


RESEARCH ARTICLE

Cyberbiosecurity in the new normal: Cyberbio risks, pre-emptive security, and the global governance of bioinformation

Noran Shafik Fouad 

History, Politics and Philosophy, Manchester Metropolitan University, Manchester, UK
Email: n.fouad@mmu.ac.uk

(Received 27 September 2023; revised 26 March 2024; accepted 3 April 2024)

Abstract

The Covid-19 pandemic saw a surge in cyber attacks targeting pharmaceutical companies and research organisations working on vaccines and treatments for the virus. Such attacks raised concerns around the (in)security of bioinformation (e.g. genomic data, epidemiological data, biomedical data, and health data) and the potential cyberbio risks resulting from stealing, compromising, or exploiting it in hostile cyber operations. This article critically investigates threat discourses around bioinformation as presented in the newly emerging field of ‘cyberbiosecurity’. As introduced by scholarly literature in life sciences, cyberbiosecurity aims to understand and address cyber risks engendered by the digitisation of biology. Such risks include, for example, embedding malware in DNA, corrupting gene-sequencing, manipulating biomedical materials, stealing epidemiological data, or even developing biological weapons and spreading diseases. This article brings the discussion on cyberbiosecurity into the realms of International Relations and Security Studies by problematising the futuristic threat discourses co-producing this burgeoning field and the pre-emptive security measures it advocates, specifically in relation to bioinformation. It analyses how cyberbiosecurity as a concept and field of policy analysis influences the existing securitised governance of bioinformation, the global competition to control it, and the inequalities associated with its ownership and dissemination. As such, the article presents a critical intervention in current debates around the intersection between biological dangers and cyber threats and in the calls for ‘peculiar’ policy measures to defend against cyberbio risks in the ‘new normal’.

Keywords: bioinformation; biological dangers; biosecurity; cyberbiosecurity; cybersecurity; cyber threats; global health

Introduction

Only those who live by the digit may die by the digit.¹

Digital technologies have been contributing significantly to developments and innovations in the life sciences for many years. The increasing use of complex information technology (IT) equipment and software for big data analytics, modelling, simulations, data sharing, and lab automation have allowed many important research and discoveries to materialise.² These include, for example,

¹ Luciano Floridi, *The Fourth Revolution: How the Infosphere Is Reshaping Human Reality* (Oxford: Oxford University Press, 2014), p. 4.

² Alireza Iranbakhsh and Seyyed Hassan Seyyedrezaei, ‘The impact of information technology in biological sciences’, *Procedia Computer Science*, 3 (2011), pp. 913–16.

decoding the human genome, creating organisms with new capabilities through synthetic biology, automating drug development, personalising genetic treatments and preventive therapies, and revolutionising food safety.³ Such convergence between computer science and biological sciences holds promise for the evolution of digital technologies too. For instance, ongoing research projects have demonstrated the possibility of storing digital data in DNA molecules, and hence potentially changing the future of data storage.⁴ These and similar innovations have created strong interests in investing heavily in digitising life sciences by governments, research organisations, and businesses. It is thus no surprise that Steve Jobs, Apple co-founder, once said that he envisioned the biggest innovations of the 21st century to happen at the intersection of biology and technology.⁵

One important implication of the growing dependency on digital technologies in life sciences is the changing perceptions of what constitutes ‘biological danger’, primarily by adding a ‘cyber’ layer to biosecurity risk analyses. Fears of cyber attacks targeting technologies used in biotechnology, bioinformatics, and pharmaceutical and biomedical domains, among other fields, have contributed to the co-production of the newly emerging field and concept of ‘cyberbiosecurity’. As introduced by scholarly literature in life sciences, cyberbiosecurity aims to understand and mitigate cyber risks engendered by the digitisation of biology to safeguard the bioeconomy. It addresses the risks of cyber attacks that may lead to destruction, misuse, or exploitation of information, processes, and materials at the interface of life sciences and digital technologies. Such risks include, for example, embedding malware in DNA, corrupting gene-sequencing, manipulating biomedical materials, stealing epidemiological data, or even developing biological weapons and spreading diseases.⁶

The Covid-19 pandemic has amplified threat discourses around cyberbiosecurity and the growing belief that *cyber* and *bio* risks are becoming essentially intertwined. In addition to the exponential rise of cyber operations against hospitals, health-care providers, and pandemic response agencies,⁷ cyber espionage campaigns targeting pharmaceutical companies and research organisations working on vaccines and treatments for Covid-19 have raised profound concerns about the (in)security of digitised bioinformation (e.g. genomic data, epidemiological data, biomedical data, and health data). Nation-state actors, particularly China, Russia, North Korea, and Iran, have been at the forefront of such cyber espionage accusations. Attacks reportedly targeted health-care entities, pharmaceutical companies, and researchers in multiple countries, including the USA, the UK, Canada, France, India, and South Korea.⁸ Even though none of these cyber incidents were deemed crippling to vaccine development or had detrimental repercussions on the pandemic, they demonstrated the strategic value of bioinformation; the potential damaging implications of stealing, compromising, or exploiting it in hostile cyber operations; and the complex link between geopolitical competitions, cybersecurity, and global health.

Yet, despite the growing attention to cyberbiosecurity in various academic and policy circles, there remains limited discussion and understanding of this new concept/field in International Relations (IR) and Security Studies.⁹ This article argues that cyberbiosecurity is not merely a technical challenge of securing technologies and their application in life sciences; it is

³Tuan D. Pham, Hong Yan, Muhammad W. Ashraf, and Folke Sjöberg, *Advances in Artificial Intelligence, Computation, and Data Science: For Medicine and Life Science* (Cham: Springer Nature, 2021).

⁴For more information on DNA data storage, see Microsoft, ‘DNA storage’, Microsoft Research, available at: {<https://www.microsoft.com/en-us/research/project/dna-storage/>}.

⁵Walter Isaacson, *Steve Jobs* (New York: Simon and Schuster, 2011), p. 539.

⁶Randall S. Murch, William K. So, Wallace G. Buchholz, Sanjay Raman, and Jean Peccoud, ‘Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy’, *Frontiers in Bioengineering and Biotechnology*, 6 (2018), doi: [10.3389/fbioe.2018.00039](https://doi.org/10.3389/fbioe.2018.00039).

⁷Zachary Cohen, Luke McGee, and Alex Marquardt, ‘UK, US and Canada allege Russian cyberattacks on Covid-19 research centers’, *CNN* (17 July 2020), available at: {<https://www.cnn.com/2020/07/16/politics/russia-cyberattack-covid-vaccine-research/index.html>}.

⁸Tom Burt, ‘Cyberattacks targeting health care must stop’, *Microsoft* (blog) (13 November 2020), available at: {<https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/>}.

⁹Thom Dixon, ‘The grey zone of cyber-biological security’, *International Affairs*, 97:3 (2021), pp. 685–702; Thom Andrew Dixon, ‘The bioinformational dilemma: Where bioinformational diplomacy meets cyberbiosecurity’, *Australian Journal of*

fundamentally also a political issue that is deeply entangled with the global politics of both cybersecurity and biosecurity. Accordingly, the article brings the discussion on cyberbiosecurity into the realms of IR and Security Studies by problematising the futuristic threat discourses co-producing this burgeoning field of cyberbiosecurity and the pre-emptive security measures it advocates. The article focuses specifically on bioinformation, which lies at the heart of threat discourses in cyberbiosecurity, and analyses how such discourses influence the existing securitised governance of bioinformation, the global competition to control it, and the inequalities associated with its ownership and dissemination.

In doing so, the article presents a critical intervention in current debates around the intersection between biological dangers and cyber threats by interrogating arguments on the peculiarity of cyberbiosecurity and unpacking their implications for security practices. It argues that futuristic scenarios integral to threat perceptions in this new field, and their Western-centric and state-centric preoccupation, overlook complex security contexts in the present, primarily engendered by geopolitical competitions and inequalities in global health. Further, the article shows how the prioritisation of high-profile threats with potential physical consequences, and the pre-emptive security measures proposed by cyberbiosecurity to address them, can have major adverse implications for the governance of both cybersecurity and biosecurity. Ultimately, the article calls for a global and scientific-led approach to securing bioinformation as a global common good rather than a national strategic resource, which ensures human privacy is protected, which does not hinder equity and fairness in sharing bioinformation, and which benefits global health rather than being solely driven by superpower competitions.

This critical approach to the study of cyberbiosecurity is advanced in three sections. The first section introduces the new concept/field of cyberbiosecurity and examines how it is being co-produced as pre-emptive security, in light of accelerating trends in digitising biology and the Covid-19 pandemic. The second section moves to an analysis of the key security modalities in discourses on cyberbio risks. Drawing comparisons with the securitisation of cybersecurity and its implications for militarising cyberspace, the article challenges cyberbiosecurity's preoccupation with *futuristic* scenarios of high-profile threats with potential *physical* consequences. In the third section, the article investigates the implications of securitising bioinformation and the pre-emptive security measures proposed by cyberbiosecurity for the complex geopolitical considerations that presently govern bioinformation. It argues that any cyberbiosecurity intervention should be integrated into current debates engendered by digitising bioinformation, particularly in regards to issues of global equity and fairness and superpower competitions over technology dominance.

The cyberbio nexus

Even though cyberbiosecurity is a relatively new area of research and policy analysis, the epistemic links between computer science and biology far precede the inception of this field. At its core, biology is sometimes conceptualised as an information science, in which information is embedded in genetic codes. Hence, language rooted in information and computer sciences is used in abundance in studying biological and natural phenomena. For instance, 'codes', 'transcriptions', and 'translations' are all terms used to describe how genes carry encoded information that is later converted into RNA, and eventually to protein. In molecular and cellular biology research too, it is common for concepts such as 'signal' and 'network' to be used extensively.¹⁰ Likewise, since the 1950s, and the advancements in computing technologies, language borrowed from biology has been contributing substantially to our digital culture, such as referring to computer's Central Processing Unit (CPU) as its 'brain'; conceptualising system networks as 'environments'; and approaching safety

International Affairs, 77:2 (2023), pp. 169–87; Rebecca J. Hester, 'Bioveillance: A techno-security infrastructure to preempt the dangers of informationalised biology', *Science as Culture*, 29:1 (2020), pp. 153–76.

