and accessibility of information. Some States have expressed concern that such malicious operations could lead not only to loss of life, but also damage to public health and trust, as well as the environment.[6] Moreover, these risks are likely to become more complex as technologies advance, further converge and diffuse around the globe in the years to come.

An increasing number of scholars, practitioners, and policymakers are examining the emerging challenges at the intersection of cyber and biological domains. In this context, terms such as 'cyberbiosecurity', 'biocybersecurity', and 'cybersecurity in the bioeconomy' have been introduced, though their definitions and scopes remain under discussion.[7] Given the unique characteristics of the infrastructure, data, vectors, and risk implications at this nexus, there may be a need for a more nuanced conceptual framework than what is typically encompassed by the broader term 'cybersecurity'.

This paper is produced as part of a UNIDIR project ('Science and Technology Watchtower: Monitoring Innovation for Disarmament') supported by the European Union and aiming to advance evidence-based research on scientific and technological innovations and their implications for disarmament and international security.[8] It contributes to the project by facilitating knowledge transfer on risks posed by emerging technologies and promoting dialogue between diverse expert communities, including in the field of biosecurity and ICT, as well providing analysis to support multilateral efforts in these two domains. To better understand the nexus between ICT and the biological field, the paper begins with an outline of some of the benefits introduced by the integration of advanced ICT in biological research and development. It then proposes a definition of the concept of 'cyberbiosecurity' and proceeds to outline some of the key risks at this nexus. The paper also considers how this cross-regime issue is being addressed in relevant multilateral forums tasked with ensuring international peace and security, notably within the United Nations, as well as nationally by States Parties to the Biological Weapons Convention (BWC).

---

6 United States of America. (2022). "United States remarks for March 2022 session of the OEWG, as prepared". https://documents.unoda.org/wp-content/uploads/2022/04/US-remarks-for-March-OEWG-norms.pdf. See also Radoini A., Siddiqui M. (2021). "The Cyber-Threat Against Chemical, Biological, Radiological and Nuclear (CBRN) Facilities" *Freedom from Fear Magazine: The past, the present and the future are in our hands* (UNICRI December) p. 106. https://unicri.it/sites/default/files/2021-12/16_cyber_threat.pdf

7 Titus, A. J., Hamilton, K. E., Holko, M. (2023). 'Cyber and Information Security in the Bioeconomy'. In: Dov Greenbaum (ed.), *Cyberbiosecurity: A New Field to Deal with Emerging Threats*. Springer. https://doi.org/10.1007/978-3-031-26034-6_3

8 See European Union Council Decision (CFSP) 2025/529 of 17 March 2025 on Union support for the United Nations Institute for Disarmament Research project 'Science and Technology Watchtower: Monitoring Innovation for Disarmament'. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32025D0529

2. ICT in Biological Research and Development

The integration of ICT in life science research and development has enabled cheaper, faster and more effective research. This in turn has unlocked new opportunities to enhance biological research and development. Specific tools to realize these opportunities introduce advanced digital and communication components to biological research and production facilities. The use of large datasets, fast network connections and powerful computer hardware has become the norm.[9]

ICT has revolutionized the collection, storage, and analysis of vast genomic datasets as well as datasets that provide a set of synthetic biology tools that can be used to design organisms with desired properties. In the pharmaceutical industry, for example, these datasets have been explored using machine learning tools to identify antimicrobial peptides for clinical trials.[10] Such efforts include trials to address antibiotic resistance, which the World Health Organization (WHO) has labelled as one of today's biggest threats to global health, food security, and development.[11]

The availability of commercial synthesized DNA, increased computational power and computer-aided design tools (CAD) have also considerably advanced genome editing capabilities, including the development of CRISPR techniques which can help in gene therapy and the correction of mutations.[12] The increase in computation power over the last decade has played an essential role in the development of CRISPR techniques and can be used to further enhance this technology in the future, potentially opening this up for important applications in multiple sectors.[13]

Furthermore, biological laboratories are increasingly relying on ICT-enabled automation technologies to perform experiments. For instance, 'cloud lab' technology allows researchers to conduct activities remotely.[14] Experiments can be planned and performed without real-time supervision, as robots undertake tasks autonomously from testing substance properties to lab cleaning.[15] Such cloud labs can help to make life science

---

9 Mueller, S. (2021). "Facing the 2020 Pandemic: What Does Cyberbiosecurity Want Us to Know to Safeguard the Future?". *Biosafety and Health*, 3(1). https://www.sciencedirect.com/science/article/pii/S2590053620301129

