Science and Technology Advancements and Biosecurity: New Horizon

Suryesh K. Namdeo

Consultant, Science and Technology, United Nations Office for Disarmament Affairs, Geneva, and Visiting Scholar, DST Centre for Policy Research, Indian Institute of Science, Bengaluru

Summary

The rapid developments in science and technology are opening new frontlines for policy priorities in biosecurity. Science and technology are also at the central to the Biological Weapons Convention. The present policy and regulatory frameworks, both at national and multilateral levels, are insufficient for managing the changes in science and technology and the concomitant opportunities and challenges they create. Policy institutions should frequently involve scientists having varied expertise to understand and develop policy expositions based on the latest scientific developments and their possible influence. Here, technology foretelling and anticipatory science policy tools could be applied, particularly for the convergence of emerging technologies.

The rapid advancements in science and technology are opening new frontiers for policy priorities in biosecurity. Science and technology are also at the core of the Biological Weapons Convention and find relevance in most of its Articles. From the perspective of biosecurity, the major areas of interest are synthetic biology, genome editing, virology, toxicology, agricultural biology, cyber biosecurity, neuro-technology, and the interface of these areas with other emerging technologies like artificial intelligence (AI). Other major risk areas include regulatory and oversight gaps in the biosafety and biosecurity practices in high containment labs as well as bio-foundries and Do-It-Yourself (DIY) labs. This article explores some of these priorities and concerns and discusses a way forward for evolving biosecurity measures with scientific developments.

Synthetic biology is used to design and create biological systems and products that have the potential to revolutionise the bio-economy by bringing new, cheaper, and more efficient products into the market.[1] Synthesized biomolecules, bio-systems, and microbes are essential for advancing research in biomedical sciences. However, robust oversight mechanisms to ensure that these synthetic biology products are not used for malicious purposes, are generally lacking.[2] Here, two particular areas of concern are the possible misuse of synthetic viruses and synthetic DNA. Synthetic viruses are generally used to study current and emerging viral diseases to understand their molecular mechanisms and develop drugs. However, the gain of function research in these viruses can create more infectious and lethal variants, which, if accidentally or intentionally released, can result in major outbreaks. Labs that work on synthetic

viruses have been relatively few, but their number is growing, and there is a need to establish a repository of details of all research activities involving synthetic viruses.

In contrast, a number of labs use synthetic DNA for molecular biology and genetic engineering experiments. Synthetic DNA can be introduced into microbes to alter their biological activity and function. The malicious application of synthetic DNA can increase the pathogenicity, transmissibility, and infectivity of dangerous microbes. It can also be used to programme microbes to produce certain kinds of toxins .[3] Generally, synthetic biology is used in combination with genome editing technology such as CRISPR-Cas9, which can manipulate genetic material in organisms. In order to prevent the malicious use of synthetic biology, the International Gene Synthesis Consortium (IGSC), an industry body of DNA synthesis companies, has developed protocols to screen DNA sequences as well as the customers who place the order.[4] However, IGSC is constrained, as it does not cover all geographies and all companies that synthesize DNA. A more international effort involving government, industry, and academia is needed to establish a robust oversight mechanism for synthetic DNA.

One of the consequences of the rapid pace of advancements in science and technology is that the essential ingredients for conducting biological research have become cheaper and more accessible than ever before. This has resulted in an increase in the number of institutional research labs along with the proliferation of DIY labs and bio-founderies.[5] The DIY labs and bio-founderies, in particular, have insufficient biosafety and biosecurity measures in place to prevent the accidental release or malicious use of biological agents. There is also a policy gap as these facilities are primarily unregulated in several parts of the world. This lack of oversight and monitoring increases the risks of non-State actors or even State-affiliated actors conducting biological research with malicious intent.

Another major priority area is maintaining high levels of biosecurity in high-containment laboratories working on dangerous pathogens. This is particularly important as several new high, and maximum-containment labs are currently being planned and established worldwide.[6] Currently, the bio-safety and biosecurity standards for these labs vary widely around the world and will require constant updating as new pathogens and risks emerge. In addition to the traditional biological risks, these labs will need to be prepared for new kinds of threats, including cyber-attacks and the possible radicalisation of researchers working in these labs.