¹⁰Barton Moffatt, 'The philosophy of biological information', in Luciano Floridi (ed.), *The Routledge Handbook of Philosophy of Information* (Abingdon: Routledge, 2016), pp. 277–89.

and security practices in cyberspace as digital ‘hygiene’.¹¹ Many computer science models were also inspired by biological models, including evolutionary programming and mutating polymorphic code, among others.¹²

Specifically, in cybersecurity, metaphoric connections with biology, seen in concepts such as ‘viruses’ and ‘worms’, have become inherent to the conceptualisation of cyber threats since the 1990s, portraying such threats as a form of ‘artificial life’. For example, references to HIV/AIDS in the 1980s constituted an essential political tool to ban certain computing activities that were deemed damaging, such as black-hat hacking.¹³ However, this ‘biologisation of technology’ has been a subject of debate in cybersecurity research,¹⁴ questioning whether it is an accurate representation of the peculiarities of technologies.¹⁵ Similar debates also surround the use of informational language in biological sciences and conceptualising ‘life as code’.¹⁶ Importantly, it is not clear how this epistemic connection has changed or influenced the production of knowledge in both fields.

Digitising biology and the rise of cyberbiosecurity

The epistemic link between computer science and biological sciences has been taking a more ‘material’ turn through intensive digitisation processes throughout the last decade. In health care, for example, patient portals, medical management software, digital assistive technologies, and care robots are transforming and facilitating the operations of hospitals, together with advancements in personalised genetic treatments and preventive therapies.¹⁷ Even more, big data is now used in predicting disease outbreaks and bioterrorist attacks as part of what global health literature refers to as ‘syndromic surveillance’, which played a key role in detecting the Covid-19 pandemic and declaring it as a global health emergency.¹⁸ Added to this, life sciences labs are becoming increasingly automated through robotics and artificial intelligence (AI), enabling scientists to conduct sophisticated, time-consuming experiments more efficiently.¹⁹ Agriculture is another field that is being transformed by digital technologies, through farm machinery automation, remote satellite data for monitoring crops, etc.²⁰ Perhaps one field that technology has a profound impact on is synthetic biology, which relies heavily on bioinformatics and digital tools for designing new molecules, genetic circuits, and commodities, such as fuels, renewable materials, and food.²¹

Nonetheless, there are various ethical dilemmas and security risks associated with such digitisation processes that have been transforming conventional thinking on biosecurity and biological danger. For example, there are fears that biotechnology and gene editing can be used to enhance existing pathogens, or create new ones, to be used as biological weapons.²² Cybersecurity too

¹¹David J. Betz and Tim Stevens, ‘Analogical reasoning and cyber security’, *Security Dialogue*, 44:2 (2013), pp. 147–64.

¹²Myriam Dunn Cavely, ‘From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse’, *International Studies Review*, 15:1 (2013), pp. 105–22.

¹³Jussi Parikka, *Digital Contagions: A Media Archaeology of Computer Viruses* (New York: Peter Lang, 2007).

¹⁴Dunn Cavely, ‘From cyber-bombs to political fallout’.

¹⁵Betz and Stevens, ‘Analogical reasoning and cyber security’.

¹⁶Hester, ‘Bioveillance’.

¹⁷Marc Mitchell and Lena Kan, ‘Digital technology and the future of health systems’, *Health Systems & Reform*, 5:2 (2019), pp. 113–20.

¹⁸Christopher Long, ‘Securitising infectious disease outbreaks: The WHO and the visualisation of molecular life’, *European Journal of International Security*, 17 (2023), pp. 1–20; Stephen L. Roberts and Stefan Elbe, ‘Catching the flu: Syndromic surveillance, algorithmic governmentality and global health security’, *Security Dialogue*, 48:1 (2017), pp. 46–62.

¹⁹Ian Holland and Jamie A. Davies, ‘Automation in the life science research laboratory’, *Frontiers in Bioengineering and Biotechnology*, 8 (2020), p. 571777.

²⁰Jonathan McFadden, Francesca Casalini, Terry Griffin, and Jesús Antón, ‘The digitalisation of agriculture: A literature review and emerging policy issues’, OECD, Paris (2022), available at: <https://doi.org/10.1787/285cc27d-en>.

²¹Christopher A. Voigt, ‘Synthetic biology 2020–2030: Six commercially-available products that are changing our world’, *Nature Communications*, 11:1 (2020), p. 6379.

²²Kate Charlet, ‘The new killer pathogens: Countering the coming bioweapons threat the gene-editing revolution’, *Foreign Affairs*, 97:3 (2018), pp. 178–85; Marko Ahteensuu, ‘Synthetic biology, genome editing, and the risk of bioterrorism’, *Science and Engineering Ethics*, 23:6 (2017), pp. 1541–61.

has begun to take up considerable space in thinking about digital biosecurity. In recent years, the health-care sector has been subject to sophisticated cyber operations that compromised medical and patients' data, caused massive financial losses, and disrupted critical operations.²³ Consequently, health care has risen to the top of cybersecurity agendas, particularly in relation to national security threats to Critical National Infrastructures (CNIs), with fears that cyber attacks targeting this sector may lead to potential loss of life.

Further, concerns about cyber attacks affecting biological laboratories and biomanufacturing have also started to grow in recent years. One important case in this regard, which played a foundational role in the development of discourses around cyberbiosecurity, was the NotPetya ransomware which affected pharmaceutical giant Merck & Co. in 2017, causing an estimated loss of \$670 million. Although NotPetya was a self-propagating malicious software (malware) that spread itself automatically, and hence did not specifically target Merck, it resulted in major disruptions to the company's manufacturing processes, leading to temporarily shut down to essential operations and shortages in the Gardasil vaccine, used to target cancers and other diseases caused by the human papillomavirus.²⁴ This incident showed how cyber attacks in the future, particularly if they are designed to target biomanufacturing activities, may impact important vaccines and medicines, potentially damaging equipment, stealing intellectual property, or risking lives.²⁵

These threat perceptions have contributed to wider discussions on the link between cybersecurity and the entity of life per se, exemplified in the co-production of the new field and concept of cyberbiosecurity. Cyberbiosecurity, also referred to as biocybersecurity, is an emerging field that combines expertise and scholarship from multiple disciplines to study the security vulnerabilities and complex ecosystem at the intersection of life sciences, information systems, biosecurity, and cybersecurity.²⁶ Such vulnerabilities, as argued by the proponents of this field, cannot be addressed by any single sector alone.²⁷ Hence, if biosecurity pertains to measures that prevent the introduction and spread of pathogens and harmful organisms that can cause infectious diseases, cyberbiosecurity, on the other hand, reconceptualises such threats and narrows them down to those resulting from the integration of animate (biological) and inanimate (cyber) substrates, which are both inherently *informational* systems.²⁸

The roots of cyberbiosecurity go back to 2014, when discussions on securing the biolabs of the future started to grow in academic circles. In 2017, the US Department of Defense (DoD) funded a project conducted by the University of Nebraska on cyberbiosecurity as a 'new field in biomanufacturing'.²⁹ This was followed by a workshop organised by academics involved in the project, which was also attended by eight US government agencies, to roll out the concept of

²³Lynne Coventry and Dawn Branley, 'Cybersecurity in healthcare: A narrative review of trends, threats and ways forward', *Maturitas*, 113 (2018), pp. 48–52.

²⁴Kim S. Nash, Sara Castellanos, and Adam Janofsky, 'One Year After NotPetya Cyberattack, Firms Wrestle with Recovery Costs', *Wall Street Journal Pro Cybersecurity* (27 June 2018), available at: <https://www.wsj.com/articles/one-year-after-notpetya-companies-still-wrestle-with-financial-impacts-1530095906>.

²⁵J. Craig Reed and Nicolas Dunaway, 'Cyberbiosecurity implications for the laboratory of the future', *Frontiers in Bioengineering and Biotechnology*, 7 (2019), available at: <https://doi.org/10.3389/fbioe.2019.00182>; Elizabeth Crawford, Adam Bobrow, Landy Sun et al., 'Cyberbiosecurity in high-containment laboratories', *Frontiers in Bioengineering and Biotechnology*, 11 (2023), available at: <https://doi.org/10.3389/fbioe.2023.1240281>.

²⁶Alexander J. Titus, Kathryn E. Hamilton, and Michelle Holko, 'Cyber and information security in the bioeconomy', in Dov Greenbaum (ed.), *Cyberbiosecurity: A New Field to Deal with Emerging Threats* (Cham: Springer International Publishing, 2023), pp. 17–36.

²⁷Murch et al., 'Cyberbiosecurity'; Lauren C. Richardson, Nancy D. Connell, Stephen M. Lewis, Eleonore Pauwels, and Randy S. Murch, 'Cyberbiosecurity: A call for cooperation in a new threat landscape', *Frontiers in Bioengineering and Biotechnology*, 7 (2019), available at: <https://doi.org/10.3389/fbioe.2019.00099> (p. 99).

²⁸Dixon, 'The grey zone of cyber-biological security', p. 686.

²⁹University of Nebraska–Lincoln, 'BPDF researchers part of team working on cyberbiosecurity issues for Defense Dept.' (9 February 2017), available at: <https://engineering.unl.edu/bpdf-researchers-part-team-working-cyberbiosecurity-issues-defense-dept/>.

cyberbiosecurity.³⁰ The term was eventually formally coined in two biotechnology articles in 2017³¹ and in 2018.³² Since then, academic publications in the field have been growing rapidly, not only in the USA, but also in the UK, Italy, Israel, China, Australia, and Nigeria.³³ Beyond academia, the discussion around cyberbio risks has been gaining prominence in policy circles and governments too. For example, in its annual report entitled ‘Cybersecurity Research and Innovation Needs and Priorities’, the European Union Agency for Cybersecurity (ENISA) identified cyberbiosecurity as an ‘urgent’ issue that ‘may have implications for life itself’.³⁴ Similarly, in a message to the G7-led Global Partnership against the Spread of Weapons and Materials of Mass Destruction, the German presidency announced plans to introduce the concept of cyberbiosecurity in the parts of the partnership concerned with biosecurity and biosafety.³⁵

In the USA, where most of the discussions on cyberbiosecurity are taking place, the Bipartisan Commission on Biodefense, an organisation of former high-ranking government officials, convened a study panel entitled ‘Cyberbio Convergence: Characterizing the Multiplicative Threat’, in which various academic, industry, and policy experts shared their insights on the challenges and peculiarities of cyberbiosecurity.³⁶ Additionally, a series of workshops on cyberbiosecurity for food and agriculture, hosted by Virginia Tech and co-funded by the National Institute for Food and Agriculture, were attended by Federal Bureau of Investigation (FBI) experts from the Weapons of Mass Destruction Directorate.³⁷ More recently, the US National Cybersecurity Center of Excellence and the National Institute of Standards and Technology has launched a new project entitled ‘Cybersecurity of Genomic Data’ that studies the peculiar cyber risks facing genomic data.³⁸

The ‘cyber’ pandemic moment

In addition to being a global health emergency, the pandemic has also been a serious cybersecurity challenge affecting all sectors. The growing reliance on digital technologies as a solution to track and curb the spread of the virus, to provide health-care services, and to establish the foundation of work and life in the ‘new normal’ has increased the number of cyber attack targets, among which the health-care sector was particularly vulnerable.³⁹ During the peak of the pandemic, there were multiple reports on growing cyber attacks against hospitals, health-care providers, and pandemic response institutions.⁴⁰ Security reports show that 66 per cent of health-care organisations

³⁰Randall Murch, ‘Introduction: Origin and intent for the new field of cyberbiosecurity’, in Dov Greenbaum (ed.), *Cyberbiosecurity: A New Field to Deal with Emerging Threats* (Cham: Springer International Publishing, 2023), pp. 7–15.