10 de la Fuente-Nunez, C. (2022). "Antibiotic Discovery with Machine Learning". *Nature Biotechnology*, 40. https://www.nature.com/articles/s41587-022-01327-w

11 World Health Organization. (31 July 2020). "Antibiotic Resistance". https://www.who.int/news-room/fact-sheets/detail/antibiotic-resistance

12 Sun, J.-Y., Hu, H.-B., Cheng, Y.X., Lu, X.-J., (2020). "CRISPR in Medicine: Applications and Challenges". *Briefings in Functional Genomics*, 19(3). https://academic.oup.com/bfg/article/19/3/151/5838014

13 The first efforts to discover such systems relied on digital programmes and databases available online including: "Basic Local Alignment Search Tool (BLAST), repeated sequence identifier program (RepeatMasker), and the DNA base-calling program Phred". Shang, S., Cai, X.S. & Qi, L.S. (2022). "Computation Empowers CRISPR Discovery and Technology". *Nature Computational Science*, 2. https://www.nature.com/articles/s43588-022-00321-1

14 Arnold, C. (13 June 2022). "Cloud Labs: Where Robots Do the Research". *Nature*. https://www.nature.com/articles/d41586-022-01618-x

15 Bose, P. (18 March 2024). "How Cloud Labs and Remote Research Shape Science". *The Scientist*. https://www.the-scientist.com/how-cloud-labs-and-remote-research-shape-science-71734

research more accessible, available and potentially cheaper.[16]

Finally, the number of facilities across the world handling dangerous pathogens and toxins is increasing alongside the growth of the bioeconomy.[17] In addition to an estimated 51 existing Biosafety level (4) (BSL-4) laboratories,[18] 18 more are reportedly underway or planned across the globe.[19] BSL-2 and BSL-3 laboratories that are capable of undertaking research on dangerous pathogens, are also understood to be increasing in number. In short, facilities handling dangerous pathogens and toxins are increasing in number and becoming 'smarter' by the day.[20]

3. New Risks and Cyberbiosecurity

The integration of ICT may have enriched biological research and development, however the convergence of these areas has introduced new risks, exacerbating traditional biosafety and biosecurity risks. Much like the other sectors considered as 'critical infrastructure', the health sector and related biological research and development systems are under an increased strain from ever-increasing and ever-evolving malicious ICT threats[21] conducted by "State [as well as] non-State actors, including terrorists and criminal groups".[22] Some States have expressed concern that cyber operations aimed at systems used by biological research and development facilities, for instance, could lead to loss of life.[23] Others cautioned of the possibility of a malicious ICT incident triggering irreparable damage to the natural environment or resulting in psychological impact to individuals.[24]

The increased interconnectedness of the systems and associated heightened risks

---

16 Arnold, C. (13 June 2022). "Cloud Labs: Where Robots Do the Research". *Nature*. https://www.nature.com/articles/d41586-022-01618-x

17 King's College London and George Mason University. (2023). *Global BioLabs Report* 2023, p. 5. https://static1.squarespace.com/static/62fa334a3a6fe8320f5dcf7e/t/6412d3120ee69a4f4efbec1f/1678955285754/KCL0680_BioLabs+Report_Digital.pdf

18 For a detailed explanation of biosafety levels, you may consult: 'Biosafety levels', Faculty of Medical and Health Sciences, Tel Aviv University. Accessed 6 May 2025. https://en-med.tau.ac.il/safty_biology_biosafety_evel-2020

19 King's College London and George Mason University. (2023). *Global BioLabs Report 2023*, p. 5. https://static1.squarespace.com/static/62fa334a3a6fe8320f5dcf7e/t/6412d3120ee69a4f4efbec1f/1678955285754/KCL0680_BioLabs+Report_Digital.pdf; Kaiser, J. (17 March 2023). *Growing Number of High-Security Pathogen Labs around World Raises Concerns*. *Science*. https://www.science.org/content/article/growing-number-high-security-pathogen-labs-around-world-raises-concerns

20 Li, J. et al. (2022). "Smart Heightened-Containment Biological Laboratory: Technologies, Modules, and Aims". *Journal of Biosafety and Biosecurity*, 4(2). https://doi.org/10.1016/j.jobb.2022.06.003

21 General Assembly. (18 March 2021). "Developments in the field of information and telecommunications in the context of international security". A/75/816, para. 15.

