GLOBAL BIOSECURITY

Laith AL-Eitan1. Addressing Cyberbiosecurity Challenges in the Modern Era of Biotechnology and Artificial Intelligence. Global Biosecurity. 2025; 7(2).

REVIEW

Addressing Cyberbiosecurity Challenges in the Modern Era of Biotechnology and Artificial Intelligence

Laith AL-Eitan[1]*, Haytham Jaouni[1], Ahmad Mihyar[1]

[1]Department of Biotechnology & Genetic Engineering, Faculty of Science and Arts, Jordan University of Science and Technology, Jordan

Abstract

In an era where artificial intelligence and technology have fully integrated and bloomed in biological sciences, the threat of cyberattacks inside the biological field has increased. With increased dependence on bioinformatics, the internet, and outsourcing for data curation and storage, the development of advanced security measures has become mandatory. They safeguard biological data, systems, and procedures against illegal access, modification, or interference. The information collected for the following article was based on the results of previously published articles. These articles were searched via worldwide search engines and databases such as Google Scholar, PubMed, and Google search engines. The search was performed via different keywords, such as “cyberbiosecurity,” “biosecurity,” “artificial intelligence,” and “biotechnology.” The inclusion criteria ensured that only cybersecurity biosafety and biosecurity-related articles were included in the reference list. To protect biological systems, data, and infrastructure from cyber-attacks, a wide range of techniques, protocols, and technologies must be included in the emerging discipline of cyberbiosecurity. Robust cyberbiosecurity measures have become increasingly necessary as biotechnology has advanced quickly, incorporating digital technologies into many areas of biological research, industry, and healthcare. The lack of infrastructure for cyberbiosecurity worldwide puts the biological and scientific research community at high risk of attack. This could hinder data availability, research validity, and the development of biotechnology, biosecurity, and science. Although cyberbiosecurity is still a new part of biosecurity, its importance must be addressed in this era of increasing technology and internet dependence in biology and medical research. This article aims to shed light on a new aspect of biosecurity from the eye of cybersecurity. The objective of the current article is to pave the way for the development of the cyberbiosecurity field.

Keywords

Artificial Intelligence; Biosecurity; Biotechnology; Cyberbiosecurity.

Introduction

In recent years, biosafety and biosecurity have caught the attention of many researchers and policymakers worldwide [1]. The term biosecurity summarizes the measurements for protecting biological information and research integrity [1]. With technology integrated into nearly every aspect of biological and medical research, a technology-based security system is needed. Therefore, cyberbiosecurity has become a non-negligible part of biosecurity. However, implementing such security measures could be difficult due to the lack of infrastructure to maintain and run such a system.

The rising reach and influence of biotechnology on several industries are the reason for the growing significance and applicability of cyberbiosecurity [2]. The advancements in and integration of technology in biology have increased the urgency of biosecurity development [1]. The COVID-19 pandemic highlighted that biotechnology is essential in responding to international health emergencies, from developing vaccines to conducting genetic monitoring [3]. It has also brought attention to the vulnerability of biological data and research platforms to cyberattacks [3]. Therefore, maintaining the cybersecurity resilience of biological systems is essential for maintaining public health and national security.

This literature review aims to thoroughly understand cyberbiosecurity, including its definition, historical development, present issues, potential future developments, ethical and legal issues, and suggestions for improving resilience. This study aims to synthesize current research and perspectives from several fields, such as cybersecurity, biotechnology, and bioethics. The current review looks forward to raising the awareness of policymakers, researchers, and the public about the critical importance of cybersecurity in protecting the integrity, security, and resilience of biological systems in the digital age. Addressing these objectives hopes to contribute to the ongoing discourse on cyberbiosecurity.