³¹Jean Peccoud, Jenna E. Gallegos, Randall Murch, Wallace G. Buchholz, and Sanjay Raman, ‘Cyberbiosecurity: From naive trust to risk awareness’, *Trends in Biotechnology*, 36:1 (2017), pp. 4–7.

³²Murch et al., ‘Cyberbiosecurity’.

³³Lucas Potter and Xavier-Lewis Palmer, ‘Mission-aware differences in cyberbiosecurity and biocybersecurity policies: Prevention, detection, and elimination’, in Dov Greenbaum (ed.), *Cyberbiosecurity: A New Field to Deal with Emerging Threats* (Cham: Springer International Publishing, 2023), pp. 37–69.

³⁴European Union Agency for Cybersecurity, ‘Annual report on cybersecurity research and innovation needs and priorities’, Report/Study (12 May 2022), available at: <https://www.enisa.europa.eu/publications/research-and-innovation-brief>}.

³⁵‘Message from the German Presidency’, Global Partnership against the Spread of Weapons and Materials of Mass Destruction (2022), available at: <https://www.gpwm.com/message-from-germany-incoming-gp-president>}.

³⁶Bipartisan Commission on Biodefense, ‘Cyberbio convergence: Characterizing the multiplicative threat – Bipartisan Commission on Biodefense’, (2019), available at: <https://biodefensecommission.org/events/cyberbio-convergence-characterizing-the-multiplicative-threat/>}.

³⁷Virginia Tech, ‘Virginia Tech hosting food and agricultural cyberbiosecurity workshop’, (16 September 2020), available at: https://news.vt.edu/content/news_vt_edu/en/articles/2020/09/cals-cyberbiosecurityworkshop.html}.

³⁸National Cybersecurity Center of Excellence (NIST), ‘Cybersecurity of genomic data | NCCoE’, available at: <https://www.nccoe.nist.gov/projects/cybersecurity-genomic-data>}.

³⁹Menaka Muthuppalaniappan LLB and Kerrie Stevenson, ‘Healthcare cyber-attacks and the Covid-19 pandemic: An urgent threat to global health’, *International Journal for Quality in Health Care*, 33:1 (2021), available at <https://doi.org/10.1093/intqhc/mzaa117>}.
⁴⁰Cohen, McGee, and Marquardt, ‘UK, US and Canada allege Russian cyberattacks on Covid-19 research centers’.

in 31 countries were hit by ransomware attacks in 2021, up from 34 per cent in 2020.⁴¹ According to Microsoft, hackers targeted attacks against Paris's hospital system, Brno University Hospital in the Czech Republic, medical clinics in Texas in the USA, hospitals in Thailand, and computer systems of Spain's hospitals, among others.⁴²

The race to develop vaccines has also sparked cyber espionage operations against research institutions and companies working on vaccines and treatments. In many such incidents, Western powers and media directed accusations towards Russia, China, North Korea, and Iran. For example, in July 2020, an advisory report issued by the UK's National Cyber Security Centre (NCSC), in agreement with security agencies in Canada and the USA, accused APT29 (also known as 'Dukes' or 'Cozy Bear'), a group widely believed to be linked to Russian intelligence, of targeting various organisations involved in Covid-19 research in the three countries to steal information and intellectual property.⁴³ In October 2021, news reports suggested that security services in the UK informed ministers that Russian hackers stole the blueprint for the Oxford/AstraZeneca coronavirus vaccine, which they allege was used by Russia in creating the Sputnik V jab.⁴⁴ The US FBI too issued separate warnings about Chinese hackers attempting to steal pandemic-related data from universities, following data breaches targeting the University of North Carolina.⁴⁵ Other universities that were reportedly targeted were the University of Oxford and Imperial College London in the UK,⁴⁶ as well as the University of Tuebingen in Germany.⁴⁷

Such espionage campaigns extended to private-sector companies too. In 2020, Microsoft announced that it had detected cyber attacks from three nation-state actors that were aimed at seven leading companies working on vaccines and treatments for Covid-19 in Canada, France, India, South Korea, and the USA.⁴⁸ There were reports that hackers with ties to Iran hacked into US drugmaker Gilead Sciences, working on antiviral treatment, using a variety of tools, including phishing emails.⁴⁹ Similarly, news reports suggested that hackers affiliated to North Korea attempted to hack nine health organisations working on the vaccine, among which were Novax and Johnson & Johnson in 2020.⁵⁰ US officials have also accused Chinese government-linked hackers of targeting biotech company Moderna Inc., a US-based coronavirus vaccine research developer.⁵¹ As a result, together with the Department of Homeland Security, the FBI sent security teams to work with biotechnology companies to help them secure their systems.⁵²

⁴¹Sophos, 'The State of Ransomware in Healthcare 2022' (May 2022), available at: <https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrcctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf>.

⁴²Burt, 'Cyberattacks targeting health care must stop'.

⁴³Julian E. Barnes and Michael Venutolo-Mantovani, 'Race for coronavirus vaccine pits spy against spy', *The New York Times* (5 September 2020), available at: <https://www.nytimes.com/2020/09/05/us/politics/coronavirus-vaccine-espionage.html>.

⁴⁴Chiara Giordano, 'Russian spy "stole Astrazeneca vaccine blueprint and used it to develop Sputnik jab"', *The Independent* (11 October 2021), available at: <https://www.independent.co.uk/news/world/europe/russia-astrazeneca-vaccine-blueprint-sputnik-b1935992.html>.

⁴⁵Barnes and Venutolo-Mantovani, 'Race for coronavirus vaccine pits spy against spy'.

⁴⁶Dan Sabbagh and Andrew Roth, 'Russian state-sponsored hackers target Covid-19 vaccine researchers', *The Guardian* (16 July 2020), available at: <https://www.theguardian.com/world/2020/jul/16/russian-state-sponsored-hackers-target-covid-19-vaccine-researchers>.

⁴⁷Raphael Satter and Jack Stubbs, 'North Korea-linked hackers targeted J&J, Novavax in hunt for COVID research', *Reuters* (2 December 2020), available at: <https://www.reuters.com/article/us-health-coronavirus-north-korea-cyber-idUSKBN28C1UE>.

⁴⁸Burt, 'Cyberattacks targeting health care must stop'.

⁴⁹Sergei Klebnikov, 'Gilead Sciences targeted by hackers linked to Iran', *Forbes* (2020), available at: <https://www.forbes.com/sites/sergeiklebnikov/2020/05/08/gilead-sciences-targeted-by-iranian-linked-hackers-report/>.

⁵⁰Satter and Stubbs, 'North Korea-linked hackers targeted J&J, Novavax in hunt for COVID research'.

⁵¹Christopher Bing and Marisa Taylor, 'Exclusive: China-backed hackers "targeted Covid-19 vaccine firm Moderna"', *Reuters* (30 July 2020), sec. Healthcare & Pharma, available at: <https://www.reuters.com/article/us-health-coronavirus-moderna-cyber-excl-idUSKCN24V38M>.

⁵²Barnes and Venutolo-Mantovani, 'Race for coronavirus vaccine pits spy against spy'.

Although none of these attacks proved detrimental to the management of the pandemic or to vaccine and drug development, they showcased the strategic significance of bioinformation, be it epidemiological data, genetic data, biomedical data, or health data, and the risks of targeting it by hostile cyber operations during a global health emergency. Further, these cyber operations targeting pharmaceutical companies and research institutes working on vaccines proved that ‘cyber’ and ‘bio’ risks are becoming increasingly intertwined, and that the links between geopolitical competitions, cybersecurity, and global health are growing more complex. This has, in turn, reinforced discourses around cyberbiosecurity, and the need to identify and address digitally induced vulnerabilities in the life sciences to prevent and mitigate any potential cyber attack in the future.⁵³

Discourses on cyberbio risks

The co-production of the new field and concept of cyberbiosecurity is advancing through diverse discourses, which have major implications on the governance of both cybersecurity and biosecurity. Such discourses share three key security modalities: (1) presenting cyberbiosecurity as a *peculiar* field, distinct from cybersecurity or biosecurity; (2) constructing threats through *futuristic* scenarios, with no past legitimating reference; and (3) centring high-profile threats with potential *physical* consequences.

As a burgeoning concept and field, cyberbiosecurity is more than a statement on the importance of cybersecurity for biological sciences and industries or its challenges and complexities. Rather, cyberbiosecurity is inherently a peculiarity and novelty thesis. As argued in life sciences literature, cyberbiosecurity represents ‘a unique problem set’,⁵⁴ posing ‘new security problems’, which go beyond ‘traditional cyber attacks’,⁵⁵ and thus requires ‘its own systematics’.⁵⁶ There are many reasons put forward by scholars and policymakers to justify the need for a new concept/field to study cyberbio risks. The most important is the current lack of awareness in biosciences about the impact of cyber attacks, the dearth of common language or topology to classify them, absence of adequate training to deal with their complexities, and their potential fatal consequences if they materialise. It follows that generic cyber and information security measures applied in other sectors are deemed insufficient even if they were optimised to deal with vulnerabilities in life sciences. As argued by Mueller, on one side, biotechnology sectors are still trapped in conceptualising security exclusively in terms of biosecurity and biosafety, and on the other, cybersecurity experts do not understand biotechnology.⁵⁷

Diverse risks are presented by the cyberbiosecurity literature as immanent unless preventive security measures are implemented. These risks can be divided into five main categories. The first are commercial losses due to intellectual property (IP) theft against cutting-edge biological therapies, vaccines, precision medicines, and research in general. For example, there were allegations that hackers with ties to the Chinese government hacked into Roche and Bayer pharmaceuticals in 2019 for IP theft.⁵⁸ Second, there is the risk of huge financial losses resulting from ransomware attacks or disruption of critical operations. Examples include the NotPetya ransomware which

⁵³ Aaron Adler, Jake Beal, Mary Lancaster, and Daniel Wyschogrod, ‘Cyberbiosecurity and public health in the age of COVID-19’, in Benjamin D. Trump, Marie-Valentine Florin, Edward Perkins, and Igor Linkov (eds), *Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues*, NATO Science for Peace and Security Series C: Environmental Security (Dordrecht: Springer Netherlands, 2021), pp. 103–15; Siguna Mueller, ‘Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future?’, *Biosafety and Health*, 3:1 (2021), pp. 11–21.

