Cyber-Biosecurity

An Emerging National Security Frontier

Mrinmayee Bhushan*

Cyber-Biosecurity, an emerging threat landscape at the intersection of cybersecurity, cyber-physical security and biosecurity has a potential to disrupt economic, social and political well-being of the nation and has tremendous national security implications. All forms of cyber-attacks impact the manufacturing industries, governments, health infrastructure, patients and bio-economy at large. Rapidly evolving Cyber-Biosecurity threat landscape has potential to disrupt the rapid growth of Indian bio-economy by compromising data security and intellectual property, disrupting manufacturing operations and supply chains resulting in destabilising investor confidence in Indian Bio-economy. Indian National Security Framework too needs to have comprehensive Cyber-Biosecurity policy and infrastructure in place before the biological equivalent of Metasploit becomes commonplace. Some important considerations for the same are the not-so-covert ongoing conflicts in the cyberspace with a probability of boiling over to the Cyber-Biosecurity landscape, and 'Defend Forward' as deterrence policy of many nations. India urgently needs to address the need for robust Cyber-Biosecurity legal infrastructure and comprehensive policy formation with the proactive participation of all the stakeholders.

Keywords: *Cybersecurity, Cyber-Biosecurity, data security, bio-economy, national security, Health Security*

* Dr Mrinmayee Bhushan is Biosecurity and Chemical Security Expert & Preparedness Consultant, Oxford-Chevening CRISP Fellow, Medical Pharmacology & Microbiology.

ISSN 0976-1004 (print); 2583-7567 (online)

Journal of Defence Studies, Vol. 17, No. 2, April–June 2023, pp. 93–119

Introduction

The last two decades have witnessed a transition of industrial and fundamental research of biotechnology from analog to digital, with data sciences and computing functioning as the accelerator for the development. The aim of this strategic analysis is to understand and appreciate the challenges posed by this Artificial Intelligence (AI) driven hybrid threat landscape with tremendous potential to disrupt the well-being of the citizens, destabilise the growth of Bio-economy and compromise the National Security.

These hybrid threats have the potential to not only disrupt the nation's digital sovereignty, but also people's trust in the health crisis response capability of the leadership.

Current global bio-weapons non-proliferation frameworks and Biosecurity policy frameworks have been designed to prevent and mitigate the risks associated with bio-weapons development, by only regulating physical access of specific biological agents, biotechnology tools and materials. However, these are insufficient and outdated to prevent the fast-evolving hybrid threats equipped with emerging technology innovations. To effectively address this challenge, the policymakers need to formalise a collaborated approach with emerging technology experts across all the disciplines, to develop regulatory frameworks to anticipate, detect and mitigate Cyber-Biosecurity threats.

Convergence of Emerging Technologies

Rapidly emerging scientific and technological advances present new economic, security, ethical, and regulatory challenges worldwide, as governments and international regulatory bodies struggle to keep pace. Transdisciplinary research is related to the collective evolution of perspectives and approaches of practitioners from various disciplines to synthesize and create novel innovations that provide integrated solutions.

These technologies not only hold great promise for advances in precision medicine, agriculture, and manufacturing, but they also introduce bio-risks, such as the potential to develop novel biological weapon agents, threaten food security, and enhance or degrade human performance. The scientific developments, innovations and the exponential growth of transdisciplinary technologies meant for the *welfare* of the people, have the potential to be utilised for their *warfare* applications as well. The products of these emerging technologies have drastically lowered the limitations and barriers of weaponising biotechnology for amateurs, resulting in tectonic shifts in the global bio-risk landscape.

The entire history of biological threats, such as bio-crimes, bioterrorism, bio-weapons (BWs) experimentation, or bio-warfare, has numerous examples of state- and non-state actors utilising *Plausible Deniability*, a unique characteristic feature of BWs, to the fullest advantage. The comparison of fatalities of COVID-19 pandemic being much more than the combined fatalities of both the world wars, has uncovered the ugly underbelly of century-old unabated BWs arms race, that has been further fueled by the emerging technologies.[1] This brutal COVID-19 arithmetic has forced average citizens to raise questions regarding the dual use nature of emerging technologies and related national security implications.

What is Cyber-Biosecurity?

Cyber-Biosecurity, an emerging discipline at the interface of Cybersecurity and Biosecurity has evolved into a new frontier of national security vulnerability as transdisciplinary technological progress continues to accelerate in Synthetic Biology, Automation, Cybernetics, Nanotechnology, Robotics, Data Sciences and Artificial Intelligence. Technologies such as biotechnology laboratory automation, Computational Biology, Computer-aided Drug Designs, Electronic Medical Records (EMRs) and Data Management Systems, Cyborgs are some of the examples of transdisciplinary innovation platforms and convergence products of emerging technologies.

Cyber-Biosecurity is an emerging frontier and rapidly evolving enterprise at the interface of Cybersecurity, Biosecurity and Cyber-physical security as applied to Biotechnology and Biomedical systems. It involves the protection of biological systems, data, and technologies from unauthorized access, theft, manipulation, and destruction.

Cyber-Biosecurity is broadly defined as, "understanding the vulnerabilities to unwanted surveillance, intrusions, and malicious and harmful activities which can occur within or at the interfaces of comingled life and medical sciences, cyber, cyber-physical, supply chain and infrastructure systems, and developing and instituting measures to prevent, protect against, mitigate, investigate and attribute such threats as it pertains to security, competitiveness and resilience."[2]

While refining this definition of Cyber-Biosecurity with expansion to differentiate it from the individual scopes of cybersecurity and biosecurity according to Richardson et al., "Cyber-Biosecurity addresses the potential for or actual malicious destruction, misuse, or exploitation of valuable information, processes, and material at the interface of the life sciences

and digital worlds; concept mastery requires an understanding of this interface in the context of the threat of malignant use of technology in general."[3]

Some key facets of Cyber-Biosecurity include:

1. *Bioinformatics security*: Bioinformatics is the application of computer science and information technology to the field of biology. It involves the analysis and interpretation of biological data, including genetic sequences, protein structures, molecular pathways and other biological information related to biological research. Bioinformatics security involves protecting the integrity and confidentiality of this data, which can be vulnerable to cyber threats, which may result in intellectual property theft.
2. *Cybersecurity in biotechnology research*: Biotechnology research involves the use of advanced technologies such as gene editing, synthetic biology, and genome sequencing. These technologies generate vast amounts of data and require the use of sophisticated computer systems. Cybersecurity in biotechnology research involves protecting the data and systems involved in this research from cyber threats.
3. *Security of bio-manufacturing facilities*: Bio-manufacturing facilities are used to produce biological products such as vaccines, therapeutics and diagnostics. These facilities use advanced technologies and automation systems that are vulnerable to cyber threats. Cyber-Biosecurity in bio-manufacturing facilities involves protecting these systems and technologies from cyber-attacks.
4. *Biosafety and biosecurity of digital biotechnologies*: Digital biotechnologies are a new class of biotechnologies that involve use of digital tools such as artificial intelligence, machine learning and blockchain. These tools can be used to analyse and interpret biological data, as well as to design and manufacture novel biological products. Cyber-Biosecurity in digital biotechnologies involves ensuring the biosafety and biosecurity of these tools and technologies.

Overall, Cyber-Biosecurity is a field that requires transdisciplinary expertise in cybersecurity, biosecurity and biotechnology. It involves the protection of biological systems, data, and technologies from cyber threats and is becoming increasingly important as biotechnology research and development continue to advance.