Cyberspecies Threats in the Biological Domain

Overview of Biological System Cyberthreats

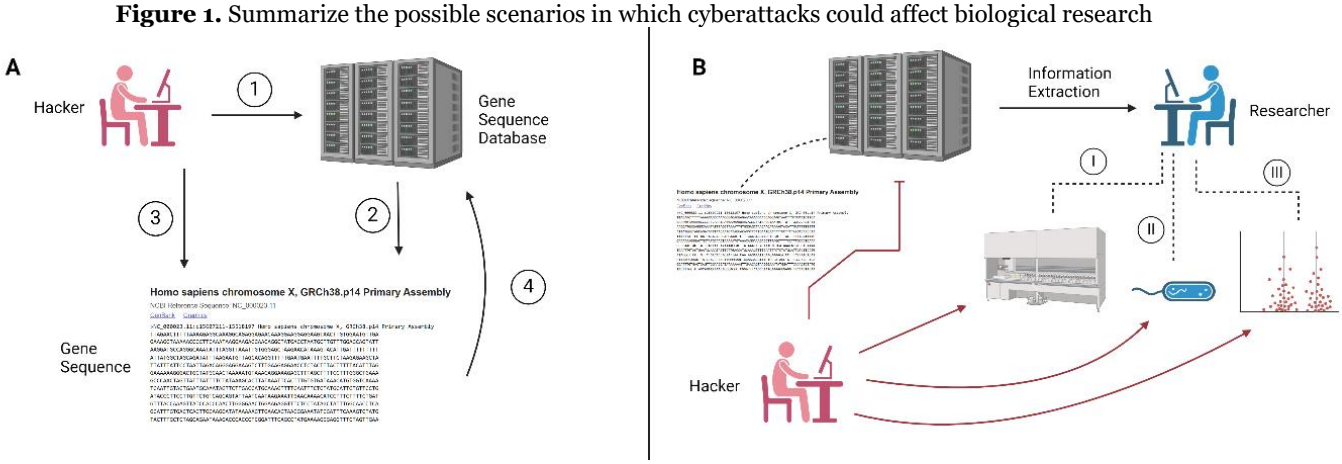
The threats to biological systems, constantly shifting, include a broad spectrum of malicious actions

meant to jeopardize the availability, confidentiality, and integrity of biological data processes and infrastructure [4]. These dangers pose severe concerns to national security, scientific research, and healthcare delivery because they exploit weaknesses in digital technology, human behavior, and organizational practices.

Data breaches, in which unauthorized parties access private information in digital databases, are among the most common cyber threats to biological systems. Such breaches may lead to theft of intellectual property, proprietary research data, or personally identifiable information (PII) [5], resulting in monetary losses, harm to one's reputation, and legal repercussions.

Another major cyber threat to the biological realm is supply chain hacks, in which hackers breach target firms by taking advantage of flaws in outside suppliers or service providers [6]. For example, hackers, corporate espionage agents, and others might use compromised software or hardware in laboratories as entry points to steal sensitive research data without authorization or tamper with trial results, ecology supporting biological research and its development [7].

Figure 1. Summarize the possible scenarios in which cyberattacks could affect biological research



A) A hacker can infiltrate security systems into a general database, such as the Gene Sequence Database (1), and the hacker can obtain access to a specific gene inside the database (2). Once the gene sequence is accessed, the hacker can manipulate it (3) and reupload it back into the database (4). B) The threat could be addressed in different scenarios if the hacker could not access the database. I) The hacker could infiltrate and disrupt the conditions of controls of an automated system. II) The attacker could also infiltrate the data after the researcher's extraction, thus producing an unknown biological threat. III) The third scenario could include the disruption of bioinformatics tools and data analysis software, leading to the publication of dangerous false information.

Examples of Cyber Incidents in Bioinformatics and Biotechnology

Bioinformatics and biotechnology have revealed several high-profile cyber events that highlight the susceptibility of biological systems to cyberattacks and the possible effects on public health, scientific research, and national security. For instance, the 2020 breach of the Bioinformatics Resource Centers (BRCs) of the National Institutes of Health (NIH) jeopardized sensitive genetic material in NIH databases. It exposed the personal information of thousands of researchers [8]. Similarly, the 2017 WannaCry ransomware attack caused significant financial losses and disruptions to patient care and drug manufacturing at several pharmaceutical companies and healthcare facilities across the globe, including Merck & Co. and the National Health Service (NHS) of the United Kingdom [9]. Therefore, as threat actors want to use the abundance of genetic data for identity theft, insurance fraud, or targeted advertising, theft of genomic data has become an increasing problem

Risks and Consequences of Cyber Attacks in the Biological Sector

Cyberattack losses may result in the loss of confidential research data or intellectual property, which may have a disastrous effect on innovation, competitiveness, and sustainability for biotech firms and research organizations [10]. In addition to that, interruptions affecting clinical trial data, diagnostic testing platforms, or electronic health records may cause delays in medical treatments, jeopardize patient safety, and make tracking and managing infectious disease outbreaks or bioterrorism threats more challenging [11]. Furthermore, cyberattacks in the biological sector significantly impact national security, especially concerning military research, biodefense capabilities, and safeguarding vital infrastructure. Threat actors may seriously jeopardize homeland security, military preparedness, and public safety by attempting to obstruct or compromise biomedical research, vaccine development, or biomanufacturing operations [12]. Thus, setting up counterthreat measures is a necessity.