⁵⁴ Daniel S. Schabacker, Leslie-Anne Levy, Nate J. Evans, Jennifer M. Fowler, and Ellen A. Dickey, ‘Assessing cyberbiosecurity vulnerabilities and infrastructure resilience’, *Frontiers in Bioengineering and Biotechnology* 7 (29 March 2019), available at: <https://www.frontiersin.org/articles/10.3389/fbioe.2019.00061>).

⁵⁵ Mueller, ‘Facing the 2020 pandemic’.

⁵⁶ Murch et al., ‘Cyberbiosecurity’.

⁵⁷ Mueller, ‘Facing the 2020 pandemic’.

⁵⁸ European Pharmaceutical Review, ‘Roche confirms cyber-attack from Winnti malware’, *European Pharmaceutical Review* (blog) (25 July 2019), available at: <https://www.europeanpharmaceuticalreview.com/news/95107/roche-confirms-cyber-attack-from-winnti-malware/>).

affected Merck & Co., as discussed earlier. Third is the risk of breach of privacy as a result of intentional or accidental release of patients' personal data. Here, the health-care sector is the most prominent, with an increase of 53.3% in the cost of data breaches since 2020, making it the industry with the most expensive data breaches, costing on average \$10.93 million.⁵⁹

However, at the core of cyberbiosecurity discourses are two separate categories of threats that accentuate life per se as primary referent object. Arguably, the three categories mentioned earlier – IP theft, privacy breaches, and financial losses – are not specific to life sciences; they affect all other sectors of society. It follows that such threats do not necessarily qualify as cyber 'bio' as such, i.e. they are not biological in nature and do not necessarily have any direct impact on life as an entity or a referent object. Cyber threats are considered simultaneously biological if, for example, they manipulate biomedical materials; corrupt gene-sequencing and genome-editing technologies; disrupt diagnostic processes or pathogen tracking; steal or distort epidemiological data; or compromise the quality of therapies or delay the production of drugs in a way that spreads diseases, causes death, or enables the development of biological weapons.⁶⁰ Many scholars argue that digitisation, lab automation, and the online accessibility of bioinformation widen the scope of threat actors who no longer need physical access to labs, samples, or to even have advanced knowledge of biological processes to perform such malicious attacks.⁶¹

Added to this is a fifth category of envisioned threats, which also lie at the heart of cyberbiosecurity discourses, in which the 'biological' and the 'cyber' are integrated in the attack tools. For example, computers are now integral to reading, analysing, and processing DNA at scale, which is used in several fields, such as genomics, medicine, and consumer testing, among others. DNA itself can now be artificially synthesised, without having natural origins. The risk analysed by proponents of cyberbiosecurity here is that malicious information or malware can be embedded in synthetic DNA, making the DNA a 'malicious information carrier' per se. This can give an attacker full control of DNA sequencing equipment and lead to 'catastrophic' data breaches.⁶² In such case, cyber attacks are qualified as simultaneously 'biological' because they are launched from biological substrates, such as DNA.

That is, cyberbiosecurity takes existing discourses that prioritise cybersecurity of CNIs a step further, by arguing that cyberbio risks represent a separate category of threats, distinct from any other sector, with even more destructive consequences.⁶³ Even when acknowledging that some risks are not exclusive to cyberbiosecurity, such as data theft, the assumption is that the consequences would be more significant if directed against biological systems.⁶⁴ This peculiarity, in part, is pitched as a basis for securing funding for cyberbiosecurity research projects. Some proponents of cyberbiosecurity argue that the greatest threat to cyberbiosecurity 'is not a nation-scale enemy at parity, internal political factions, or internecine strife. It is money.'⁶⁵ They further compare the insufficient funding for nuclear security in the past to cyberbiosecurity as a new field, arguing that cyberbiosecurity threats 'are far more insidious and may have a higher likelihood of occurring

⁵⁹IBM Security, 'Cost of a data breach report' (2023), available at: https://www.ibm.com/reports/data-breach?utm_content=SRCWW&p1=Search&p4=43700075239448391&p5=p&gclid=CjwKCAjw8symBhAqEiwAaTA_GUGrx15AETYUWlyWTIVtICTNt5adIU6FwE7QJNjuD2_5WB12-j6KR0cMakQAvD_BwE&gclid=aw.ds.

⁶⁰Mueller, 'Facing the 2020 pandemic'.

⁶¹Schabacker et al., 'Assessing cyberbiosecurity vulnerabilities and infrastructure resilience'.

⁶²Peter Ney, Arkaprabha Bhattacharya, Luis Ceze, Karl Koscher, Tadayoshi Kohno, and Jeff Nivala, 'Cybersecurity across the DNA—digital boundary: DNA samples to genomic data', in Dov Greenbaum (ed.), *Cyberbiosecurity: A New Field to Deal with Emerging Threats* (Cham: Springer International Publishing, 2023), pp. 95–114.

⁶³Diane DiEuliis, 'Revisiting the digital biosecurity landscape', in Dov Greenbaum (ed.), *Cyberbiosecurity: A New Field to Deal with Emerging Threats* (Cham: Springer International Publishing, 2023), pp. 71–8.

⁶⁴Eric Ni, Gamze Gürsoy, and Mark Gerstein, 'Security vulnerabilities and countermeasures for the biomedical data life cycle', in Dov Greenbaum (ed.), *Cyberbiosecurity: A New Field to Deal with Emerging Threats* (Cham: Springer International Publishing, 2023), pp. 79–93.

⁶⁵Potter and Palmer, 'Mission-aware differences in cyberbiosecurity and biocybersecurity policies', p. 45.

than nuclear threats.⁶⁶ According to this argument, risks are mainly linked to state actors, or as one study calls them, ‘rogue states’, which can fund advanced persistent threats (APTs) and can conduct sophisticated cyberbio attacks resulting in damaging consequences.⁶⁷

Further, cyberbiosecurity discourses operate according to futuristic threat constructions and hypothetical scenarios of cyberbio danger that have not actually materialised. The security measures they advocate are, therefore, primarily pre-emptive. As put by Randall Murch, one of the key contributors to the field, the main difference between biosecurity and cyberbiosecurity is that the former focuses on ‘current and emerging threats’ whereas the latter is ‘an alternative philosophy or approach’ aiming to understand *potential* cyberthreats and to devise defensive and resilience strategies accordingly.⁶⁸ This in itself contributes to claims of peculiarity. As argued by Anderson in his discussion of pre-emptive security, ‘the future is the realm of troubling and unforeseen novelty’.⁶⁹

To make up for this absence of past legitimisers, some examples of previous lower-scale cyber attacks against pharmaceutical companies or hospitals are used to establish an argument on the vulnerability of such sectors and the potential for such attacks to escalate. Besides, some studies rely on recent scientific experiments that demonstrate the feasibility of cyberbio attacks and the credibility of the arguably damaging consequences. A very widely cited example in this regard is an experiment conducted in 2017 in which scientists at the University of Washington inserted malware in DNA strands and then took over the computer system that was used in analysing the DNA.⁷⁰ Another example is a study that demonstrated the possibility of acquiring information leaked from a DNA synthesiser via acoustic side-channels, through the use of microphones placed in close proximity to the synthesiser, which the study called the ‘Oligo-snoop’ attack.⁷¹

Against this background, this article brings conversations on cyberbiosecurity into the fields of IR and Critical Security Studies (CSS) by problematising three aspects in the above-mentioned discourses on cyberbiosecurity. First, the article interrogates arguments on the *peculiarity of cyberbiosecurity*, not to disprove them, but rather to unpack what they do to security practices. Second, it questions the futuristic threat scenarios integral to threat perceptions in this field and how they mask complex security contexts in the present. Third, the article highlights the Western-centric and state-centric preoccupations of such threat representations that, in many ways, overlook the complex links between geopolitical competitions and inequalities in global health on one side and cyberbio risks on the other. It does so by focusing specifically on bioinformation, which lies at the core of these threat discourses.

Bioinformation and pre-emptive security

Bioinformation occupies a central position in biological sciences and,⁷² in turn, in cyberbiosecurity thinking.⁷³ Since 2003, when the human genome project was completed,⁷⁴ a shift towards data-driven biosciences started to materialise. Subsequent projects produced massive amounts

⁶⁶Potter and Palmer, ‘Mission-aware differences in cyberbiosecurity and biocybersecurity policies’, p. 46.

⁶⁷Xavier-Lewis Palmer, Lucas Potter, and Saltuk Karahan, ‘An exploration on APTs in biocybersecurity and cyberbiosecurity’, *International Conference on Cyber Warfare and Security*, 17:1 (2022), pp. 532–5.

⁶⁸Murch, ‘Introduction’.

⁶⁹Ben Anderson, ‘Preemption, precaution, preparedness: Anticipatory action and future geographies’, *Progress in Human Geography*, 34:6 (2010), pp. 777–98.

⁷⁰Antonio Regalado, ‘Scientists hack a computer using DNA’, *MIT Technology Review* (10 August 2017), available at: <https://www.technologyreview.com/2017/08/10/150013/scientists-hack-a-computer-using-dna/>.

⁷¹Sina Faezi et al., ‘Oligo-snoop: A non-invasive side channel attack against DNA synthesis machines’, in *Proceedings 2019 Network and Distributed System Security Symposium* (San Diego, CA: Internet Society, 2019), available at: <https://doi.org/10.14722/ndss.2019.23544>.

⁷²Sabina Leonelli, *Data-Centric Biology: A Philosophical Study* (Chicago: University of Chicago Press, 2016), available at: <https://press.uchicago.edu/ucp/books/book/chicago/D/bo24957334.html>.

⁷³Dixon, ‘The grey zone of cyber-biological security?’.

⁷⁴Francis S. Collins, Michael Morgan, and Aristides Patrinos, ‘The human genome project: Lessons from large-scale biology’, *Science*, 300:5617 (2003), pp. 286–90.

of data, creating the need for more complex computational power to store, analyse, and share large databases and develop simulation and modelling tools that could advance scientific research. Such data-intensive practices contributed to the evolution of various important fields, such as bioinformatics and computational biology.⁷⁵ Currently, there are various digitally accessible bioinformatics databases, with primary and secondary, or curated, data. These include, for example, the Global Initiative on Sharing Avian Influenza Data (GISAID), DNA Databanks of Japan (DDBJ); GenBank at the National Center for Biotechnology Information (NCBI), USA; and the European Nucleotide Archive at the European Bioinformatics Institute, European Molecular Biology Laboratory (EMBL-EBI), UK. Some of these databases are free, such as GISAID, and some obtain monetary benefits for providing curated data, such as PROSITE, which is affiliated with the Swiss Institute of Bioinformatics.