Examples of such transdisciplinary emerging cyber-biophysical systems and devices vulnerable to attacks include:

- Neuromorphic computing and 3-D bio-printing;

- Encoding digitized DNA with malware; and increasing security risks to cyber-biophysical informatics and materials from industrial espionage.
- Bio-mechatronics, which can be defined as science that aims to integrate biology, mechanics, electronics, robotics and neuroscience.[4]
- Bio-megatronics focuses on the research and design of assistive, therapeutic and diagnostic devices to partially compensate for the loss of human physiological functions or to enhance these functions.
- Recent developments include artificial organs and tissues, prosthetic limbs, orthotic systems, wearable systems for physical augmentation, physical therapy and rehabilitation, robotic surgery, and natural and synthetic sensors.
- Artificially developed organic materials mimic their natural counterparts when deployed in cyber-enabled technologies.

Cyber-Biosecurity Threat Landscape

Reminiscent to cyberattacks on physical assets such as industrial security, control networks and critical infrastructures, Cyber-Biosecurity attacks remotely inflict damage to, steal intellectual property of and sabotage bio-industrial processes or critical research pathways, compromise digital health data and healthcare devices, and threaten integrity of high-containment laboratory security. These Cyber-Biosecurity vulnerabilities and threats have potential to affect many critical infrastructures such as Critical Manufacturing, Emergency Medical Response Services, Public Health, Healthcare, Chemical industries, Defence Assets, Food Industry and Agriculture.

Digital Health and Health Infrastructure

A series of events sent shockwaves to the entire medical devices industries across the world including the wireless settings of the US Vice President Dick Cheney's pacemaker being deactivated in 2013 to avoid an assassination attempt; a revelation by former hacker and security expert, Barnaby Jack of reverse engineering a pacemaker to release a series of 830 volt shocks as a demonstration of hacking; followed by US FDA recalling half a million pacemakers from the market, with a fear of being hacked, with a statement, "As medical devices become increasingly interconnected via the Internet, hospital networks, other medical devices,

and smartphones, there is an increased risk of exploitation of cybersecurity vulnerabilities".[5]

The cyber-threat attack frequency to the medical and healthcare sector has been increasing steadily with the discovery of up to 500 attacks every minute. As stated by an Advanced Threat Research Report-2021, the Hive Ransomware family prevalence as part of a new campaign of ransomware developers was first observed in India, Belgium, Italy, the United States, Turkey, Thailand, Mexico, Germany, Colombia and Ukraine, compromising healthcare and critical infrastructure organisations operating as a Ransomware-as-a-Service written in Go-language.[6]

The increasing frequency of recent ransomware attacks on premier Indian health establishments such as the All India Institute of Medical Sciences (AIIMS) and Indian Council of Medical Research (ICMR), New Delhi have highlighted the need to protect critical national health infrastructures.[7] The cyberattack on the AIIMS Delhi sever potentially exposed critical data including employee login credentials, and hospital records of 40 million patients, fueled the discussions on Cyber-Biosecurity across the nation.[8] The public awareness of data security, economic, political and social consequences of such high-profile ransomware attacks and overall awareness about the cyber-biosecurity threat landscape and mitigation measures is lacking in research, healthcare and bio-industries.

A recent survey in India involving 50 urban healthcare leaders throws light on the ground realities of the Indian healthcare sector. Though the response to technology spending is encouraging with 80 per cent respondents having plans to significantly invest in digital solutions and technology initiatives by leveraging 5G to drive healthcare outcomes; 66 per cent respondents lacked confidence in the capability of their digital infrastructure to prevent cyber-attacks, with only 40 per cent being positive that technology infrastructure could ensure patient data privacy.[9]

Medical Devices

Another such related report indicates (Figure 1) that the most impacted product category of devices and software, comprises of records and management software, contributing to 17 per cent. [10]

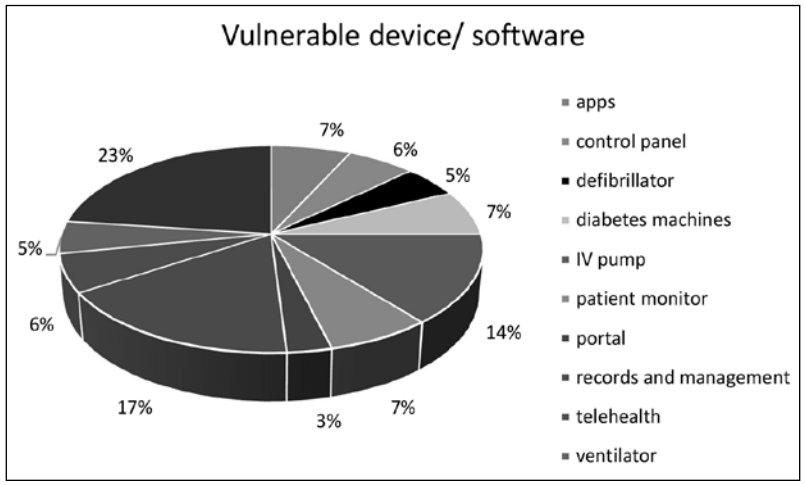

Figure 1 Device vulnerabilities by product category and software impacted [5]

The cybercrime implications of Internet-of-Medical-Things (IoMTs) based medical devices entering the market are often overlooked. A forward-thinking mechanism of 'Cyber-Biosecurity by design' is required to create awareness amongst the medical device developers to incorporate the cybersecurity features during the product development cycle and during the navigation through the medical device regulatory pathway, to address the potential risks before the widespread use of the medical devices in the market.[11]

Brain–Computer Interfaces (BCIs)

Human enhancement via Brain–Computer Interfaces has been debated for years for its ethical considerations. The patient's physical health, personality, cognition and decision making may get reflected in the BCI data. The data is often not encrypted while passing through various software and wired or wireless devices, creating myriad touch-points for increasing Cyber-Biosecurity threats.[12]

Cyber-Biosecurity and Advanced Persistent Threats (APTs)

Advanced Persistent Threats (APTs) are the threats targeting primarily the nation states, associated entities including the corporate and private sector

in the target zone. A state- or non-state APT attacker has been known for peculiar characteristics:

- Pursues objectives repeatedly for an extended period of time
- Adapts according to the defenders' strategies
- Determined to maintain the level of interaction required to achieve the objectives

COVID-19 was a learning experience for Cyber-Biosecurity challenges, highlighting the APT risks for bio-manufacturing industries.[13]

Cyber-Biosecurity threats related to Surveillance & Management of Infectious Diseases

Cyber-Biosecurity vulnerabilities and challenges of public health agenda such as infectious disease surveillance, contact tracing and management of infectious disease have been illustrated in Figure 2.[14]