22 Ibid., p. 16.

23 United States of America. (2022). "United States remarks for March 2022 session of the OEWG, as prepared". https://documents.unoda.org/wp-content/uploads/2022/04/US-remarks-for-March-OEWG-norms.pdf

24 Radoini A., Siddiqui M. (2021). "The Cyber-Threat Against Chemical, Biological, Radiological and Nuclear (CBRN) Facilities". *Freedom from Fear Magazine: The past, the present and the future are in our hands* (UNICRI December), p. 106. https://unicri.it/sites/default/files/2021-12/16_cyber_threat.pdf

dictate the commitment to cybersecurity,[25] understood as the collection of actions intended to protect ICT systems and aimed at preserving their availability, integrity and confidentiality.[26] ICT threats can be classified as intentional or unintentional (or accidental), as well as active or passive threats. Active ICT threats aim to alter the state of a system; the objective of a passive threat, on the other hand, often ends with data collection.[27] This is not to say that passive threats cannot enable or even evolve into active ones; indeed, unauthorized penetration of an ICT system and passive data collection can serve as so-called 'pre-positioning' and may very well enable alteration of the said system and its operation.

While there is no agreed definition, we could situate the concept of **cyberbiosecurity** at the intersection of biosafety, biosecurity and cybersecurity. **Cyberbiosecurity refers to a collection of practices aimed at addressing the potential ICT threats to those systems at the intersection of the digital and biological domains. More specifically, it includes methods, procedures and measures to tackle ICT threats to biosafety and biosecurity.**

Broadly, **ICT threats to biosafety** manifest as unintentional malperformance of ICT systems with unintended consequences. More specifically, ICT threats to biosafety could take the shape of an accidental release online of the genome sequence for a highly pathogenic virus due to human error interacting with the ICT infrastructure or due to software malfunction. In the context of cybersecurity, measures to promote behaviour known as 'cyber hygiene' are the principal countermeasures against such threats.

ICT threats to biosecurity could include the intentional compromising of a computerized system that is part of or adjacent to a biological research and development facility. As per the above-outlined taxonomy of threats, an ICT threat to biosecurity could be passive or active in nature. Unauthorized passive observation of the ICT systems does "not result in any modification to any information contained in the system(s) [so that] neither the operation nor the state of the system is changed".[28] Active ICT threats to biosecurity, on the other hand, are characterized by unauthorized modification of the targeted ICT system (operation) or connected assets.[29]

---

25 General Assembly. (31 January 2003). "Creation of a global culture of cybersecurity". A/RES/57/239.

26 For comprehensive definition of *cybersecurity*, see International Telecommunication Union. (April 2008). "Overview of Cybersecurity". Recommendation X.1205. https://www.itu.int/rec/T-REC-X.1205-200804-I

27 International Telecommunication Union. (March 1991). "Security Architecture for Open Systems Interconnection for CCITT Applications". Recommendation X.800. https://www.itu.int/rec/T-REC-X.800-199103-I

28 Ibid., para. A.2.4.3.

29 Ibid.

4. Threats to International Peace and Security

Cyberbiosecurity is an important consideration in the context of international peace and security. Cyberbiosecurity measures aim, for instance, to reduce the risk of release of security-sensitive biological information that could be used to develop biological weapons; the potential for sabotage of biological facilities; as well as the potential for the manipulation of sensitive information to undermine credibility of medical countermeasures through disinformation campaigns. ICT incidents impacting biological research and development facilities and resulting in "losses from productivity, system downtime, data loss, shortages of critical medical supplies, and loss of public trust"[30] could lead to consequences beyond inconvenience and potentially have impact on international peace and security.

In the context of international peace and security, ICT incidents present a spectrum of consequences, from minor to significant. For example, a minor event could involve a malicious actor spoofing an agricultural facility's sensors to transmit false data to owner, impacting the annual production of crops. Conversely, a significant event could involve a malicious actor infiltrating the ICT systems of a biological research and development facility, to interfere with an automated production system, remotely altering the compounds, thus rendering its product ineffective, or worse, harmful. Alternatively, malicious cyber actors could also interfere with the physical components of a biological research and development facility, such as the supervisory control and data acquisition systems.[31] Such interference could hamper the capabilities of the laboratory to deliver immunization compounds in times of a pandemic or could disable mechanisms preventing the accidental release of deadly pathogens. Research has also illustrated that malicious actors could remotely interfere with synthetic DNA orders to encode harmful agents.[32]

5. Cyberbiosecurity and the United Nations

The potential negative effects of ICT threats to biosafety and biosecurity on international peace and security have not escaped the attention of the international community. Indeed, States have availed to the various multilateral institutions to engage in discussion on the issue at hand, even if in a rather fragmented and limited manner for now. An overview of current debates and initiatives in the international system featuring cyberbiosecurity follows.