Access to bioinformation databases is therefore becoming essential for public health and, in particular, for studying and tracing pathogens. The Covid-19 pandemic revealed the importance of sharing bioinformation and genetic sequence data (GSD) in a timely manner. It was due to the early availability of GSD, and the thousands of sequences uploaded on open online databases, such as GenBank and GISAID, that scientists around the world were able to work on diagnostic test kits, start research for developing vaccines and antiviral medications, and detect the transmission of the virus and the emergence of new variants and mutations. This all happened without accessing physical samples and ‘in a spirit of scientific openness’ by scientists, as there are currently no regulations to mandate the sharing of such information.⁷⁶ Data collected and analysed from hospitals, pharmacies, telephone calls to health-care agencies, or absences from work were also used as part of ‘syndromic surveillance’, according to which the pandemic was securitised and declared as a global health emergency.⁷⁷

Correspondingly, bioinformation occupies central position in cyberbio risk discourses and is usually presented as a primary target for cyber attacks affecting life sciences. It is through manipulating, stealing, or altering such information that the majority of scenarios of biological disaster are envisioned in cyberbiosecurity. Particular attention is given to the ‘openness’ of bioinformation databases as a cybersecurity risk, or the ability to freely access, download, or upload information, sometimes anonymously,⁷⁸ and what one study refer to as ‘naïve trust’ in research communities in the life sciences, according to which scientists share the data openly.⁷⁹ Many studies outline the security weaknesses in many of these databases, including the absence of access control measures for downloading data, no requirements for strong passwords or multifactor authentication in registration, and no methods to check data in transfer processes.⁸⁰ Further, some databases have unidentified users, even if they require registration. For example, in a survey conducted by the WHO PIP Advisory Group’s Technical Working Group, GISAID EpiFlu Database and OpenFluDB admitted they have unidentified users on their systems.⁸¹

Although none of these databases have been reportedly targeted by cyber attacks before, various pre-emptive security measures are proposed by cyberbiosecurity in order to prevent and mitigate

⁷⁵Dov Greenbaum, ‘The convergence of biotechnology and cybersecurity: A primer on the emerging field of cyberbiosecurity’, in Dov Greenbaum (ed.), *Cyberbiosecurity: A New Field to Deal with Emerging Threats* (Cham: Springer International Publishing, 2023), pp. 1–6; Ni, Gürsoy, and Gerstein, ‘Security vulnerabilities and countermeasures for the biomedical data life cycle’.

⁷⁶Michelle Rourke, Mark Eccleston-Turner, Alexandra Phelan, and Lawrence Gostin, ‘Policy opportunities to enhance sharing for pandemic research’, *Science*, 368:6492 (2020), pp. 716–18.

⁷⁷Long, ‘Securitising infectious disease outbreaks’.

⁷⁸Jacob Caswell, Jason D. Gans, Nicholas Generous, et al., ‘Defending our public biological databases as a global critical infrastructure’, *Frontiers in Bioengineering and Biotechnology*, 7 (2019), available at: <https://doi.org/10.3389/fbioe.2019.00058>; Peccoud et al., ‘Cyberbiosecurity’; Boris A. Vinatzer et al., ‘Cyberbiosecurity challenges of pathogen genome databases’, *Frontiers in Bioengineering and Biotechnology*, 7 (2019), available at: <https://www.frontiersin.org/articles/10.3389/fbioe.2019.00106>).

⁷⁹Peccoud et al., ‘Cyberbiosecurity’, 2017.

⁸⁰Vinatzer et al., ‘Cyberbiosecurity challenges of pathogen genome databases’.

⁸¹Caswell et al., ‘Defending our public biological databases’.

any future attacks against them. The advocated measures range from standard security practices and restricting access to data to government intervention. Standard practices may include applying strong passwords, multifactor authentication, and registration requirements for both downloading and uploading data. Others call for restricting access to databases, either by making them accessible once a grant application has been peer-reviewed or only during the time of research collaborations.⁸² Importantly, there are strong voices behind treating cybersecurity of bioinformation databases as a matter of *national security*, and thus demanding government intervention to secure it.⁸³ Private actors are perceived as incapable of providing such security, especially since the source of attacks is envisioned to be nation-state actors with capacity both to conduct sophisticated cyber attacks and to develop advanced biological weapons.⁸⁴

Government intervention, as proposed by many studies, can take the form of integrating the security of bioinformation in the cybersecurity strategies of military and intelligence agencies,⁸⁵ or depositing the data in government-managed databases,⁸⁶ and urging governments to use ‘advanced encryption algorithms’, akin to those used by banks to secure financial transactions, to protect those databases.⁸⁷ Additionally, because of fears that data published by scientific journals could be tampered with, one study called for establishing a ‘super-governmental framework for academic research’, which could set specific guidelines for data sharing for academic journals to ensure no suspicious or ‘false information’ has been embedded in public data.⁸⁸ Government involvement has also been called for on a global level, by proposing treating such databases as a ‘global critical infrastructure’, requiring global governance to secure it against any malicious use.⁸⁹

Lessons from cyber securitisation

The ongoing co-production of cyberbiosecurity and the various modes of securitising bioinformation in cyberbio risk discourses resembles the way cyber threats have been constructed since the 1990s. As Hansen and Nissenbaum argue, cybersecurity discourses relied heavily on *hypersecuritisation*, i.e. using hypothetical doom scenarios that do not necessarily have founding incidents in history, or using historical analogies, e.g. Cyber Pearl Harbor or Cyber 9/11. This created a perception of urgency to avoid ‘cascading disaster’ through immanent political interventions.⁹⁰ Such fear-based analogies and hypothetical cyber-doom scenarios have been central to policymakers’ cybersecurity discourses, especially in the ‘West’.⁹¹ Here, CNIs are prioritised, since disruption in their operations could lead to catastrophic consequences.⁹²

The emphasis on CNIs played a key role in constructing cybersecurity as an issue of national security.⁹³ It has also been instrumental in militarising ‘cyberspace’ and cybersecurity, and in turn,

⁸² Vinatzer et al., ‘Cyberbiosecurity challenges of pathogen genome databases’.

⁸³ DiEuliis, ‘Revisiting the digital biosecurity landscape’.

⁸⁴ Asha M. George, ‘The national security implications of cyberbiosecurity’, *Frontiers in Bioengineering and Biotechnology*, 7 (2019), available at: {<https://www.frontiersin.org/articles/10.3389/fbioe.2019.00051>}.

⁸⁵ George, ‘The national security implications of cyberbiosecurity’.

⁸⁶ Vinatzer et al., ‘Cyberbiosecurity challenges of pathogen genome databases’.

⁸⁷ Natasha E. Bajema, Diane DiEuliis, Charles Lutes, and Yong-Bee Lim, ‘The digitization of biology: Understanding the new risks and implications for governance’, Center for the Study of Weapons of Mass Destruction (9 July 2018), available at: {<https://wmdcenter.ndu.edu/Publications/Publication-View/Article/1569559/the-digitization-of-biology-understanding-the-new-risks-and-implications-for-go/https%3A%2F%2Fwmdcenter.ndu.edu%2FPublications%2FPublication-View%2FArticle%2F1569559%2Fthe-digitization-of-biology-understanding-the-new-risks-and-implications-for-go%2F>}.

⁸⁸ Potter and Palmer, ‘Mission-aware differences in cybersecurity and biocybersecurity policies’.

⁸⁹ Caswell et al., ‘Defending our public biological databases’.

⁹⁰ Lene Hansen and Helen Nissenbaum, ‘Digital disaster, cyber security, and the Copenhagen School’, *International Studies Quarterly*, 53:4 (2009), pp. 1155–75.

⁹¹ Sean T. Lawson, *Cybersecurity discourse in the United States: Cyber-doom rhetoric and beyond* (Routledge, 2019).

⁹² Noran Shafik Fouad, ‘Securing higher education against cyberthreats: From an institutional risk to a national policy challenge’, *Journal of Cyber Policy*, 6:2 (2021), pp. 137–54.

⁹³ Myriam Dunn Cavely, ‘Cyber-security and private actors’, in Rita Abrahamsen and Anna Leander (eds), *Routledge Handbook of Private Security Studies* (Abingdon: Routledge, 2015), pp. 89–99.

overlooking security approaches that consider wider societal implications of cyberthreats and its human aspects.⁹⁴ Further, the fear of potentially *destructive* cyber attacks against CNIs had protected cybersecurity from the budget cuts that other aspects of national security were subjected to in the post financial crash years.⁹⁵ This security framing, focusing on protecting CNIs and the military's role in securing 'cyberspace', which is primarily influenced by the experiences of the most advanced economies, has shaped what cybersecurity should like.⁹⁶ That is, it created an understanding that countries that manage to develop their economic and digital capacities and transition into the status of 'emerging economies' should invest heavily in militarising their cybersecurity strategies. For example, emerging economies such as Argentina, Brazil, Indonesia, Philippines, Mexico, and South Africa have all either already established or are in the process of establishing specialised military agencies for cybersecurity, i.e. cyber commands.⁹⁷ This increasing role of military and intelligence agencies in cybersecurity around the world has been criticised extensively by cybersecurity scholars for various reasons, including its negative impact on digital human rights and internet freedoms;⁹⁸ undermining trust among nations;⁹⁹ and challenging democratic governance in fragile political settings.¹⁰⁰

However, the scenarios of cyber wars resembling nuclear catastrophes, which were long imagined by many academics and cyber strategists, have not actually taken place. Instead, cyber incidents are now considered the 'new normal'. They happen on a daily basis in a persistent, albeit non-destructive manner. They destabilise without being apocalyptic.¹⁰¹ In addition, as argued by Rid, the violence resulting from cyberattacks is inherently indirect and less physical than conventional forms of violence.¹⁰² The indirect nature of the majority of cyberattacks and the non-physicality of their consequences challenge assumptions of existentiality, traditionally linked to physical damages in cybersecurity. That is to say, the scope of the cybersecurity challenge should not be reduced to the threat of one big incident or disaster. Cybersecurity is as much about less-than-high-profile operations as it is about highly publicised ones.¹⁰³ Importantly, as argued by Hansen and Nissenbaum, relying primarily on the future in constructing threats in the absence of prior catastrophes leads to ambiguity in security discourses, which may in turn be charged with exaggerations.¹⁰⁴

In the same vein, perceptions of biological danger, envisioned as primarily physical and catastrophic, could further contribute to a hyped, militarised, and state-centric approach to cybersecurity that ignores the ostensibly mundane threats if they do not carry destructive consequences. This is particularly because cyberbio risks impose a *physical* understanding of threats on cybersecurity. Fundamentally, cyber threats have always been invisible, with no adequate imagery. Visuality and imagery in cybersecurity are conditioned by the non-physical aspects of digital information.