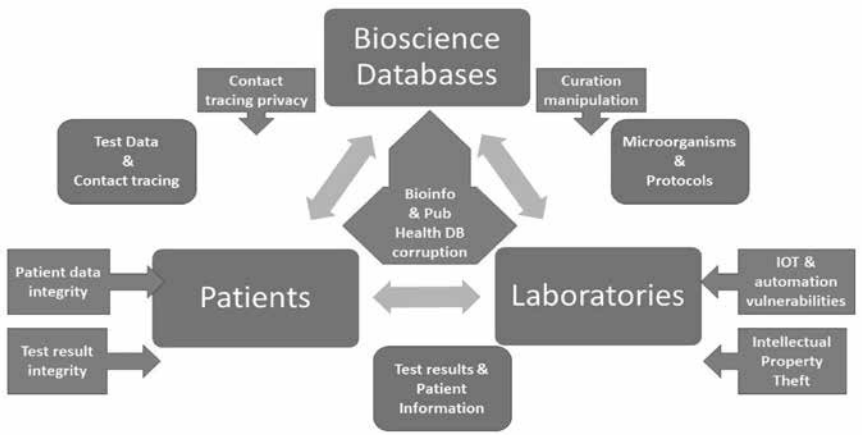

Figure 2 Cyber-Biosecurity threats related to Surveillance & Management of Infectious diseases

The Cyber-Biosecurity challenges to public health management of infectious disease such as COVID-19 include:

1. Privacy of contact tracing data
2. Integrity of public health and disease surveillance data
3. Data integrity of self-administered testing
4. Integrity of public bioinformatics databases
5. Integrity of laboratory automation
6. Protection of intellectual property

Synthetic Biology and DNA databases

There are several large global genomic databases which are relatively more accessible to scientists as open source databases for their fundamental scientific research within the research institutions, or for their commercial purposes in the industries. The integrity and confidentiality of these genomic databases may be compromised for either malicious purposes of weaponisation, or intellectual property theft for commercial exploitation by rival industries by luring insider scientists.

What is Genomic Data?

A genome (one may call it a 'software') of a living organism (bacteria, viruses, plants, animals or humans) contains entirely mapped genetic information which controls the features or behaviour in the form of deoxyribonucleic acid (DNA) or ribonucleic acid (RNA). Entire genome sequencing and mapping functional capabilities along with the advances in Synthetic Biology tools like CRISPR-CAS9, have enabled scientists to edit and engineer the genomic data of living organisms and resurrect and reconstruct extinct or novel organisms.

The DNA-database related threat landscape may be further sub-divided into three categories and potential National Security risks, as genomic data of pathogens, human and industrial genomic data.

Genomic Data of Pathogens

In 2002, a team of scientists, enthused with the success of synthetically recreating a live Polio virus, using genomic sequences and research data available on the internet, started planning to recreate Ebola, small pox and 1918-Influenza pandemic viruses from scratch.[15]

The digitization of biology has made genome editing and synthetic biology tools such as CRISPR-Cas9 more accessible, predictable and cost effective. First bacteria with a synthetically digitized genome from scratch was born in 2010. The need to have a physical sample of DNA to study or edit a DNA has become redundant since then, allowing scientists working with computer-aided designs and bioinformatics modelling tools to manipulate or rewrite entire genomes of interest.

Over the years, the methods of whole genome sequencing are preferred to single gene, or DNA fingerprinting methods; for detection, identification, surveillance and tracking of pathogens. While these whole-genome based methods are becoming increasingly cost effective, accessible and having distinct advantages over the previous methods; the increased reliance on public pathogen

genomic databases has made them more vulnerable to cyberattacks by illegal access, manipulation of data and taking the data base hostage.[16]

The entire genomic research knowledge generated across the globe over the decades stored within these public genome databases, is an ideal data resource for anticipating potential risks for Cyber-Biosecurity as well as potential targets for such cyberattacks.

The two largest genomic data repositories hosting most, if not all, molecular sequence data are hosted by the National Center for Biotechnology Information (NCBI) at the National Institutes of Health (NIH) in the United States, and genome databases hosted at the European Molecular Biology Laboratory (EMBL). The Joint Genome Institute (JGI) has developed three platform projects, with unique and important features for functional analysis of microbial genomes, with the support of Department of Energy (United States):

1. The integrated genome and metagenome comparative data analysis system (IMG/M): A database containing tools to annotate microbial genomes and metagenomes.
2. MycoCosm: A web portal that hosts fungal genome data.
3. Genomes OnLine Database (GOLD): A database that manages metadata and raw data for genome and metagenome sequencing

Human Genomic Data

Mapping of human genome enabled better understanding of many chronic health conditions and helped the scientists to develop targeted therapies and personalised medicine for patients. Policymakers across the world were relatively unaware of the threats posed by the genomic knowledge of disease pathways, vulnerabilities to chronic illnesses and infectious diseases. Adversary nations can potentially exploit such knowledge of such vulnerabilities of specific races, genetic groups, genders or food habits to develop targeted bioweapons. The national security experts of many nations have raised concerns regarding China's collection of largest global genomic databases across the world,[17] along with 'All-of-the-Nation' approach to AI, that makes them a formidable competitor in this domain. Aware of the potential up-side of leading the global Bio-revolution, China has been collecting genomic datasets at Beijing Genomic Institute (BGI) via research collaboration, investing in and taking over genomic sequencing companies in the US.[18] Big data computing and analytics along with the knowledge of molecular pathways of certain genetic vulnerabilities, potentially facilitate the targeted attacks for genocide by the adversaries.

Tailoring infectious-disease-agent based bio-weapons for specific ethnicities is not exactly easy. However, a sophisticated adversary state equipped with a capability to hack or bypass cybersecurity barriers to access genomic data, health metadata and bioinformatics, may develop bio-weapons targeted towards the specific vulnerabilities of the subpopulations. For example, retroviruses, which are known to integrate with the host genome upon infection, could be gene-edited to target one subpopulation over the other using techniques like high-throughput screening, directed evolution and computer modeling to fine-tune the targeted Bio-weapon. It is feared that it may be further fine-tuned to develop 'Personalized Bioterrorism'.[19]

The Indian population of 1.3 billion has a peculiar genetic diversity with distinct variations and disease-causing mutations. Other nations such as the United States, China and the United Kingdom have their own genomic databases of their populations. However, these research findings cannot be extrapolated to Indian population with distinct diversity. The Genome India project to sequence Indian Human genome and create a database has promise to fulfill this gap by for furthering critical research on population-based or disease-based human genetic research for Indian population.[20] However, the concerned authorities need to be vigilant with respect to the Cyber-Biosecurity threats to these databases with the National Security perspective.

Industrial Genomic Data

Bio-pharmaceutical and bio-engineering industries develop and possess their own genomic databases that are utilised for lucrative and competitive proprietary manufacturing activities related to human and animal health, drug discovery, vaccines, food security and bio-fuels that fuels the growth of bio-economy of the nation. Cyberattacks on such industrial genomic databases may be motivated to steal intellectual property to gain competitive commercial advantage, or to sabotage either a critical infrastructure or the bio-economy.

The cyber-attacks enabled by email-phishing or malware to gain access to a secure facility, are motivated to disrupt ongoing research, steal technology knowhow, genetic modification of virus, bacteria or therapeutics like vaccines, without the knowledge of the targeted public or private research facility.