---

[30] Crawford, E. et al. (2023). "Cyberbiosecurity in high-containment laboratories". *Frontiers in Bioengineering and Biotechnology*, 11, p. 4. https://www.frontiersin.org/articles/10.3389/fbioe.2023.1240281/full

[31] See D. -J. Kang, J. -J. Lee, S. -J. Kim and J. -H. Park. (2009). "Analysis on cyber threats to SCADA systems". *2009 Transmission & Distribution Conference & Exposition: Asia and Pacific, Seoul, Korea (South)*, 1-4. https://ieeexplore.ieee.org/abstract/document/5357008

[32] Puzis, R., Farbiash, D., Brodt, O. et al. (2020). "Increased cyber-biosecurity for DNA synthesis". *Nature Biotechnology* 38, 1379–1381. https://doi.org/10.1038/s41587-020-00761-y

The New Agenda for Peace launched by the Secretary-General in 2023 highlights the need for Member States to prevent the weaponization of emerging domains and promote responsible innovation (Action 11). As a policy brief in preparation for the **Summit of the Future**, the Agenda outlined as part of Action 11 recommendations for tackling the extension of conflict in hostilities to cyberspace (para. 73) and for improving global anticipation, coordination and preparedness to address biorisks (paras. 78–79).[33] The 2024 Summit of the Future was an opportunity for Member States to reaffirm their commitment to the prevention of biorisks and misuse of emerging technologies.[34] This was particularly reflected in the **Pact for the Future**, specifically in Action 26 (to uphold disarmament obligations and commitments) and Action 27 (to seize opportunities associated with new and emerging technologies and address potential risks posed by their misuse).[35] Cyberbiosecurity appears at the junction of these two goals.

In the context of the **Biological and Toxin Weapons Convention** (BWC), limited attention has been given to cyberbiosecurity related issues. There are however cyber-related elements mentioned in documents and statements of the last 10 years. Most of these references to cyberbiosecurity are presented by States Parties and experts in the context of discussions on scientific and technological developments. For example, a working paper submitted by Canada to the Ninth BWC Review Conference in 2022 indicates that the United States is implementing projects with cyberbiosecurity components in the context of the Global Partnership;[36] a working paper submitted by the Russian Federation in 2021 summarizes a BWC-focused conference panel where one participant raised the "emerging challenge of cyberbiosecurity at the intersection of life sciences and information technology",[37] and a working paper submitted by the European Union in 2022 notes that "Germany organised a Global Partnership Conference on Current Biosecurity Challenges, where stakeholders discussed high-risk research, the possible use of high-consequence pathogens as a weapon, cyber-biosecurity, and disinformation as well as risk reduction measures".[38]

Cyberbiosecurity has received tangential attention in the multilateral discussion on international ICT security, specifically the General Assembly subsidiary bodies the **Groups of Governmental Experts** from 2004 to 2021 and **Open-ended Working Groups** since 2019. Extensive discussion on threats to and measures for protecting critical infrastructure has taken place and States have agreed norms of voluntary, non-binding State behaviors in cyberspace.

---

33 General Assembly. (3 July 2023). "Our Common Agenda. Policy Brief 9: A New Agenda for Peace". United Nations. A/77/CRP.1/Add.8. https://digitallibrary.un.org/record/4015374

34 United Nations. Summit of the Future (website). Accessed 6 May 2025. https://www.un.org/en/summit-of-the-future

35 United Nations. (September 2024). *Pact for the Future, Global Digital Compact, and Declaration on Future Generations*. https://www.un.org/sites/un2.un.org/files/sotf-pact_for_the_future_adopted.pdf

36 Ninth Review Conference of the States Parties. (6 December 2022). "International Activities of Global Partnership Member Countries related to Article X of the Biological and Toxin Weapons Convention (2017-2022)". Biological and Toxin Weapons Convention. BWC/CONF.IV/WP.51. https://documents.un.org/doc/undoc/gen/g22/606/46/pdf/g2260646.pdf