⁹⁴Joe Burton and Clare Lain, 'Desecuritisising cybersecurity: Towards a societal approach', *Journal of Cyber Policy*, 5:3 (2020), pp. 449–70.

⁹⁵Robert M. Lee and Thomas Rid, 'OMG cyber!: Thirteen reasons why hype makes for bad policy', *The RUSI Journal*, 159:5 (2014), pp. 4–12.

⁹⁶Ciaran Martin and Noran Shafik Fouad, 'Five tests for risk-based approaches to national cybersecurity in resource-constrained environments', Digital Pathways at Oxford (2022), available at: {https://doi.org/10.35489/BSG-DP-WP_2022/05}.

⁹⁷Carlos Solar, 'Cybersecurity and cyber defence in the emerging democracies', *Journal of Cyber Policy*, 5:3 (2020), pp. 392–412.

⁹⁸Aaron Franklin Brantly, 'The cyber losers', *Democracy and Security*, 10:2 (2014), pp. 132–55.

⁹⁹Myriam Dunn Cavelty, 'The militarisation of cyberspace: Why less may be better', in Christian Czosseck and Katharina Ziolkowski (eds), *2012 4th International Conference on Cyber Conflict (Tallinn: CYCON 2012)* (IEEE, 2012), pp. 1–13, available at: {http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6243971}.

¹⁰⁰Solar, 'Cybersecurity and cyber defence in the emerging democracies'.

¹⁰¹Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* (Cambridge, MA: Harvard University Press, 2020).

¹⁰²Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013).

¹⁰³Fouad, 'Securing higher education against cyberthreats'.

¹⁰⁴Hansen and Nissenbaum, 'Digital disaster, cyber security, and the Copenhagen School'.

We cannot possibly visualise a phishing campaign or have an imagery of the aftermath of data being stolen in the same way we visualise wars or environmental crises through photographic imagery. This inherent invisibility of cyber insecurity makes claims of existentiality in regards to cyber threats hardly imaginable, even if they can be analysed through data visualisations and computational modelling. Cyberbiosecurity discourses that emphasise the high-profile threats that target life as a referent object, therefore, can transform these fundamental logics of cybersecurity by fostering a physical and existential understanding of security threats.

Futuristic security framings that emphasise peculiarity and high-profile threats could also have negative implications on biosecurity per se. This can be seen in the various processes through which governments monitor the thoughts, behaviours, and activities of life scientists on one side and control the development, dissemination, and publication of life science research on the other as key implications of this security framing.¹⁰⁵ Further, perception of biological dangers can have a major impact on our understanding and attitudes towards data privacy and security too. A case in point here is the Covid-19 pandemic and how surveillance practices, using contact tracing apps, mandatory wearable and telecommunication data tracking were all normalised and accepted as necessary responses to a global health emergency. As argued by Lyon, Covid-19 is the first pandemic in the context of surveillance capitalism and big data, in which tech solutionism aided by big corporations were portrayed as the gateway to the new normal. This allowed governments to use the disaster situation and shock factor to consolidate their power.¹⁰⁶ Similarly, fears of biological disaster caused by cyber attacks can result in security practices that further limit human privacy and security as collateral damage of protecting national security.

In fact, there are important issues related to human privacy in the security of bioinformation that are not given enough space in cyberbiosecurity discourses. One significant example is genomic privacy in relation to direct-to-consumer genetic testing companies (DTC-GT), which sell services directly to consumers by collecting and analysing their DNA samples and giving them insights about their ancestry and health. Such data can be shared or sold by these companies to universities, pharmaceutical companies, or law enforcement agencies. This currently remains one of the least regulated bio-informational spaces, despite the sensitivity of the data collected. A survey of the privacy and disclosure policies of DTC-GT companies operating in the USA, for instance, showed that more than third of the 90 companies examined did not have any privacy or security policy documents or were ambiguous over how the data is shared or used.¹⁰⁷ In June 2023, the US Federal Trade Commission implemented an enforcement action, considered the first of its kind, against the genetic testing company 1Health.io for not securing sensitive data and misleading consumers about its security and privacy policies.¹⁰⁸

What is more, unlike open-access databases that have not been subject to any reported cyber attack or breach, DTC-GT companies have. For example, in 2018, it was reported that DTC-GT company MyHeritage suffered a data breach that compromised the passwords and emails of 92 million user accounts, although not genetic data.¹⁰⁹ Also, in 2022, many genetic testing companies and fertility firms confirmed they have been subject to breaches that affected more than 3.5 million people.¹¹⁰ Most recently, 23andMe, another big company in the DTC-GT market, was subject to a

¹⁰⁵Rebecca J. Hester, 'Bioveillance: A techno-security infrastructure to preempt the dangers of informationalised biology', *Science as Culture*, 29:1 (2020), pp. 153–76.

¹⁰⁶David Lyon, *Pandemic Surveillance* (Cambridge: Polity, 2021).

¹⁰⁷James W. Hazel and Christopher Slobogin, 'Who knows what, and when: A survey of the privacy policies proffered by U.S. direct-to-consumer genetic testing companies', *Cornell Journal of Law and Public Policy*, 28:1 (2018), pp. 35–66.

¹⁰⁸Federal Trade Commission, 'FTC says genetic testing company 1Health failed to protect privacy and security of DNA data and unfairly changed its privacy policy' (16 June 2023), available at: <https://www.ftc.gov/news-events/news/press-releases/2023/06/ftc-says-genetic-testing-company-1health-failed-protect-privacy-security-dna-data-unfairly-changed>.

¹⁰⁹Norton, 'MyHeritage data breach exposes info of more than 92 million users' (8 August 2018), available at: <https://us.norton.com/blog/emerging-threats/myheritage-data-breach-exposes-info-of-more-than-92-million-user>.

¹¹⁰Aaron Schaffer, 'Hacks of genetic firms pose risk to patients, experts say', *Washington Post* (21 July 2022), available at: <https://www.washingtonpost.com/politics/2022/07/21/hacks-genetic-firms-pose-risk-patients-experts-say/>.

data breach, in which hackers accessed DNA ancestry data of 7 million users.¹¹¹ It was also reported that a subset of this stolen data, specifically about Ashkenazi Jews, was sold online by hackers, for \$1–10 per account, revealing genetic and geographic ancestry details.¹¹² That is, the risk of breaching genomic privacy is not hypothetical and consequently demands more consideration in cyberbiosecurity discussions, even if it does not lead to the same fatal, catastrophic consequences that other envisioned threats may produce. This aligns with calls for human-centric approaches in both cybersecurity¹¹³ and biosecurity.¹¹⁴

Besides, cyberbiosecurity's arguments on peculiarity, future threats, and physical damages resulting from high-profile attacks raise important questions: to what extent are cyberbio risks faced by biological sciences different from those faced by other CNIs (e.g. emergency, manufacturing, finance, or even health care)? Most importantly, does this arguable peculiarity justify the need for a whole new concept/field like cyberbiosecurity? This is an important discussion, especially in that similar arguments on peculiarity have been put forward in sectors like finance,¹¹⁵ manufacturing,¹¹⁶ and education,¹¹⁷ resulting in calls for sector-specific standards and policies, without necessarily establishing new fields/concepts. That is, we do not currently have cyber-finance security, cyber-manufacturing security, or cyber-education security as distinct fields of research and policy analysis. Although it is true that cyberbiosecurity pertains to information systems that combine both animate and inanimate substrates, in contrast to these other fields, this article argues that calls for inherent peculiarity should still be warranted. Specifically, it is important to consider what such arguments on peculiarity do to security politics and practices and how they may influence the current securitised governance of bioinformation.

The securitised governance of bioinformation

Bioinformation is currently subject to various modes of securitisation that affect its international flow and thus challenge assumptions of 'openness' in cyberbiosecurity discourses. That is, imposing cybersecurity's inherently exclusionary logics and recommendations to restrict access to bioinformation or to increase government involvement in managing bioinformation databases should be questioned. Moreover, as argued by Aradau and Van Munster in discussing threat perceptions around future terrorist attacks, 'arguments about what could happen and how to reduce vulnerability are formulated and demonstrated within this parallel world, at a distance from the complexities and political decisions of the manifest world.'¹¹⁸ Likewise, there are various governance challenges engendered by digitised bioinformation, often overlooked in cyberbiosecurity discussions, which require a global, rather than national, and a scientific, rather than state-led, approach to address them. In short, cybersecurity of biological sciences and bioinformation is important, but any approach to address the challenges it poses should be integrated within a holistic approach to bioinformation that ensures human privacy is protected, which does not further

¹¹¹Edward Helmore, 'Genetic testing firm 23andme admits hackers accessed DNA data of 7 m users,' *The Guardian* (5 December 2023), available at: {<https://www.theguardian.com/technology/2023/dec/05/23andme-hack-data-breach>}.

¹¹²Lily Hay Newman, '23andMe user data stolen in targeted attack on Ashkenazi Jews,' *Wired* (6 October 2023), available at: {<https://www.wired.com/story/23andme-credential-stuffing-data-stolen/>}.

¹¹³Ronald J. Deibert, 'Toward a human-centric approach to cybersecurity,' *Ethics & International Affairs*, 32:4 (2018), pp. 411–24.

¹¹⁴Craig Albert, Amado Baez, and Joshua Rutland, 'Human security as biosecurity: Reconceptualizing national security threats in the time of Covid-19,' *Politics and the Life Sciences*, 40:1 (2021), pp. 83–105.

¹¹⁵Md. Hamid Uddin, Md. Hakim Ali, and Mohammad Kabir Hassan, 'Cybersecurity hazards and financial system vulnerability: A synthesis of literature,' *Risk Management*, 22:4 (2020), pp. 239–309.

¹¹⁶Uchenna P. Daniel Ani, Hongmei (Mary) He, and Ashutosh Tiwari, 'Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective,' *Journal of Cyber Security Technology*, 1:1 (2017), pp. 32–74.

¹¹⁷Fouad, 'Securing higher education against cyberthreats.'

¹¹⁸Claudia Aradau and Rens Van Munster, *Politics of Catastrophe: Genealogies of the Unknown* (London: Routledge, 2011), p. 44.

hinder equity and fairness in sharing bioinformation, and which benefits global health rather than being solely driven by superpower competitions, as will be discussed next.