Malware in the DNA

The digitization of biology refers not only to facilitation of scientific research and bio-industrial production but also to utilization of biological

information on computing platforms, incorporated in databases, analyzed using software and shared via email. A DNA is digitized by converting its subunits (known as amino acids) denoted as A, T, G and C into ones and zeros that can be read by a computer. This technique of digitization of DNA may be utilized both ways; either to create a digital sequence of a physical DNA, that may be stored in a digital database and shared online; or for translating the genetic information on the digital database for physical de novo gene synthesis to create a living organism in a lab. This process of digitization of genomic data has revolutionized the genomic research, as the scientists can easily store, share, generate and analyze the data. However, that has made the genomic data equally vulnerable to all cyberattacks inherent to digital world.[21]

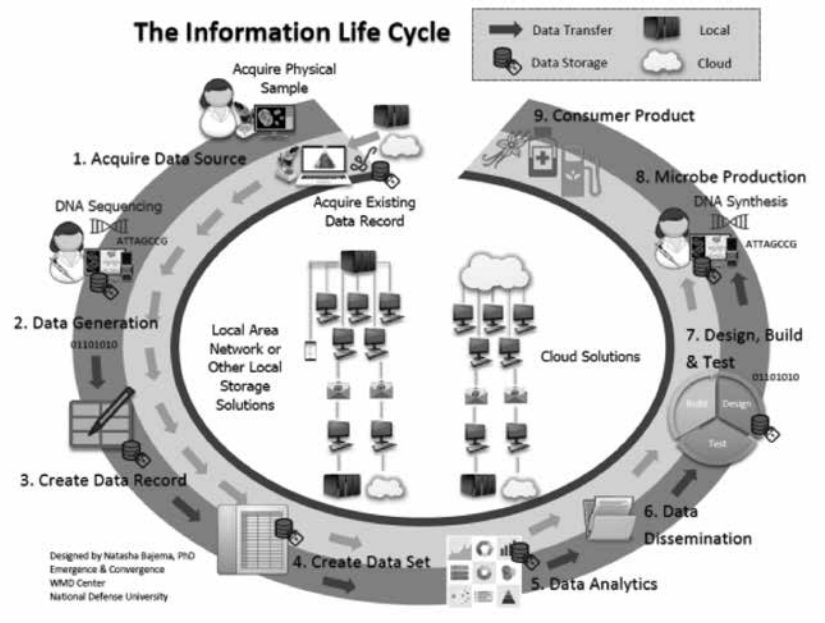

Figure 3 Information life cycle of genomic data

This comprehensively discussed diagram by Bajema et al. (Figure 1)[22] illustrates the information lifecycle of genomic data, composed of two pathways; one indicating the acquisition of physical sample (dark grey) and the other acquiring an existing digital genomic data, as well

as many touch points along the bio-industrial production or scientific research pathways. These touch-points along these pathways indicate the vulnerabilities to a variety of risks including human errors, accidental release, unauthorized access, theft, sabotage or cyber-hacking of the genomic data.[22]

This bio-informational life cycle consists of:

- *Sample acquisition*: Scientists acquire physical DNA sample for sequencing from either the field as living organisms, by requesting other researchers or ordering the samples from American Type Culture Collection (ATCC), a bio-resources repository for microorganisms and cell lines.
- *Gene Sequencing*: The gene sequencing is done to create a digital record of the sample by converting the amino acid sequence (A, T, G & C) into ones and zeros, the scientists use in-house sequencing facilities or send the sample for sequencing to companies providing such services.
- *Gene sequence and Metadata*: Scientists and the research institutions create individual data storages of gene sequences of physical samples or may choose to store these records to online databases. Each record contains the raw genetic sequence and its metadata (sample description, name of the organism, specific strain and source of the sample etc.).
- *Data Storage*: Large research organisations process many samples leading to multitude of datasets. The institutions may store such large datasets either on services provided by commercial bioinformatics platforms or cloud services such as Microsoft, Amazon and Google, or prefer to store in-house servers within the LAN networks without the internet access. These decisions are usually governed by the factors such as the sensitivity of the database, need to share the datasets over the internet and in-house storage capacity. The cloud service providers allow the users to control access to their databases and share selective access to scientists from larger scientific community and students.
- *Product Development*: The customized product development and manufacturing of the end products of such industries involves engineering principles of 'Design-Build-Test' by tweaking of the genomes and large scale manufacturing using automation. The increased use of remote automation for efficient monitoring of production cycles, involves large computer and communication networks, sometimes accessible over the internet.

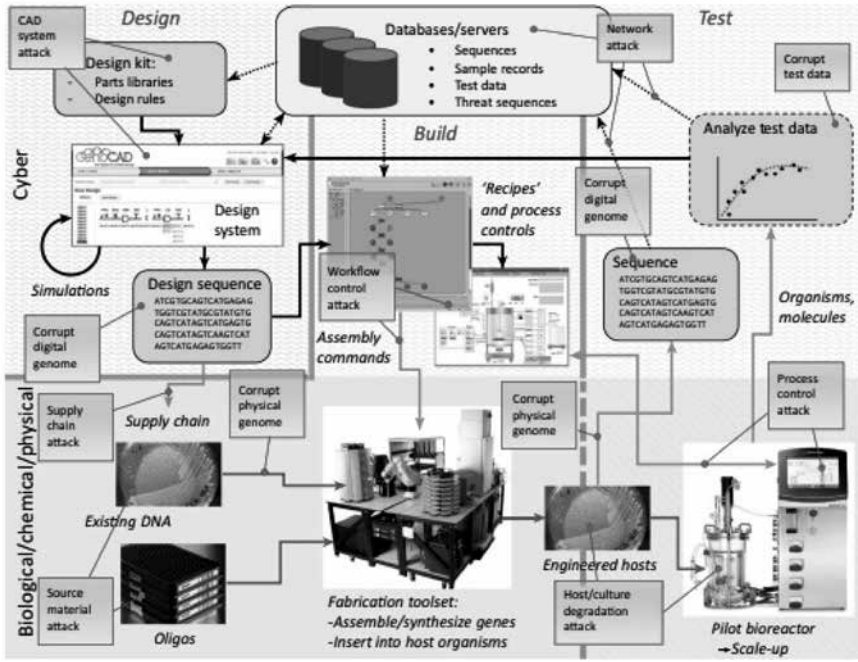

Figure 4 Cyber-Physical Bio-manufacturing process

The many touch points along the Cyber-Physical Bio-manufacturing process and scientific research pathways as described by Peccoud et al. (2018) are illustrated in Figure 4.[23]

These examples elaborate the fundamental difference between cyber-physical attack (which may result in, for example, crashing of a drone) and cyber-biological attack, (utilising a DNA as an executable code in a non-digital environment) has a potential to subvert a DNA sequencing machine, propagating the malicious code back into the cyberspace. A comprehensive overview of the associated risks for variety of genomic data as discussed by Bajema et al. is tabulated in Table 1.[22] This comparative analysis of associated risks for all three categories of databases serves as a one-page summary for quick reference.