Current Cyberbiosecurity Measures

Existing Cybersecurity Protocols in Biological Laboratories

Biological labs use a range of cybersecurity procedures and policies to reduce online threats and safeguard infrastructure and private information. These tools provide network traffic monitoring, abnormal behavior detection, and the prevention of illegal access attempts. Furthermore, encryption methods often safeguard data, whether in motion or at rest, guaranteeing that private data are safe even if unauthorized individuals capture it [13]. Biological labs need clear standards and processes for controlling cybersecurity threats, which is where organizational policies come into play. In that, the cybersecurity posture of laboratory employees is reinforced even more by regular security awareness training and incident response exercises, which provide them with tools to identify possible threats and take appropriate action [13].

Institutional and Regulatory Frameworks

Institutional and regulatory frameworks include rules for maintaining research integrity and preserving sensitive data while ensuring that all relevant laws and regulations are followed. For example, in the U.S., organizations that receive government money for research must abide by cybersecurity laws such as the Health Insurance Portability and Accountability Act (HIPAA) [14] and the government Information Security Modernization Act (FISMA). Similarly, international bodies such as the International Electrotechnical Commission, the IEC [15], and the Global Organization for Standardization (ISO) [16] provide internationally accepted standards for cybersecurity management systems, such as ISO/IEC 27001 [17] and ISO/IEC 27002 [18].

Moreover, industry-specific rules and standards provide specialized advice for handling cybersecurity threats in biological research facilities. One example is the US Biosafety in Microbiological and Biomedical Laboratories (BMBL) [19] guidelines. The specific difficulties and factors that come with working with biological agents and materials are covered in these recommendations, along with the need to safeguard laboratory safety and security from physical and virtual dangers.

Technological safeguards

Effective cyberbiosecurity measures are built on technological safeguards and best practices, providing crucial defenses against cyber threats. These security measures include software and hardware products designed to identify, stop, and lessen security flaws and breaches. To prevent unwanted access to sensitive data and cryptographic keys, hardware-based protections include deploying secure computer equipment, tamper-resistant servers, encrypted storage devices, and hardware security modules (HSMs) [20].

Various security techniques and technologies are part of software-based safeguards that assist in identifying and thwarting hostile actions, such as malware infections, phishing scams, and efforts at data exfiltration. Examples include antivirus software, intrusion detection/prevention systems (IDS/IPS) [21], data loss prevention (DLP) solutions, and secure email gateways.

Additionally, data encryption ensures that even if data are intercepted or hacked, they remain unreadable to unauthorized parties, helping to safeguard sensitive information from illegal access. Similarly, with custom-developed software applications and online services, safe coding standards such as input validation, output encoding, and parameterized queries assist in eliminating typical vulnerabilities such as SQL injection and cross-site scripting (XSS) [22].