37 Meeting of Experts on Institutional Strengthening of the Convention. (1 September 2021). International research and practical Conference "Global Biosecurity Challenges. Problems and Solutions" (Sochi, 24-25 June 2021)". Biological and Toxin Weapons Convention. BWC/MSP/2020/MX.5/WP.5 https://documents.un.org/symbol-explorer?s=BWC/MSP/2020/MX.5/WP.5&i=BWC/MSP/2020/MX.5/WP.5_0574157

38 Ninth Review Conference of the States Parties. (29 November 2022). "Support of the European Union and its Member States to Strengthening Biosafety and Biosecurity Globally". Biological and Toxin Weapons Convention. BWC/CONF.IV/WP.38. https://documents.un.org/symbol-explorer?s=BWC/CONF.IX/WP.38&i=BWC/CONF.IX/WP.38_7328911

As recently as 2024, the progress report of the Open-ended Working Group on developments in ICT in the context of international security recognized the healthcare sector as integral critical infrastructure and warned that cyber operations targeting such infrastructure can have "cascading national, regional and global effects".[39] Previously, the 2021 report of the Group of Governmental Experts on responsible State behaviour in cyberspace recognized that the "COVID-19 pandemic heightened awareness of the critical importance of protecting health care and medical infrastructure and facilities, including through the implementation of the norms addressing critical infrastructure".[40] Furthermore, a number of States consider the agriculture, medical research, and health care – all sectors where cyberbiosecurity is an important concern – as critical national infrastructure.[41]

To reduce the risks to international peace, security, stability, States have elaborated 11 norms of voluntary State behaviour in cyberspace. Some of these norms are aimed specifically at, or have relevance for, critical infrastructure protection,[42] although they do not necessarily speak to State ICT behaviour in relation to specific agricultural, medical, pharmaceutical or other contexts.

In the past years, several States have expressed concern in the Security Council over the increase in cyber operations targeting critical infrastructure, including in the health sector, particularly during the COVID-19 pandemic.[43] In November 2024, the WHO Director-General briefed the Security Council on ransomware attacks on healthcare as well as cyberattacks affecting this sector and their significant impacts.[44] While not encompassing all aspects of this issue, these discussions can help in sensitizing the international community and practitioners on the need for better measures.

Further to its cyberbiosecurity sensitizing efforts within the United Nations system, the **World Health Organization** recently published a guidance for laboratory biosecurity, updating a previous guidance from 2006.[45] The guidance highlights the importance of cybersecurity and provides concrete recommendations on how to introduce cybersecurity in biosecurity risk assessments – a useful resource for States and organizations considering the implementation of cyberbiosecurity measures.

---

39 General Assembly. (22 July 2024). "Developments in the field of information and telecommunications in the context of international security". A/79/214, para. 14.

40 General Assembly. (14 July 2021). "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security". A/76/135, para. 45.

41 See, e.g., European Union. (2023). "EU statement (Agenda item 5: Existing and Potential Threats). Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021-2025 06.03-10.03.2023." https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/EU_THREATS.pdf

42 See, e.g., General Assembly. (14 July 2021), Norm 13 (g) and Norm 13 (h).

43 As argued by, for instance, Ambassador Maritza Chan, Deputy Permanent Representative of Costa Rica to the United Nations: "[We] must take immediate and decisive action to prevent and stop cyberattacks that target hospitals, health care, and research organizations"; Costa Rica, Permanent Mission to the United Nations. (26 August 2020)

44 World Health Organization. "WHO Director-General's remarks at Meeting of the UN Security Council on threats posed by ransomware attacks against hospitals and other healthcare facilities and services". 8 November 2024. https://www.who.int/director-general/speeches/detail/who-director-general-s-remarks-at-meeting-of-the-un-security-council-on-threats-posed-by-ransomware-attacks

45 World Health Organization. (2024). *Laboratory Biosecurity Guidance*. https://www.who.int/publications/i/item/9789240095113

Doctor using a tablet (generated with AI). Credit: Adobe Stock / Arterego Studio.

6. Cyberbiosecurity at the National Level

While discussion in multilateral forums may be limited, there is some evidence that States have begun to consider cyberbiosecurity-related issues domestically. The UNIDIR-VERTIC BWC National Implementation Measures Database[46] showed at the time of writing that 20 States among the 187 BWC States Parties have implemented some form of cyberbiosecurity measures. These measures vary and sometimes take the form of broader efforts to secure critical infrastructure.[47] They include protocols for digital access management, drafting users' manuals, or the implementation of remedial activities such as backups for critical information.