Table 1 Risks associated with genomic data

The Risks of Genomic Data	Pathogen	Human	Industrial
Capability risks			
Obtaining genomic data to harm	Y	Y	Y
Using genomic data to engineer pathogens	Y	Y	Y
Using genomic data to recreate extinct, high impact pathogens	Y	N	N
Using genomic data to modify low-risk pathogens to become high-impact	Y	Y	Y
Using genomic data to increase the likelihood of disease	Y	Y	N
Using genomic data to enhance targeting of the recipient	Y	Y	N
Using genomic data to enhance pathogens	Y	Y	Y
Data Risks			
Creating inaccurate data through machine or human error	Y	Y	Y
Finding ways to consistently catch and fix inaccurate data	Y	Y	Y
Prioritizing data storage as storage space diminishes (data loss)	Y	Y	Y
Cybersecurity risks			
Transferring data securely to the correct end users	Y	Y	Y
Accessing proprietary of high-risk information without authorization	Y	Y	Y
Editing data deliberately to be incorrect	Y	Y	Y
Stealing proprietary or high-risk data	Y	Y	Y
Stealing proprietary tools to analyse datasets	Y	Y	Y
Societal risks of Privacy and Discrimination		Y	Y
Releasing human genomic data unintentionally	N	Y	N
Releasing human genomic data intentionally	N	Y	N
Engaging in discriminatory practices	N	Y	N

Y - Applies to this type of genomic data
N - Doesn't apply to this type of genomic data

Cyber-Biosecurity of Life Sciences Research Infrastructure

Last two decades have witnessed digital transformation of Life Sciences laboratories including academic, scientific research, industrial biotechnology, molecular biology and bio-pharmaceutical innovation laboratories. Digitalisation of laboratory equipment, cloud-based software, interconnected devices and networks involving efficient workflows and automation, scientific collaborations involving cloud-based databases have not only resulted in explosive growth of technological innovations but also created millions of internet access touch points or nodes for cyber-hackers to exploit for various malicious objectives discussed above.

India's Bio-economy

As evidenced during the recent COVID-19 pandemic, the Government of India's pandemic response has been enabled by the emerging BioEconomy, which provides core biosecurity capabilities that are essential to the success of the mission. The government's engagement with the BioEconomy has grown in recent years, encompassing a range of agencies with a focus on laboratory and product safety and an emphasis on supporting research and development (R&D). However, there are no existing mechanisms to partner with the BioEconomy for providing a broader strategic focus that integrates priorities, including biosecurity and biodefence.

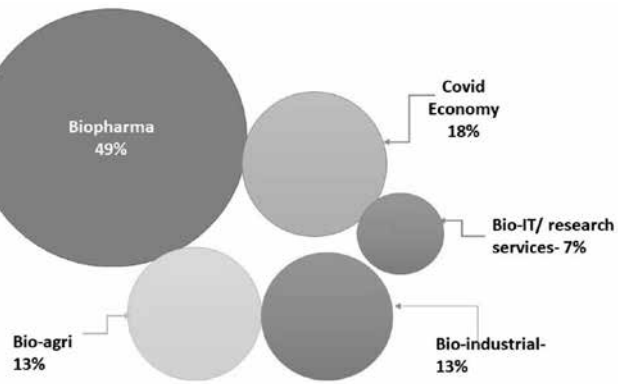

Figure 5 Indian Bio-economy 2021

Amidst the raging COVID-19 pandemic, 2021 has been a remarkable year for India's BioEconomy in spite of lockdowns and other disruptions.

The Indian biotechnology industry has been the pole-bearer by developing and deploying a variety of tools such as vaccines, anti-virals, diagnostic tests. In this remarkable year the BioEconomy grew at 14.1 per cent from US$ 70.2 billion to US$ 80.12 billion in 2021 with BioPharma segment accounting the largest share of 49 per cent.

India's robust Bio-economy is growing rapidly and is estimated to reach US$ 300 billion by year 2030. [23]

Cyber-Biosecurity Threats and Impact on Bio-Economy

The focus to protect the Indian BioEconomy against the Cyber-Biosecurity threats, is missing due to the lack of awareness regarding the extent and severity of the potential impact. The critical manufacturing industries are key drivers of the growth of Bio-economy, including high-value and capital-intensive industries that are manufacturing life-saving bio-pharmaceutical products such as drugs, monoclonal antibodies, vaccines and other biologicals. These key drivers of the Bio-economy have become soft targets across the globe for cyber-attacks such as sabotage, corporate espionage and cybercrimes for extortion. All forms of attacks impact the manufacturing industries, governments, health infrastructure, patients and Bio-economy at large.

In 2017, one of the world's largest bio-pharmaceutical company, Merck was attacked with a modified form of worm known as NotPetya, resulting in permanent encryption of data. It affected the manufacturing control networks of Merck, resulting in severe shortages of Gardasil and Hepatitis B vaccine. The total financial impact of this cyberattack was close to US$ 1 billion to Merck, including Merck's borrowing of Gardasil from US Center for Disease Control stockpiles worth US$ 240 million.[24] Similar attacks on Roche and Bayer using Winti malware, attributed to hackers based in China, were detected early and without any sensitive information being stolen. These incidences highlight the probable risks involved in deliberate, tailored and coordinated synchronized attacks on critical infrastructures and their potential to not only disrupt the Bio-economy but also the health security of a nation.

A 2022 report of CloudSEK on cyberattacks reveals that the number of such cyberattacks against the global healthcare industries has increased by 95.34 per cent in the first four months of 2022.[25]

India recorded the second highest (7.7%) of total attacks on the healthcare industries, in the previous year, 2021. The year 2021 also witnessed

couple of internet posts selling vaccination records of 150 million Indian citizens. Though many cybersecurity experts believed it to be a scam, such incidences highlight the interest of the state- or non-state hackers to harm and compromise the healthcare industry data.

As reported by cyber intelligence firm Cyfirma, a Chinese state-backed hacking group APT10, also known as Stone Panda cyber-attacked India's two premier vaccine manufacturers Serum Institute of India (SII) and Bharat Biotech supplying COVID-19 vaccines for India's vaccination campaign. With a primary objective of intellectual property exfiltration to gain competitive advantage, APT10 attacked SII, which had weak and vulnerable web servers.[26]

While highlighting the vulnerabilities, another report by Indusface for the year 2022 revealed that 2,78,000 cyberattacks in Indian healthcare industry were reported every month. According to a statement by CEO of Indusface,

> Lack of risk awareness, use of legacy technologies by healthcare companies, and massive traffic loads make the Indian healthcare segment highly vulnerable to cyber-attacks. Attacks were primarily done using brute force. Now hackers are deploying surgical methods such as bots to first find vulnerabilities and then spread Ransomware. This problem will only get exacerbated when there's the full-fledged deployment of public APIs. While this integration is already in place for payment gateways, going forward, healthcare providers will open up more possibilities through integrations with diagnostic service providers, telehealth providers, and so on. This necessitates urgent deployment of advanced VAPT and WAF solutions that prevent cyber-attacks against web applications and APIs.[27]

As reported by Cyfirma, a Singapore based threat intelligence firm, cyberattacks on Serum Institute, Bharat Biotech, Dr Reddy's Labs, Abbot India, Patanjali and AIIMS were part of 15 active hacking campaigns. According to Cyfirma statement, "Our research showed the suspected threat actors were mainly sponsored by China, Pakistan and North Korea. The hackers' objectives were centered around smearing India's reputation, cause productivity loss, create operational damage and seek financial gains," [28] The campaign "UnwPock" was launched to steal intellectual property, medical devices, medicine chemical combination, sensitive database and customer information along with other campaign "unseco33" with objectives such as to steal sensitive personal, clinical trial information, health care report and customer information. The third campaign "PuM4Y" was launched by targeting Patanjali to steal sensitive medical database.[11] A ransomware attack

on one of the leading global pharmaceutical giant Sun Pharmaceuticals, that sells pharmaceutical products in more than 100 countries with a revenue of US$ 5 billion in 2022 and has more than 37,000 employees, shocked the industry highlighting the vulnerabilities of this industry sector handling sensitive data and critical supply chain delivery models and the severe consequences of any such cybersecurity breaches. Though the total impact is yet unknown, this attack on Sun Pharma has impacted its operations with anticipated drop in revenues.[29] Indian large pharma companies such as Arati Drugs and IPCA Labs, too fell prey to cyber-attacks. However, according to cyber-experts in spite of persistent cyber-attacks Indian healthcare industry awareness and preparedness is minimal and even after security audits the vulnerabilities reported remain unpatched.[30]

There is a significant contribution of innovations facilitated by the tools of emerging technologies such as industrial and research laboratory automation, synthetic biology, and databases in genomics which is pivotal to the growth of Indian BioEconomy. Similarly, bilateral and multilateral collaborations with industrial partners from the developed economies, increased exchange of technology and human capital, FDI investments in cutting-edge technologies for creation of intellectual property and infrastructure are crucial for the robust growth of Indian BioEconomy. As evidenced by large scale and persistent cyberattacks on Indian BioEconomy for research and industrial data, intellectual property thefts and impact on industry operations and revenues, comprehensive and robust Cyber-Biosecurity measures are imperative to build investor confidence and invigorate the Indian BioEconomy.