Equity, fairness, and the challenge of ‘openness’

Cyberbiosecurity literature considers the ‘openness’ of bioinformation databases and sharing processes as a security risk, but to what extent is information-sharing in life sciences actually open? Even though information-sharing and open access to data is fundamental to scientific research and a desired model for scientific advances, equitable distribution of benefits resulting from such sharing has always been a subject of debate from a global perspective.¹¹⁹ In fact, there are wide disparities and inconsistencies in data generation and sharing on the global level, the effects of which were seen in the Covid-19 pandemic in a way that affected global health outcomes.¹²⁰ Some studies show that more than a third of 62 countries reporting sequencing volumes for SARS-CoV-2 uploaded less than 50 per cent of their sequences to public repositories. Similarly, about 27 per cent of high-income countries uploaded less than 50 per cent of their total variant sequences.¹²¹ This means that a significant proportion of sequencing data is not actually shared internationally, and it follows that the majority of variant-related sequences are not uploaded to public databases in a timely manner.

There are many reasons behind the reluctance to share such data openly. For example, in the case of pathogen data, Elbe argues that more governments are subjecting lethal viruses to novel bordering practices.¹²² As argued by Elbe, countries exert ownership on viruses circulating within their territorial borders, maintaining what is referred to as ‘viral sovereignty’. Many countries express concerns about the inequitable access to biomedical interventions generated from international sharing of such data. This was evident during the Covid-19 pandemic when high-income countries engaged in vaccine nationalism by purchasing more doses than they needed, while the rest of the world’s nations were struggling to satisfy first-dose needs for their population.¹²³ There are always also political and economic ramifications resulting from sharing pathogen information, for example, for the first country to report a case, or for countries dependent on tourism and trade, thus creating strong economic incentives to withhold data, or to subject them to lengthy reviewing processes.¹²⁴

Digital sequence information (DSI), specifically, poses even more challenges to equity and benefit-sharing; one prominent case here is global biodiversity research. The Convention on Biological Diversity (CBD), which 196 nations are part of, commits countries to fair and equitable sharing of benefits of genetic resources, a commitment that is also codified in the Nagoya Protocol on Access and Benefit Sharing (ABS), which became effective in 2014. This is done by acknowledging the right of the country to regulate access to its genetic resources to ensure it benefits from profits resulting from using the shared data. Yet DSI lies outside the scope of CBD and NP, which focuses mainly on physical samples. In fact, DSI challenges a lot of the assumptions based on which ABS policies were developed, including the clear identification of ownership and the feasibility of tracing value throughout the research process.¹²⁵ This affects national sovereignty,

¹¹⁹ Amber Hartman Scholz, Amber Hartman, Jens Freitag, et al, ‘Multilateral benefit-sharing from digital sequence information will support both science and biodiversity conservation’, *Nature Communications*, 13:1 (2022), p. 1086.

¹²⁰ Rob Johnson et al., ‘Intelligent open science: A case study of viral genomic data sharing during the Covid-19 pandemic’, Research Consulting (2022), available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1118628/intelligent-open-science.pdf.

¹²¹ Zhiyuan Chen, Andrew S. Azman, Xinhua Chen, et al., ‘Global landscape of Sars-Cov-2 genomic surveillance and data sharing’, *Nature Genetics*, 54:4 (2022), pp. 499–507.

¹²² Stefan Elbe, ‘Who owns a deadly virus? Viral sovereignty, global health emergencies, and the matrix of the international’, *International Political Sociology*, 16:2 (2022), p. olab037.

¹²³ Elbe, ‘Who owns a deadly virus?’.

¹²⁴ Johnson et al., ‘Intelligent open science’.

¹²⁵ Sarah Laird, Rachel Wynberg, Michelle Rourke, Fran Humphries, Manuel Ruiz Muller, and Charles Lawson, ‘Rethink the expansion of access and benefit sharing’, *Science*, 367:6483 (2020), pp. 1200–2.

as many biodiverse low- and middle-income countries argue that commercial benefits from DSI are not shared with them, the same as with genetic resources. As a result, many believe that DSI constitutes a 'loophole' in existing bioinformation-sharing systems and appears in negotiations as a main hurdle to reaching any political consensus on a 'Global Biodiversity Framework'.¹²⁶ It is important to note here that discussions around including DSI in CBD only started in 2016, and there is still wide contestation on defining DSI precisely.¹²⁷

On the other side, some governments criticise how online databases do not protect the national sovereignty of the state, by allowing users to upload and download data without signing users' agreements or registrations. Thus, by uploading the data, researchers could violate their countries' national laws and regulations.¹²⁸ However, national regulatory regimes aiming to maximise the commercial benefits from genetic resources and maximise state control remain a big hurdle in international collaborations, through lengthy permits and transaction costs and complex bureaucratic procedures.¹²⁹ To tackle this issue, the WHO is championing ABS as a solution to the ethical challenges of equity in information sharing, and it is exploring its applicability to pathogen information sharing. However, there is no easy solution, as such discussions sometimes clash with the WHO's mission, especially in times of health emergencies, when it would not be feasible or time-efficient to negotiate ABS agreements for sharing pathogens, which could take years.¹³⁰

Inequalities also extend to scientific communities. Due to financial limitations, lack of research funding, and limited training and career opportunities, many researchers in low- and middle-income countries are put in a disadvantaged position.¹³¹ This is what Elbe argues denotes the whiteness of global health security and the legacies of racialised colonial expansion, extraction, and capitalism that led to epistemic privilege for scientists in the Global North and their access to sophisticated laboratory facilities, funding, etc.¹³² Moreover, scientists in the Global South often complain that the data they share in good will have been used in international conferences without proper acknowledgements in authorship agreements or any prior notification.¹³³ This leads to underrepresentation in many of the available data, due to inequalities and biases in research practices. Most of the data in the largest genomic databases comes from Europe, USA, and Canada, in stark difference with countries such as India, Pakistan, and Bangladesh, which have a significant percentage of world population, despite making up less than 2 per cent of human microbiome samples.¹³⁴

In light of the above discussion, it becomes clear that the assumption of 'openness' and 'naïve trust' in life-science research communities as presented in cyberbiosecurity literature should be questioned. Countries already exert varying degrees of control over bioinformation and subject it to various security, political, and economic considerations that hinder scientific research. Similarly, researchers are often reluctant to share data until they publish their own research since this could affect their careers and competition with other scientists. Thus, a state-centric and national security-focused approach to the cybersecurity of bioinformation would provide the legitimate basis to governments and other actors to withhold data on cybersecurity grounds too. Additionally, any restriction to data access for cyberbiosecurity should take into consideration

¹²⁶Scholz et al., 'Multilateral benefit-sharing from digital sequence information'.

¹²⁷Laird et al., 'Rethink the expansion of access and benefit sharing'.

¹²⁸Nithin Ramakrishnan and Chetali Rao, "'Open" databases undermine access and benefit sharing' (March 2023), available at: <https://www.twn.my/title2/health.info/2023/hi230301.htm>}.
¹²⁹K. Divakaran Prathapan, Rohan Pethiyagoda, Kamaljit S. Bawa, et al., 'When the cure kills: CBD limits biodiversity research', *Science*, 360:6396 (2018), pp. 1405–6.

¹³⁰Rourke et al., 'Policy opportunities to enhance sharing for pandemic research'.

¹³¹Scholz et al., 'Multilateral benefit-sharing from digital sequence information'.

¹³²Stefan Elbe, 'Bioinformational diplomacy: Global health emergencies, data sharing and sequential life', *European Journal of International Relations*, 27:3 (2021), pp. 657–81.

¹³³Elbe, 'Bioinformational diplomacy'.

¹³⁴Richard J. Abdill, Elizabeth M. Adamowicz, and Ran Blekman, 'Public human microbiome data are dominated by highly developed countries', *PLOS Biology*, 20:2 (2022), available at <https://doi.org/10.1371/journal.pbio.3001536>}.
<https://doi.org/10.1017/eis.2024.19> Published online by Cambridge University Press

equity and fairness and should be integrated in current conversations on regulating open access to DSI to ensure equitable share of benefits. This is mainly because the processes of digitisation and opening access were primarily seen as a way to enhance access for researchers in the Global South, which could be hindered by cybersecurity-driven restrictions, which could also over-complicate prospects of cross-national collaborations.¹³⁵ This is taking into consideration that the majority of these databases are hosted by a small number of high-income countries, and they retain the right to suspend access to users as part of their terms and conditions.¹³⁶ That is why it has always been questioned to what extent such platforms attend to the interests of global stakeholders in the first place.¹³⁷ Increasing government intervention or complicated licensing processes can make access to data lengthy and costly and therefore will restrict access to a small number of researchers who are capable of dealing with such bureaucratic hurdles,¹³⁸ which is why most of the published research currently relies on open access databases.¹³⁹

Superpower competition

Bioinformation plays a central role in great power competitions and in the race for technology domination. Information is now capable of driving innovation in various fields, developing novel tools, organisms, and products that would enhance countries position in the global bioeconomy. Genomic data, in particular, is generating substantial commercial value in multiple fields, especially in precision medicine and healthcare. The AI in Healthcare Market, which relies heavily on access to large genomic data sets, is projected to grow from USD 9.01 billion in 2022 to USD 187.76 billion by 2031.¹⁴⁰ As argued by one study, ‘the basic currency of biotechnology is genomic data and its associated metadata across all aspects of the life sciences’.¹⁴¹ This has transformed bioinformation, especially in the form of genomic data, into a strategic resource, subject to competition among superpowers, and especially between the USA and China.

Although the USA remains the leading country in biotechnology, especially in infrastructure, China is achieving fast progress, and the gap between the two countries is getting narrower.¹⁴² Following China’s decision to list biotechnology as one of the key areas for national development under its state-led industrial policy entitled ‘Made in China 2025’,¹⁴³ it managed to achieve major scientific leaps. According to Nature Index Annual Tables in 2023, China has surpassed the USA, UK, and Germany in high-quality international publications in natural sciences, including biological sciences, raising its share by 21 per cent from 2021 to 2022. Institutionally, half of the 20 institutions with the highest score for natural science publications are based in China.¹⁴⁴ China also produces most biotechnology patents annually, increasing its global share from 1 per cent in 2000 to 28 per cent in 2019, while the US share dropped from 45 per cent to 27 per cent.¹⁴⁵ Its share of the global biopharmaceutical market is increasing too, becoming the second largest globally

¹³⁵Scholz et al., ‘Multilateral benefit-sharing from digital sequence information’.

¹³⁶Caswell et al., ‘Defending our public biological databases’.

¹³⁷Johnson et al., ‘Intelligent open science’.

¹³⁸Robert M. Hauser, Maxine Weinstein, Robert Pool, and Barney Cohen (eds), *Conducting Biosocial Surveys Collecting, Storing, Accessing, and Protecting Biospecimens and Biodata* (The National Academies Press, 2010).

¹³⁹Ni, Gürsoy, and Gerstein, ‘Security vulnerabilities and countermeasures for the biomedical data life cycle’.