To provide some examples, Argentina has established a cybersecurity committee which is in charge of adopting measures to protect critical infrastructure which may apply to laboratories or hospitals.[48] In France, §5.3.3 of the Order of 23 January 2013 regulating good practices for biosafety and biosecurity requires specific data protection measures to avoid the loss or theft of microorganisms and toxins.[49] In Pakistan, Section 8 of the Prevention of Electronic Crimes Act of 2016 prohibits interference with critical infrastructure information system or data (which may include biotechnology-related information systems).[50] In the Russian Federation, art. 14 of Federal Law

---

46 See "cybersecurity" (filters) at https://bwcimplementation.org/

47 Ibid.

48 See Profile of Argentina on the UNIDIR-VERTIC BWC National Implementation Measures Database: https://bwcimplementation.org/states/argentina

49 See Order of 23 January 2013 on "rules of good practice to ensure biological safety and security" referred to in Article R. 5139-18 of the Public Health Code. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000027047902

50 See Act No. XL of 2016 on the "Prevention of Electronic Crimes". https://pakistancode.gov.pk/english/UY2Fqa-Jw1-apaUY2Fqa-apaUY2Jvbp8%3D-sg-jjjjjjjjjjjj

No. 492 on Biological Safety requires the establishment of a State information system in the field of biological safety.[51] And in Türkiye, art. 22 of Regulation No. 32266 on Medical Laboratories of 2024 requires the protection of laboratory information systems against external access and data destruction, notably through secure backups.[52]

These efforts are promising and there could be much to learn from an exchange of good practices in this area. Yet activities appear only to have been undertaken by a small number of States Parties and may require further collaboration globally to reach an understanding on the kinds of measures, good practices, and resources required to protect these systems.

7. Conclusion

Cyberbiosecurity is a critical issue considering the increased digitalization of biological research and development. It can be situated at the intersection of biosafety, biosecurity and cybersecurity. It aims to address the potential ICT threats to these systems at the nexus of the digital and biological domains.

Several measures to mitigate ICT threats to biosecurity and biosafety could be implemented but a first step would be to put this issue on the agenda of relevant multilateral forums. ICT threats to biosafety and biosecurity could indeed become significant threats to international peace and security and thus merit full attention. As of today, limited coverage has been given to cyberbiosecurity issues as they are mostly addressed through the lens of operations affecting healthcare systems, such as ransomware attacks targeting hospitals. One way forward could be to clarify the breadth of the concept of cyberbiosecurity through exchanges with relevant communities, and considering cyberbiosecurity in the context of the ongoing BWC Working Group, notably discussions on scientific and technological developments. This approach could allow for an exchange of views and good practices in the cyber domain and their applicability to biological research and development facilities. Cyberbiosecurity considerations could also find their way into the dedicated multilateral discussions on State use of ICT in the context of international security, this currently being the Open-ended Working Group 2021–2025.

To raise awareness of cyberbiosecurity risks and good practices to address them, States could also make use of a number of confidence-building mechanisms or tools, such as UNIDIR's Cyber Policy Portal[53] and UNIDIR-VERTIC's Biological Weapons Convention National Implementation Measures Database,[54] both of which aim to promote transparency and sharing of good practices in addressing international cybersecurity, and biosafety and biosecurity, respectively.

---

51 See Federal Law No. 492-FZ of 30 December 2020 "On Biological Safety in the Russian Federation" (with amendments and additions). https://base.garant.ru/400156868/888134b28b1397ffae87a0ab1e117954/#friends

52 See Regulation No. 32266 on Medical Laboratories of 2024. https://bwcimplementation.org/sites/default/files/resource/TR_Regulation on Medical Laboratories_EN.pdf

53 www.cyberpolicyportal.org

54 www.bwcimplementation.org

List of References

Arnold, C. (13 June 2022). "Cloud Labs: Where Robots Do the Research". *Nature*. https://www.nature.com/articles/d41586-022-01618-x

Bose, P. (18 March 2024). "How Cloud Labs and Remote Research Shape Science". *The Scientist*. https://www.the-scientist.com/how-cloud-labs-and-remote-research-shape-science-71734

Costa Rica, Permanent Mission to the United Nations. (26 August 2020) "Statement at the Security Council Arria Formula: Cyber Attacks Against Critical Infrastructure". New York.

de la Fuente-Nunez, C. (2022). "Antibiotic Discovery with Machine Learning". *Nature Biotechnology*, 40. https://www.nature.com/articles/s41587-022-01327-w