Regulatory and Legal challenges

The genetically modified organisms (GMOs) and the products thereof are regulated in India under the "Rules for the manufacture, use, import, export & storage of hazardous microorganisms, genetically engineered organisms or cells, 1989", notified under the Environment (Protection) Act, 1986. These rules are very broad in scope essentially covering entire spectrum of activities involving GMOs and products thereof. However, in absence of any clarity on how the emerging technologies will be dealt in India, the definition of modern biotechnology according to the Cartagena Protocol on Biosafety is yet to be incorporated in the national regulations.

India has neither an exclusive biosecurity law nor an exclusive cybersecurity law, though sector specific regulations exist within both the domains. There are numerous laws, regulations, frameworks, Standard Operating Procedures and

guidelines for contained research, biologics, confined field trials, food safety assessment, environmental risk assessment, cybersecurity (such as IT Act 2021) and Biosecurity. The National Cybersecurity Policy 2013 released by Department of Electronics and Information Technology, and National Information Security Policy and Guidelines have been issued by Ministry of Home Affairs with an aim to prevent cyber intrusions. However, the rapid convergence of dual use emerging technologies, along with the all-pervasive Cyber-Biosecurity threats with their potential to disrupt the wellbeing of citizens and national security, Cyber-Biosecurity domain needs to be regulated after comprehensive review of the entire legal framework. Various stakeholder ministries, governmental agencies and the legislative bodies responsible for implementing laws need to work together to design frameworks to reduce Cyber-Biosecurity challenges.[31]

Hopefully, this need to address Cyber-Biosecurity threats will be answered by the National Cyber Security Strategy 2020 with a goal to serve as the official guidance for stakeholders, policymakers and corporate leaders to prevent cyber threats, cyber terrorism and espionage in cyber space.

Similarly, international disarmament and non-proliferation regime, the Biological Weapons Convention (BWC) is already ineffective in absence better implementation tools; as exemplified by Chemical Weapons Convention, such as an executing authority, a scientific advisory board and a verification regime. The BWC needs additional reforms to answer the challenges posed by these convergent emerging technology threats.

National Security Implications

Global internet accessibility and online availability of biotechnology and synthetic biology tools have lowered the barriers to develop, access and acquire Bio-weapons, making those attractive propositions for non-state, state-sponsored and state- actors. Similarly, cyber tools to compromise critical bio-industrial assets have the potential to compromise National Security infrastructure.

The COVID-19 pandemic, the related health costs of the pandemic, along with the cybersecurity threats to critical health infrastructure and supply chains have impacted the economic, social and political wellbeing of all the nations. Awareness and training of scientific community to understand and appreciate the national security implications of such cyber-attacks is necessary for anticipating the threats and preparation of strategies for preventing attacks on scientific research, healthcare and bio-industry considering the sensitive and competitive nature of dual use biotechnologies.

Previous section of the Cyber-Biosecurity threat landscape described a variety of cyber-attacks on critical health infrastructure, digital and health infrastructure, surveillance and management of infectious diseases, DNA databases and Malware via DNA, research and manufacturing infrastructure with various objectives such as to demand ransom, to steal intellectual property to gain competitive research or commercial advantage, or to sabotage either a critical infrastructure or the bio-economy. Adversary nation states or non-state actors potentially may utilize such cyber-attacks with severe national security implications for India. Such coordinated cyber-attacks on critical health infrastructure may happen concurrent with other national security challenges such as conflicts on the border.

Some hypothetical attack scenarios may be utilized for creating awareness to endorse the need for such awareness and training programs and the national security implications of the same.

Malware in a strand of DNA

The disruptive nature of cyber-physical nature of attacks is exemplified by an experimental attack in 2017 designed by Washington University scientists. When an experimental DNA strand incorporated with malware was sent for processing to a DNA sequencer, the malware activated and the team of scientists sending the sample took over the computer of the DNA sequence analyzer.[32] This ability to hack and weaponise any DNA sequence stored on any computer forced the US Intelligence agencies to incorporate Cybersecurity threats to genome editing to the lists of threats to the national security.[33]

Another hypothetical scenario of a bioterror attack in a critical lab is described by Greenbaum (2021) in which a hacker, Alice hacks a DNA sequence order placed by a genuine researcher, Bob to a genetic sequencing company of Charles. In spite of Charles diligently following universally accepted standard operating procedures to inspect the ordered DNA strand, Alice's cleverly designed malicious DNA strand using standard cyber-hacking tools, by-passes the screening. Bob, unaware of this remote manipulation of his DNA, receives his order and employs the malicious DNA for his experiments, potentially ruining the experiment or worse resulting in a bioterror attack due to resulting toxic protein.[34] Unfortunately, most communication by the scientists with gene synthesis companies comprising of placing and tracking of the orders, occurs through the email or company website, which in case of an attack are already controlled by the hacker.[35]

An adversary nation may potentially cause a remotely manipulated laboratory outbreak by leakage of a highly infectious bio-agent in a low-containment laboratory to push it in a politically inconvenient situation.

Cybernetics and Biosecurity

Along with long history of aerial deployment and testing bio-weapons, the cybernetics has opened up a new Pandora's box of drone swarms and autonomous drones capable of deploying modern made-to-order synthetic bio-weapons.[36] This has added a whole new aerial dimension to the Cyber-Biosecurity threat landscape. For example, dual use of drone technology with tremendous applications for precision agriculture also involves potential use of autonomous drone swarms for precision bioterrorism attacks.[34]

Food and Agriculture

Agriculture processing, food processing, dairy, poultry and related supply chains are part of critical components of a nation's food security and are probable targets for disruption. There is increasing appeal of blockchain technology in the agricultural sector for having a sustainable business, enhancing supply chain efficiency, reduction of waste, informed consumer purchasing decisions and smooth future transactions with fraud elimination.[37] Such smart technologies and automation has been increasingly used in agriculture, food production and processing industries. In order to secure the supply chains, Cyber-Biosecurity threats have been recognized by the security experts to mitigate any crippling effects on the food security of the nations.[38]

Bio-veillance and Cyber-Biosecurity

While defending the use of term Cyber-Biosecurity (or Biocybersecurity according to the context) instead of simply referring as 'Cybersecurity in the Healthcare Sector', Palmer et al.[39] emphasize the importance of increasing role of biology along with the complexities of challenges, and the need of centering the discussion on the intersection of cybersecurity, cyber-physical security and biosecurity.[39]

International discussions by scientific and security agencies continue to promote the concept as defined by Hester et al. as of Bio-veillance. Considering the novel security threat landscape arising out the Cyber- Bio interface, it is increasingly advocated to institutionalize the techno-security infrastructure for pre-emptively managing and securing the biological information with a potential for nefarious use.[40]

Defending Forward

Several Western nations including France and Germany apparently have adopted an offensive approach with increasing activities of international actors such as 'Paris Call for Trust and Cybersecurity'; along with France initiating a 'Paris Call' doctrine and Germany's new cyber defense strategy along with components of offensive operations. Described as 'Defending Forward' the US stance has shifted from defensive to offensive as elaborated in the US Department of Defence Cyber Strategy 2018, that states, 'will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict.' There are three components of this cybersecurity strategy:[40]

1. positioning to degrade cyber operations;
2. warning to gather information about threats and inform defenses; and
3. influencing adversaries to discourage them from deploying cyber operations against the United States.