¹⁴⁰Transparency Market Research, ‘AI in healthcare market’ (April 2023), available at: {<https://www.transparencymarketresearch.com/ai-in-healthcare-market.html>}.

¹⁴¹DiEuliis, ‘Revisiting the digital biosecurity landscape’.

¹⁴²Scott Moore, ‘China’s role in the global biotechnology sector and implications for U.S. policy’, Brookings (April 2020), available at: {https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_china_biotechnology_moore.pdf}.

¹⁴³Adolfo Arranz, ‘Beijing bets on biotech’, *South China Morning Post* (9 October 2018), available at: {<https://multimedia.scmp.com/news/china/article/2167415/china-2025-biotech/index.html?src=social>}.

¹⁴⁴Chris Woolston, ‘What China’s leading position in natural sciences means for global research’, *Nature*, 620:7973 (2023), pp. S2–S5.

¹⁴⁵A. I. Salitskii and E. A. Salitskaya, ‘China on the way to global technology leadership’, *Herald of the Russian Academy of Sciences*, 92:3 (2022), pp. 262–7.

after the USA.¹⁴⁶ Private-sector companies are achieving similar successes, with Chinese genomics company BGI becoming the world's largest genetics research centre, sequencing data six times less expensively than competitors.¹⁴⁷

China declared biomedical data as 'national strategic resource' in 2016, with the power to revoke approved licences to research, without even disclosing reasons. For example, in 2018, the government confiscated exported genomic data and revoked licences granted to two high-profile projects: one between UCLA and Shanghai Jiaotong University, and another between Oxford University and Peking University. China now has very complicated regulations to govern bioinformation, especially genomic data. Laws were also issued in 2019 and 2021 restricting Chinese organisations from sharing certain types of genetic information with foreign groups. Collecting, storing, or sharing genetic materials or information requires ministry-level approval at every step, especially if it involves any extraterritorial possession.¹⁴⁸ Data generated by non-health institutions (biobanks, research institutes, clinical labs, hospitals, etc.) has to get approval from government before it is transferred overseas.¹⁴⁹

It is thus no surprise that the US government has been expressing concerns over the rising power of China in biotechnology and its control of and access to bioinformation. For example, the US National Counterintelligence and Security Center issued a report in 2021 arguing that China's ability to access health-care data from the USA is contributing to its advancements in AI and precision medicine, and eventually to its bid to own the world's largest bio-database.¹⁵⁰ From the US perspective, this is a problem because China restricts foreign access to its own data, which therefore disadvantages the USA and its biotechnology industry. According to the report, this dynamic will allow China to outpace and displace the US biotechnology firms and their leadership and will create what they characterise as 'dependency' on innovation and medicine developed in China, which will have massive economic ramifications. The US government has also expressed concerns about increasing Chinese investments in US-based genomic sequencing companies. Prominent examples include the China-based company WuXi investing in the US-based company 23andMe and the acquisition of Complete Genomics.¹⁵¹

This is a rivalry that cyberbiosecurity discourses contribute to, by focusing on state-centric threats of sophisticated cyber attacks that can impact life and spread disease. Allegations against hackers in China targeting research institutes, universities, and biotech companies during Covid-19 have particularly heightened fears in the USA and Western countries. As expressed by Edward You, a Supervisory Special Agent in the FBI's Weapons of Mass Destruction Directorate, 'we don't know how much bio data has left our shores'.¹⁵² That is why national security agencies in the USA urged states not to accept offers from Chinese companies to set up testing labs for Covid-19 for fears of accessing DNA.¹⁵³ There were also security concerns in the UK around the UK Biobank and its

¹⁴⁶ Franck Le Deu, Serina Tang, and Gaobo Zhou, 'Biopharma in China: Insights into a market at a crossroads', McKinsey & Company (29 May 2019), available at: <https://www.mckinsey.com/industries/life-sciences/our-insights/biopharma-in-china-insights-into-a-market-at-a-crossroads>].

¹⁴⁷ Antonio Regalado, 'China's BGI says it can sequence a genome for just \$100', *MIT Technology Review* (26 February 2020), available at: <https://www.technologyreview.com/2020/02/26/905658/china-bgi-100-dollar-genome/>].

¹⁴⁸ Smriti Mallapaty, 'China expands control over genetic data used in scientific research', *Nature*, 605:7910 (2022), p. 405, available at <https://www.nature.com/articles/d41586-022-01230-z>].

¹⁴⁹ Yongxi Chen and Lingqiao Song, 'China: Concurring regulation of cross-border genomic data sharing for statist control and individual protection', *Human Genetics*, 137:8 (2018), pp. 605–15.

¹⁵⁰ The National Counterintelligence and Security Center, 'Protecting critical and emerging U.S. technologies from foreign threats' (October 2021), available at: https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_Emerging%20Technologies_Factsheet_10_22_2021.pdf].

¹⁵¹ Julian E. Barnes, 'U.S. warns of efforts by China to collect genetic data', *The New York Times* (22 October 2021), sec. U.S., available at: <https://www.nytimes.com/2021/10/22/us/politics/china-genetic-data-collection.html>].

¹⁵² David J. Lynch, 'Biotechnology: The US–China dispute over genetic data', *Financial Times* (31 July 2017).

¹⁵³ Greg Myre, 'China wants your data – and may already have it', *NPR* (24 February 2021), available at: <https://www.npr.org/2021/02/24/969532277/china-wants-your-data-and-may-already-have-it>].

300 projects in collaboration with researchers in China, which gave researchers access to a biomedical database containing the DNA of half a million British citizens, leading to calls for a review of data-transfer policies.¹⁵⁴ Arguably, although such fears may result in security measures that protect human privacy by securing citizens' DNA data, they are primarily driven by state-centric, rather than human-centric security approaches.

This all contributes to the securitised governance of bioinformation, and especially that of genomic data. There is an increasing fear that losing control of such data will have economic consequences that might be decisive in this superpower competition. On multiple occasions, the FBI and the Directorate on Weapons of Mass Destruction have expressed fears that digital data can be lethal, due to the possibility of monetisation and its implications for the competitive advantage of nations.¹⁵⁵ This creates more barriers to transfer of bioinformation and affects other countries' ability to access it, especially low- and middle-income countries. Increasing barriers even towards Chinese biomedical investment might be damaging to the US biomedical industry itself, because they deprive it of a huge amount of investment and talent and the low-cost and large-scale genetic sequencing that China is capable of.¹⁵⁶ As such, the extra level of securitisation brought forward by some arguments in cyberbiosecurity could have negative implications for scientific advancements that are essential for global health, such as precision medicine, which requires access to huge data sets.

Conclusion

This article analysed the co-production of the new field and concept of cyberbiosecurity as presented in academic literature in the life sciences. It investigated the key discourses co-producing cyberbiosecurity and the various security modalities that constitute the foundation of threat perceptions around the intersection of cyber threats and biological dangers. Acknowledging the increasing vulnerability of biological sciences to cyber threats due to their digital dependency, in addition to the security context of the Covid-19 pandemic that demonstrated the close links between cybersecurity and global health, the article approached cyberbiosecurity as a political challenge that is deeply entangled with the global politics of both cybersecurity and biosecurity. As such, the article brought discussions on cyberbiosecurity into the realm of IR and Security Studies by investigating the relationship between discourses on cyberbio risks and the pre-emptive security measures they propose on one side and the existing securitised governance of bioinformation on the other.

The article argued that presenting cyberbiosecurity as a peculiar field, constructing cyberbio threats through futuristic scenarios, and prioritising high-profile threats with potential physical consequences can have major implications for the governance of both cybersecurity and biosecurity. On the one hand, imposing a *physical* understanding of threats that target life as a referent object can further intensify the militarisation of cybersecurity and the neglect of the ostensibly mundane threats that target human security and which have damaging societal impacts even if they do not qualify as 'destructive'. On the other hand, perceptions of cyber attacks leading to catastrophic biological danger and many of the pre-emptive security measures proposed by cyberbiosecurity contribute to state-centric approaches to biosecurity, primarily influenced by superpower competitions for technology dominance. The consequences of such security framing could thus shape the future of both cybersecurity governance and global health.

Since the field of cyberbiosecurity is at an early stage of its evolution, it matters how the discussions are being formulated and what sort of security logics are driving them. As shown in the article, bioinformation is already subjected to various modes of securitisation and state

¹⁵⁴Shanti Das and Vincent Ni, 'Fears over China's access to genetic data of UK citizens', *The Observer* (20 August 2022), available at: {<https://www.theguardian.com/science/2022/aug/20/fears-over-chinas-access-to-genetic-data-of-uk-citizens>}.

¹⁵⁵Lynch, 'Biotechnology'.

¹⁵⁶Lynch, 'Biotechnology'.

control, with implications for scientific research, equity and fairness, and global health more generally. Securing bioinformation against potential future cyber threats is important, and initiating multidisciplinary discussions to prepare for such risks is a logical response to the cybersecurity challenges posed by the Covid-19 pandemic. Yet any cyberbiosecurity intervention should not impose a national security framing on the entirety of biological sciences. Rather, a global, rather than national, approach is needed to consider the security of bioinformation as a global common good, rather than a national strategic resource that should be militarised and restricted. This approach should distinguish between different types of data and determine which is integral to global scientific cooperation. Moreover, assumptions of peculiarity in cyberbiosecurity should be directed towards creating peculiar standards for life sciences industries, without detaching them from existing discussions in other sectors and CNIs, for which international cyber norms to determine responsible state behaviour are being debated. It is important too to prioritise persistent and existing threats, e.g. against health care, pandemic misinformation, and human genomic privacy, which may not qualify as high-profile, yet have major political, economic, and societal implications. As argued by Aradau and Van Munster, absence of catastrophic language can have major implications on our judgement of the present.¹⁵⁷

Acknowledgements. I was lucky to design and teach a masterclass for postgraduate students on the topic of cyberbiosecurity, and I am grateful to all my students for the insightful and thought-provoking discussions that inspired me in writing this article. I would also like to thank the participants of the 16th EISA Pan-European Conference on International Relations (September 2023) for their feedback on an earlier version of this article. I extend my thanks to the anonymous reviewers and the editors of *EJIS* for their very constructive comments.

Noran Fouad is Lecturer in Digital Politics at Manchester Metropolitan University, UK. She has a PhD in International Relations from the University of Sussex and worked previously as a postdoctoral researcher at the University of Oxford. Her research and teaching lie at the intersection of technology, security, and governance, with a particular focus on cybersecurity. Her research interests include critical approaches to cybersecurity in International Relations, cybersecurity of the everyday, the global politics of cyber governance, and the co-production of cybersecurity policies and practices between human and non-human agency.

¹⁵⁷ Aradau and Van Munster, *Politics of Catastrophe*, p. 4.