Crawford, E. et al. (2023). "Cyberbiosecurity in high-containment laboratories". *Frontiers in Bioengineering and Biotechnology*, 11. https://www.frontiersin.org/articles/10.3389/fbioe.2023.1240281/full

European Commission. "The bioeconomy means using renewable biological resources from land and sea, like crops, forests, fish, animals and micro-organisms to produce food, materials and energy". Accessed 18 November 2024. https://research-and-innovation.ec.europa.eu/research-area/environment/bioeconomy_en

European Union Council Decision (CFSP) 2025/529 of 17 March 2025 on Union support for the United Nations Institute for Disarmament Research project 'Science and Technology Watchtower: Monitoring Innovation for Disarmament'. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32025D0529

European Union. (2023). "EU statement (Agenda item 5: Existing and Potential Threats). Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021-2025 06.03-10.03.2023." https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/EU_THREATS.pdf

Fouad, N. S., (2024). "Cyberbiosecurity in the New Normal: Cyberbio Risks, Pre-Emptive Security, and the Global Governance of Bioinformation". *European Journal of International Security*, 9(4). https://doi.org/10.1017/eis.2024.19

France. Order of 23 January 2013 on "rules of good practice to ensure biological safety and security" referred to in Article R. 5139-18 of the Public Health Code. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000027047902

General Assembly. (31 January 2003). "Creation of a global culture of cybersecurity". A/RES/57/239. https://docs.un.org/en/A/RES/57/239

General Assembly. (18 March 2021). "Developments in the field of information and telecommunications in the context of international security". A/75/816. https://docs.un.org/en/A/75/816

General Assembly. (22 July 2024). "Developments in the field of information and telecommunications in the context of international security". A/79/214. https://docs.un.org/en/a/79/214

General Assembly. (14 July 2021). "Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security". A/76/135. https://docs.un.org/en/A/76/135

General Assembly. (3 July 2023). “Our Common Agenda. Policy Brief 9: A New Agenda for Peace”. United Nations. A/77/CRP.1/Add.8. https://digitallibrary.un.org/record/4015374

International Telecommunication Union. (April 2008). “Overview of Cybersecurity”. Recommendation X.1205. https://www.itu.int/rec/T-REC-X.1205-200804-I

International Telecommunication Union. (March 1991). “Security Architecture for Open Systems Interconnection for CCITT Applications”. Recommandation X.800. https://www.itu.int/rec/T-REC-X.800-199103-I

INTERPOL. (4 August 2020). “INTERPOL Report Shows Alarming Rate of Cyberattacks during COVID-19”. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Kaiser, J. (17 March 2023). *Growing Number of High-Security Pathogen Labs around World Raises Concerns. Science.* https://www.science.org/content/article/growing-number-high-security-pathogen-labs-around-world-raises-concerns

D. -J. Kang, J. -J. Lee, S. -J. Kim and J. -H. Park. (2009). “Analysis on cyber threats to SCADA systems”. *2009 Transmission & Distribution Conference & Exposition: Asia and Pacific, Seoul, Korea (South)*. https://ieeexplore.ieee.org/abstract/document/5357008

King’s College London and George Mason University. (2023). *Global BioLabs Report 2023*. https://static1.squarespace.com/static/62fa334a3a6fe8320f5dcf7e/t/6412d3120ee69a4f4efbec1f/1678955285754/KCL0680_BioLabs+Report_Digital.pdf

Li, J. et al. (2022). “Smart Heightened-Containment Biological Laboratory: Technologies, Modules, and Aims”. *Journal of Biosafety and Biosecurity*, 4(2). https://doi.org/10.1016/j.jobb.2022.06.003

Meeting of Experts on Institutional Strengthening of the Convention. (1 September 2021). International research and practical Conference "Global Biosecurity Challenges. Problems and Solutions" (Sochi, 24-25 June 2021)”. Biological and Toxin Weapons Convention. BWC/MSP/2020/MX.5/WP.5. https://documents.un.org/symbol-explorer?s=BWC/MSP/2020/MX.5/WP.5&i=BWC/MSP/2020/MX.5/WP.5_0574157

Mueller, S. (2021). “Facing the 2020 Pandemic: What Does Cyberbiosecurity Want Us to Know to Safeguard the Future?”. *Biosafety and Health*, 3(1). https://www.sciencedirect.com/science/article/pii/S2590053620301129

Ninth Review Conference of the States Parties. (6 December 2022). “International Activities of Global Partnership Member Countries related to Article X of the Biological and Toxin Weapons Convention (2017-2022)”. Biological and Toxin Weapons Convention. BWC/CONF.IV/WP.51. https://documents.un.org/doc/undoc/gen/g22/606/46/pdf/g2260646.pdf