This apparent trend reflects in the US Department of Defense Cyber Strategy 2019 with concept of 'persistent engagements' and 'Defend Forward'.[41]

While acknowledging these strategic changes as indicators of ongoing conflicts in the cyberspace, Palmer et al, advocate that Cyber-Biosecurity needs to be considered as an essential component of the US cybersecurity doctrine within the Defending Forward Framework![42] These recommendations are expected to shape future US cyber policy developments.

In a hard-hitting argument, advocating the inclusion of Cyber-Biosecurity to Rwanda's national deterrence policy or Defend Forward initiative to counter threats from neighboring or faraway nation states, apparently the most practiced deterrence policy at this time, Samori et al. have emphasized that, countries need to have adequate Cyber-Biosecurity infrastructure and policy in place before the biological equivalent of Metasploit becomes commonplace.[43]

Conclusion

Though the convergent emerging technologies have complicated the Cyber-Biosecurity related threats, these challenges are not insurmountable. The regulatory policy-makers, equipment manufacturers and end users need to respect, value and protect their data with the inherent threat perspective in mind.

A culture that fosters innovation through secure, regulated and transparent ecosystem has the potential to strengthen and flourish the Indian BioEconomy. There is a need to create a secure ecosystem in India facilitated by comprehensive analysis of the entire BioEconomy with respect to the Biosecurity and Cyber-Biosecurity landscape, SWOT analyses of existing legal and regulatory provisions, reinforcements with legal and constitutional amendments as necessary, and effective response networks are required. Such a robust ecosystem has a potential to build FDI investor confidence to propel Indian BioEconomy further by investing in high-risk cutting-edge technologies. The FDI investors are always looking for high-growth opportunities with a potential to create intellectual property that promises long-term economic benefits in a robust BioEconomy, which is well-regulated and protected against Cyber-Biosecurity risks.

Various stakeholder ministries, governmental agencies and the legislative bodies responsible for implementing laws need to work together to design frameworks to reduce Cyber-Biosecurity challenges. With the approach of training and awareness to identify and mitigate the threats, the Cyber-Biosecurity vulnerabilities can be minimized to the benefit of bio-economy, scientific institutions and national security. To effectively address this emerging challenge, the policymakers need to formalize a collaborated approach with emerging technology experts across all the disciplines to develop regulatory frameworks to anticipate, detect and mitigate Cyber-Biosecurity threats. National Cyber Security Strategy is currently undergoing review process. On the same lines, National Biosecurity Strategy needs to be formulated with a joint annexure on Cyber-Biosecurity Strategy.

There is an urgent need to appreciate the entire Cyber-Biosecurity threat landscape from the Indian National Security perspective, especially considering the not-so-covert conflict ongoing in the cyberspace, and has a probability of boiling over to the Cyber-Biosecurity landscape.

Notes

1. Mrinmayee Bhushan, 'Plausible Deniability & Proliferation of Bio-Weapons: The Elephant in The Room', *CBW Magazine*, January–June 2022, available at https://www.idsa.in/system/files/page/2015/cbw-winter-jan-jun-2022.pdf
2. R.S. Murch, W.K. So, W.G. Buchholz, S. Raman and J. Peccoud, 'Cyber-Biosecurity: An Emerging New Discipline to Help Safeguard the Bioeconomy', *Front. Bioeng. Biotechnol.*, Vol. 6, 2018.

3. *L.C.* Richardson, N.D. Connell, S.M. Lewis, E. Pauwels and R.S. Murch, 'Cyber-Biosecurity: A Call for Cooperation in a New Threat Landscape', *Front. Bioeng*, available at https://www.frontiersin.org/articles/10.3389/fbioe.2019.00099.
4. M. Popovic, *Biomechanics and Robotics*, 2013, doi:10.4032/9789814411387, available at https://www.researchgate.net/publication/258918397_Biomechanics_and_Robotics
5. 'FDA recalls close to half-a-million pacemakers over hacking fears', *Engadget*, available at https://www.engadget.com/2017-08-31-fda-pacemakers-abbott-hacking.html.
6. 'Advanced Threat Research Report', October 2021, available athttps://www.trellix.com/en-us/assets/threat-reports/trelllix-threat-report-oct-2021.pdf.
7. 'AIIMS Delhi turns manual following ransomware attack', Healthcare IT News, 2022, available at https://www.healthcareitnews.com/news/asia/aiims-delhi-turns-manual-following-ransomware-attack; 'After AIIMS Delhi, hacking attempts on Indian Council of Medical Research's server', *India Today, available at* https://www.indiatoday.in/india/story/6000-hacking-attempts-aiims-indian-council-of-medical-research-server-november-30-2305972-2022-12-06.
8. 'Cyber Attack Derails AIIMS Delhi Services: How Data of Patients is in Danger', *Outlook*, 2022, available at https://www.outlookindia.com/ https://www.outlookindia.com/business/aiims-ransomware-attack-cyber-attack-derails-aiims-delhi-services-how-data-of-patients-is-in-danger-news-241071.
9. G.T. Bharat, 'Technology transformation for future-ready healthcare', available at https://www.grantthornton.in/globalassets/1.-member-firms/india/assets/pdfs/technology-transformation-for-future-ready-healthcare-gt-ahpi-13-feb.pdf.
10. 'Connected Healthcare: A Cybersecurity Battlefield We Must Win', available at https://www.trellix.com/en-us/about/newsroom/stories/research/connected-healthcare-a-cybersecurity-battlefield-we-must-win.html.
11. M. Elgabry, 'Towards cyber-biosecurity by design: an experimental approach to Internet-of-Medical-Things design and development', *Crime Sci.*, Vol. 12, No. 3, 2023, available at https://doi.org/10.1186/s40163-023-00181-8.
12. D. Greenbaum, 'Cyber-Biosecurity: An Emerging Field that has Ethical Implications for Clinical Neuroscience', *Camb. Q. Healthc. Ethics*, Vol. 30, 2021, pp. 662–68.
13. *X.L.* Palmer, L. Potter and S. Karahan, 'An Exploration on APTs in Biocybersecurity and Cyber-Biosecurity', *Int. Conf. Cyber Warf. Secur.*, Vol. 17, 2022, pp. 532–35, available athttps://papers.academic-conferences.org/index.php/iccws/article/view/67.
14. A. Adler, J. Beal, M. Lancaster and D. Wyschogrod, 'Cyber-Biosecurity and Public Health in the Age of COVID-19', in B.D. Trump, M.V. Florin, E. Perkins and I. Linkov (eds), *Emerging Threats of Synthetic Biology and Biotechnology* (pp. 103–115), Springer Netherlands, 2021, DOI:10.1007/978-94-024-2086-9_7.
15. 'Ebola virus could be synthesised', *New Scientist*, available at https://www.newscientist.com/article/dn2555-ebola-virus-could-be-synthesised/.
16. B.A. Vinatzer et al., 'Cyber-Biosecurity Challenges of Pathogen Genome Databases', *Front. Bioeng. Biotechnol.*, Vol. 7, 2019, available at https://www.frontiersin.org/articles/10.3389/fbioe.2019.00106.