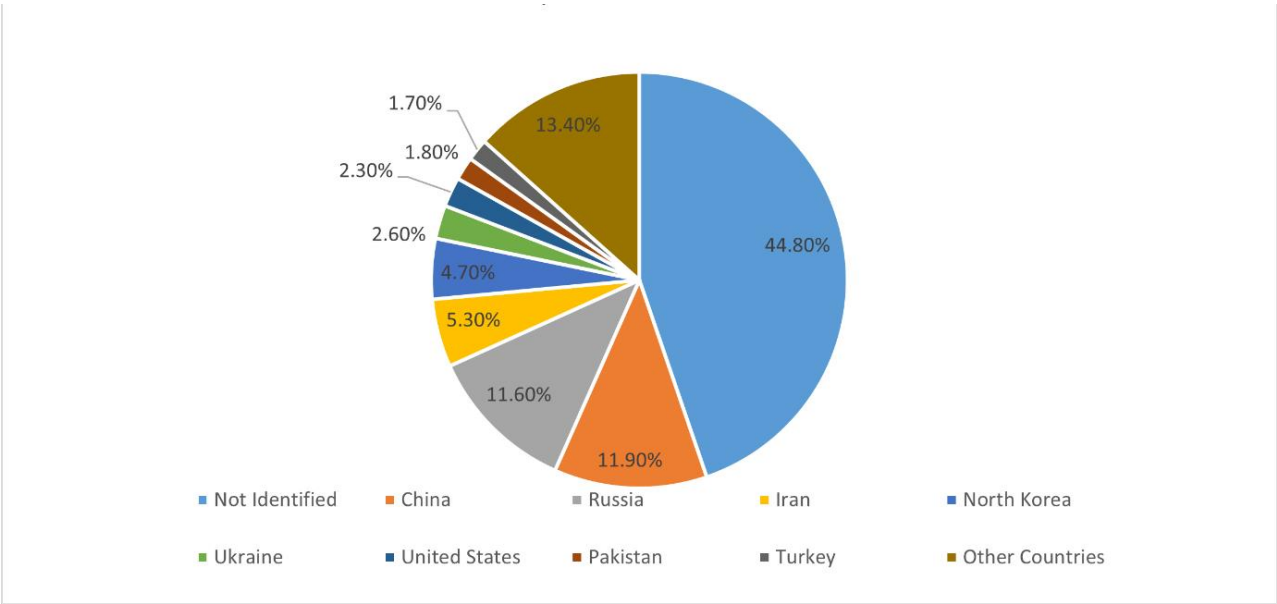
Vulnerabilities in Cyberbiosecurity

Identification of Weaknesses in Current Systems

Biological systems remain susceptible to attacks because of the inherent flaws in present systems, even when different cybersecurity solutions are deployed [4]. Threat actors use these vulnerabilities, which could result from a convergence of technological, human, and organizational factors, to obtain unauthorized access, alter data, or interfere with regular business processes. Today's crucial technological weakness in most cyberbiosecurity systems is using antiquated hardware and software. Many research institutes and biological laboratories use outdated hardware and software that cannot receive security fixes or upgrades from manufacturers [23]. This makes them vulnerable to hackers, who may quickly exploit and obtain unauthorized access to systems. Moreover, insufficient network segmentation and access safeguards increase the susceptibility of biological systems to cyberattacks. Administrative networks, laboratory management systems, and data from biological research are often linked, which makes it possible for attackers to travel laterally inside the network after gaining initial access [24] (Figure 2).

.

Figure 2. Distribution of Cyber incidents between 2000 and 2023.



The data show that the source of cyber threats is global and not limited to a specific region [25]. As can be seen, most cyber incidents are of non-identified origins. At the same time, China has the second most number of cyber incidents

Cyberbiosecurity vulnerabilities are also heavily influenced by human factors, as human mistakes or carelessness may unintentionally expose biological systems to cyberattacks. Typical instances include staff members falling prey to phishing schemes, thus unintentionally exposing private information or disregarding established security guidelines and practices [26]. Organizational flaws such as insufficient cybersecurity awareness, lack of specialized cybersecurity personnel, and restricted funding for cybersecurity development add to the vulnerabilities of current cyberbiosecurity systems. Without a robust security awareness culture and an unwavering dedication to prioritizing cybersecurity, companies may face difficulties efficiently reducing cyber risks and promptly addressing new threats.

Case studies illustrating cyberbiosecurity failures

Numerous well-known case studies highlight the possible repercussions of cyberbiosecurity lapses and their practical effects on biological research, medical care, and national security. In the United Kingdom, for example, a breach of the National Health Service (NHS) in 2017 caused extensive disruptions to healthcare services, including missed appointments, postponed procedures, and subpar patient care. Over 80 NHS trusts and 603 primary care practices were impacted by the WannaCry ransomware assault [27], which used a known vulnerability in outdated Windows computers. This highlights the need for timely software patching and vulnerability management to reduce cyber threats [28].

Furthermore, there are serious privacy and security hazards for people when genomic data are stolen from research facilities. Unlawful access to genomic data, which can lead to identity theft and genetic discrimination, may undermine people's trust in biomedical research and healthcare services [29]. In addition, threat actors may attack public health organizations, biomanufacturing companies, or research institutions to steal or alter genetic data, viruses, or vaccine formulations for bioterrorism needs [30].

Gaps in Understanding and Mitigating Cyber Threats

Better threat intelligence and information sharing are vital to moving forward and establishing a solid regional and global infrastructure to counter cyber threats. Research institutes, governmental organizations, and stakeholders in the private sector can work together more closely to exchange threat intelligence, best practices, and lessons from cyber incidents [31]. This will make spotting new threats and vulnerabilities easier and facilitate the development of correct mitigation plans to counter them. Improving cybersecurity knowledge and education by funding cybersecurity education and training initiatives for lab staff, researchers, and administrators may help increase awareness of cyber hazards and advance best practices for thwarting attacks [32]. This would increase the preparedness of human forces to address threat mitigation.