Complex synergies are emerging at the interface of different areas of biological sciences, especially synthetic biology and neurobiology on the one hand and developments in artificial intelligence, nanotechnology, cyber technologies, blockchain, and robotics, on the other. These synergies are likely to create huge opportunities for innovations that could boost the bio-economy but, at the same time, can create new risks concerning biological safety and security. For example, the rapid increase in the collection and processing of biological data in labs and hospitals has created risks of cyber-attacks to steal, exploit, manipulate or destroy such data.[7] In fact, several cyber-attacks were recorded in research labs that were in the race to develop vaccines during the first two years of the COVID-19 pandemic, and measures were in place to prevent them.[8] The biological data is inherently personal and can be used for malicious purposes, including blackmailing, extortion, bio-discrimination, and the creation of customized biological weapons.

The integration of digital and biological systems can pose new kinds of risks. For example, cyber-attacks on digital devices linked to the human body could impair biological functions. This risk is especially high with neuro-technology and other human augmentation techniques. Neuroscience and neuro-technology have a long history of interest for possible military applications.[9] In future, neuro-technology could be used for reading, manipulating and destroying memories and thoughts, interrogation, and enhancing combatant performance. At the individual level, malicious applications of neuro-technology can affect privacy and mental integrity. There needs to be more clarity on what aspects of neuroscience and nanotechnology should be considered under the Biological Weapons Convention (BWC).

Similarly, new concerns are emerging from the convergence of AI with synthetic biology, neuro-technology, and agro-biology. For example, AI could be used to help identify and synthesize more dangerous pathogens and toxins. There have been some recent reports of such attempts that heighten such fears.[10] Further, the application of AI in neuro-devices working on a brain-computer interface could be used for surveillance and pose severe risks to mental integrity and privacy. On the other hand, there are several possible benefits of the application of AI. For example, AI could help create epidemiological and medical countermeasures in case of a biosafety or biosecurity incident. Advanced algorithms, including AI, can help with the surveillance of crops to detect and prevent biosecurity incidents using images and data acquired by satellites, drones, or any other means. AI could also be used to discover cyber-vulnerabilities in research labs, hospitals, and offices of regulatory agencies.

Overall, the current policy and regulatory frameworks, both at national and multilateral levels, are inadequate for managing the developments in science and technology and the associated opportunities and challenges they create. Policy institutions should regularly engage with scientists having diverse expertise to understand and develop policy solutions based on the latest scientific developments and their possible impact. Here, technology forecasting and anticipatory science policy tools could be applied, particularly for the convergence of emerging technologies. Scientific advice at different levels of Government should be integrated with security requirements to create robust frameworks for biosecurity. At the time of writing, the Ninth Review Conference of the BWC is deliberating on establishing a science and technology advisory mechanism. While most State Parties of the BWC support establishing such a mechanism, it remains a challenge to build a consensus on the scope, authority, structure, responsibilities, and mode of function that such a mechanism would have. If such a structure comes up, it could act as a significant coordination and resource centre, providing credible technical advice for biosecurity worldwide.

Endnotes:

1 Bio-foundries are integrated infrastructure facilities to enable rapid and efficient design, construction, and testing for bio-manufacturing and engineering biology.

2 Y.F. Bueso, and M. Tangney, "Synthetic biology in the driving seat of the bioeconomy", *Trends in biotechnology*, 35(5), 2017, pp. 373-378.

3 "Biodefense in the age of synthetic biology," National Academies of Sciences, Engineering, and Medicine, Washington DC, 2018.

[4] N.J. Taylor, and S. C. Kesterson, "Pathogens and Toxins of High Consequence: Category A and B Agents and Synthetic Biology: A Practical Guide to Understanding", *Physician Assistant Clinics*, 4(4), 2019, pp. 727-738.

[5] https://genesynthesisconsortium.org/, Accessed on March 11, 2023

[6] https://www.globalbiolabs.org/map, Accessed on March 11, 2023

[7] S. Mueller, "Facing the 2020 pandemic: What does cyber biosecurity want us to know to safeguard the future?" *Biosafety and Health*, 3(1), 2021, pp.11-21.

[8] https://www.f5.com/labs/articles/threat-intelligence/cybersecurity-threats-to-the-covid-19-vaccine

[9] https://thebulletin.org/2017/10/neuroscience-and-the-new-weapons-of-the-mind/

[10] https://www.scientificamerican.com/article/ai-drug-discovery-systems-might-be-repurposed-to-make-chemical-weapons-researchers-warn/ Accessed on March 11, 2023