17. 'U.S. Intelligence Community Warns About China Collecting Healthcare Data', *Digital Guardian*, available at https://www.digitalguardian.com/blog/us-intelligence-community-warns-about-china-collecting-healthcare-data.
18. P.F. Walsh et al., *Threats, Risks and Vulnerabilities at the Intersection of Digital, Bio and Health*, 2021, DOI:10.13140/RG.2.2.28130.20163, available at https://www.researchgate.net/publication/352478030_Threats_Risks_and_Vulnerabilities_At_the_Intersection_of_Digital_Bio_and_Health.
19. *Biodefense in the Age of Synthetic Biology*, National Academies Press, 2018, p. 92, DOI:10.17226/24890.
20. '10,000 Indian genomes to be sequenced by year-end', The Hindu, available athttps://www.thehindu.com/news/national/10000-indian-genomes-to-be-sequenced-by-year-end/article66710592.ece.
21. A. Greenberg, 'Biohackers Encoded Malware in a Strand of DNA', *Wired*, available at https://www.wired.com/story/malware-dna-hack/.
22. N.E. Bajema, D. DiEuliis, C. Lutes and Y.B. Lim, 'The Digitization of Biology: Understanding the New Risks and Implications for Governance', 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.
23. 'BIRAC (DBT) Report on India BioEconomy 2022', available at https://birac.nic.in/webcontent/1658318307_India_Bioeconomy_Report_2022.pdf.
24. D. Guttieres, S. Stewart, J. Wolfrum and S.L. Springs, 'Cyber-Biosecurity in Advanced Manufacturing Models', *Front. Bioeng. Biotechnol.*, Vol. 7, 2019, available at https://www.frontiersin.org/articles/10.3389/fbioe.2019.00210.
25. A. Mittal, H. Saxena and I.Tripathi, 'Increased Cyber Attacks on the Global Healthcare Sector', available at https://uploads-ssl.webflow.com/635e632477408d12d1811a64/63cfd7034745927b1c74ca2a_Increased-Cyber-Attacks-on-the-Global-Healthcare-Sector-WhitePaper-CloudSEK%20(1).pdf.
26. 'Chinese state-backed hackers attack Serum Institute, Bharat Biotech: cybersecurity firm', *Business Today*, available at https://www.businesstoday.in/technology/news/story/chinese-state-backed-hackers-attack-serum-institute-bharat-biotech-cybersecurity-firm-289629-2021-03-01.
27. 'India's healthcare industry targeted by more than 2,78,000 cyberattacks every month', Indusface report, available at https://www.financialexpress.com/healthcare/healthtech/indias-healthcare-industry-targeted-by-more-than-278000-cyber-attacks-every-month-indusface-report/2841384/.
28. 'Indian pharma companies and hospitals targeted by Chinese, Russian and Korean hackers groups', Mint, available at https://www.livemint.com/technology/tech-news/indian-pharma-companies-and-hospitals-targeted-by-chinese-russian-and-korean-hackers-groups-11614618146968.html.

29. 'Sun Pharma warns of a dip in revenue after a ransomware attack', Business Today, available at https://www.businesstoday.in/technology/story/sun-pharma-warns-of-a-dip-in-revenue-after-a-ransomware-attack-374943-2023-03-27.
30. 'After Ipca Laboratories, pharma major Aarti Drugs hit by ransomware attack; data leaked on dark web', available at https://ciso.economictimes.indiatimes.com/news/after-ipca-laboratories-pharma-major-aarti-drugs-hit-by-ransomware-attack-data-leaked-on-dark-web/94913796.
31. 'Mapping the Cyber-Biosecurity Enterprise', Frontiers Research Topic, available at https://www.frontiersin.org/research-topics/8353/mapping-the-Cyber-Biosecurity-enterprise#articles.
32. 'Researchers are sounding the alarm on Cyber-Biosecurity', available at https://www.c4isrnet.com/dod/2018/02/08/researchers-are-sounding-the-alarm-on-Cyber-Biosecurity/.
33. A. Greenberg, 'Biohackers Encoded Malware in a Strand of DNA', Wired, available at https://www.wired.com/story/malware-dna-hack/.
34. D. Greenbaum, 'Cyberbiosecurity: An Emerging Field that has Ethical Implications for Clinical Neuroscience', *Camb. Q. Healthc. Ethics*, Vol. 30, 2021, pp. 662–68.
35. D. Farbiash, and R. Puzis, 'Cyber-Biosecurity: DNA Injection Attack in Synthetic Biology', 2020, available at https://doi.org/10.48550/arXiv.2011.14224.
36. M. Bhushan, 'Biological and Chemical Threats and UAV Delivery Systems: A Lethal Combination', *Journal of Defence Studies*, Vol. 16, No. 4, available at https://www.idsa.in/system/files/jds/jds-16-4_Mrinmayee-Bhushan_10.pdf.
37. 'How Blockchain Benefits Agriculture and Food Industry in Future?', available at https://appinventiv.com/blog/blockchain-in-agriculture-and-food-sector/.
38. T. Drape et al., 'Assessing the Role of Cyber-Biosecurity in Agriculture: A Case Study', Front. Bioeng. Biotechnol., Vol. 9, 2021, available at https://www.frontiersin.org/articles/10.3389/fbioe.2021.737927.
39. R.J. Hester, 'Bioveillance: A Techno-security Infrastructure to Preempt the Dangers of Informationalised Biology', Sci. Cult., Vol. 29, 2020, pp. 153–76, available at https://doi.org/10.1080/09505431.2019.1705270.
40. J. Kosseff, 'The Contours of "Defend Forward" Under International Law', 11th International Conference on Cyber Conflict (CyCon), 2019, Vol. 900, pp. 1–13.
41. X. Palmer, L.N. Potter and S. Karahan, 'COVID-19 and Biocybersecurity's Increasing Role on Defending Forward', *Int. J. Cyber Warf. Terror*, Vol. 11, 2021, pp. 15–29, available at http://services.igi-global.com/resolvedoi/resolve.aspx?doi=10.4018/IJCWT.2021070102.
42. R.J. Hester, 'Bioveillance: A Techno-security Infrastructure to Preempt the Dangers of Informationalised Biology', *Sci. Cult*, Vol. 29, 2020, pp. 153–76.
43. I. Samori, G. Odularu, L. Potter and X.L. Palmer, 'Biocybersecurity and Deterrence: Hypothetical Rwandan Considerations', *Int. Conf. Cyber Warf. Secur*, Vol. 18, 2023, pp. 348–54, available at https://papers.academic-conferences.org/index.php/iccws/article/view/1012.