Ninth Review Conference of the States Parties. (29 November 2022). “Support of the European Union and its Member States to Strengthening Biosafety and Biosecurity Globally”. Biological and Toxin Weapons Convention. BWC/CONF.IV/WP.38. https://documents.un.org/symbol-explorer?s=BWC/CONF.IX/WP.38&i=BWC/CONF.IX/WP.38_7328911

Pakistan. Act No. XL of 2016 on the “Prevention of Electronic Crimes”. https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Jvbp8%3D-sg-jjjjjjjjjjjj

Petersen, I., Kollek, R., Brüninghaus, A., Döring, M. (2015). Systems Biology, Information Technology, and Cancer Research. In: *Contextualizing Systems Biology*. Springer. https://doi.org/10.1007/978-3-319-17106-7_4

Puzis, R., Farbiash, D., Brodt, O. et al. (2020). “Increased cyber-biosecurity for DNA synthesis”. *Nature Biotechnology* 38, 1379–1381. https://doi.org/10.1038/s41587-020-00761-y

Radoini A., Siddiqui M. (2021). “The Cyber-Threat Against Chemical, Biological, Radiological and Nuclear (CBRN) Facilities”. *Freedom from Fear Magazine: The past, the present and the future are in our hands* (UNICRI December). https://unicri.it/sites/default/files/2021-12/16_cyber_threat.pdf

Russian Federation. Federal Law No. 492-FZ of 30 December 2020 "On Biological Safety in the Russian Federation" (with amendments and additions). https://base.garant.ru/400156868/888134b28b1397ffae87a0ab1e117954/#friends

Shang, S., Cai, X.S. & Qi, L.S. (2022). “Computation Empowers CRISPR Discovery and Technology”. Nature Computational Science, 2. https://www.nature.com/articles/s43588-022-00321-1

Sun, J.-Y., Hu, H.-B., Cheng, Y.X., Lu, X.-J., (2020). “CRISPR in Medicine: Applications and Challenges”. *Briefings in Functional Genomics*, 19(3). https://academic.oup.com/bfg/article/19/3/151/5838014

Tel Aviv University. ‘Biosafety levels’. Faculty of Medical and Health Sciences. Accessed 6 May 2025. https://en-med.tau.ac.il/safty_biology_biosafety_evel-2020

Titus, A. J., Hamilton, K. E., Holko, M. (2023). ‘Cyber and Information Security in the Bioeconomy’. In: Dov Greenbaum (ed.), *Cyberbiosecurity: A New Field to Deal with Emerging Threats*. Springer. https://doi.org/10.1007/978-3-031-26034-6_3

Türkiye. Regulation No. 32266 on Medical Laboratories of 2024. https://bwcimplementation.org/sites/default/files/resource/TR_Regulation on Medical Laboratories_EN.pdf

UNIDIR. Biological Weapons Convention National Implementation Measures Database. https://bwcimplementation.org/

UNIDIR. Cyber Policy Portal. www.cyberpolicyportal.org

United Nations. (September 2024). *Pact for the Future, Global Digital Compact, and Declaration on Future Generations*. https://www.un.org/sites/un2.un.org/files/sotf-pact_for_the_future_adopted.pdf
United Nations. Summit of the Future (website). Accessed 6 May 2025. https://www.un.org/en/summit-of-the-future

United States of America. (2022). “United States remarks for March 2022 session of the OEWG, as prepared”. https://documents.unoda.org/wp-content/uploads/2022/04/US-remarks-for-March-OEWG-norms.pdf

World Health Organization. (31 July 2020). “Antibiotic Resistance”. https://www.who.int/news-room/fact-sheets/detail/antibiotic-resistance

World Health Organization. (2024). *Laboratory Biosecurity Guidance*. https://www.who.int/publications/i/item/9789240095113

World Health Organization. WHO Director-General's remarks at Meeting of the UN Security Council on threats posed by ransomware attacks against hospitals and other healthcare facilities and services. 8 November 2024. https://www.who.int/director-general/speeches/detail/who-director-general-s-remarks-at-meeting-of-the-un-security-council-on-threats-posed-by-ransomware-attacks

@unidir
/unidir
/un_disarmresearch
/unidirgeneva
/unidir

UNIDIR

Palais des Nations
1211 Geneva, Switzerland

WWW.UNIDIR.ORG