Current rules and guidelines should be updated and harmonized to reflect new cyber risks in the biological realm [33]. Unifying a safe protocol and measures for biological and medical institutions such as research labs, pharmaceutical companies, and hospitals would allow for more solid anticipation programs and more accessible updates. Cooperation with international partners is needed to address global

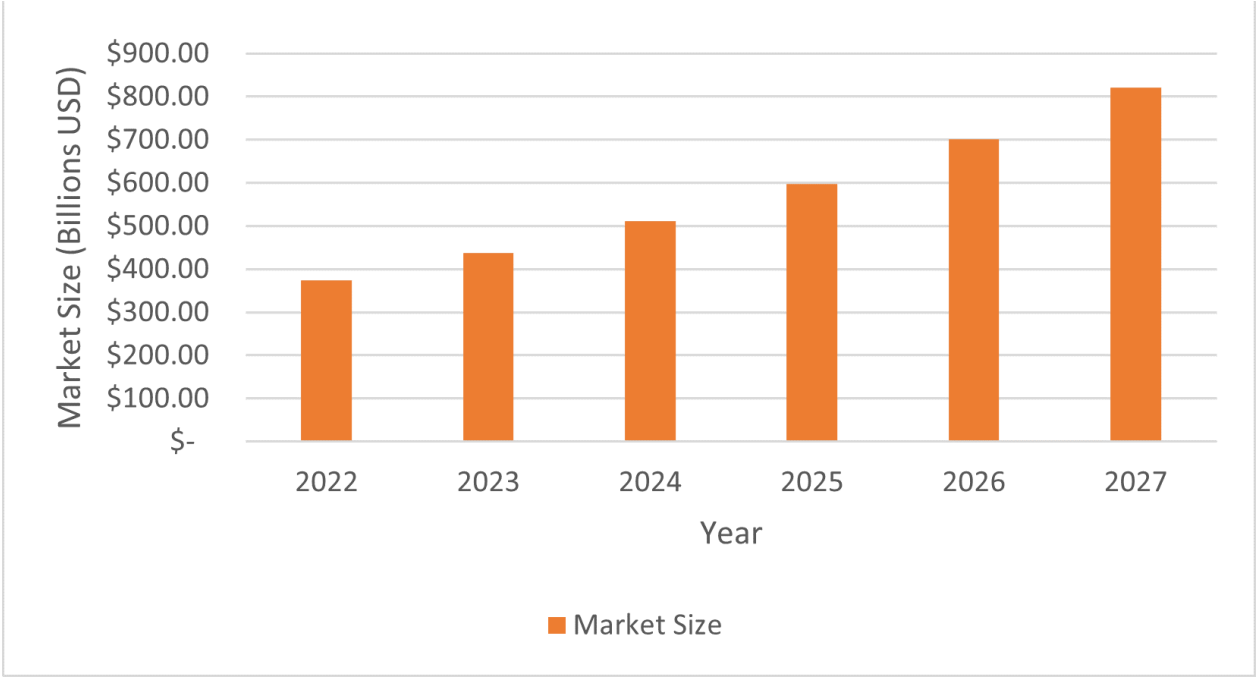
cyber threats and foster a cohesive response to new challenges. It is essential to strengthening international cooperation and coordination on cyberbiosecurity issues [34]. This includes information sharing, capacity building, and cooperative research initiatives [34]. Developing a cybersecurity council and expertise-sharing platforms between countries would allow for a nearly unified strength in cyber threat reduction worldwide.

Interconnectedness of Cybers and Biological Security

Exploration of the nexus between cybersecurity and biosafety

The interconnection between cybersecurity and biosafety reflects the convergence of digital and biological technology and the necessity for integrated methods to manage rising risks and vulnerabilities [35]. As biological systems increasingly become more digitalized, networked, and dependent on digital technology [36], biosafety intersects with cybersecurity. For example, digital infrastructure and networked communication protocols play a significant role in the processing, analyzing, and sharing of biological data via laboratory automation systems [37], next-generation sequencing platforms, and bioinformatics tools [38]. However, combining these technologies also introduces new cybersecurity threats, such as the possibility of genetic data being accessed without authorization, manipulation of experimental findings, or interruption of crucial research processes [39]. Furthermore, the lines between cybersecurity and biosafety are becoming increasingly hazy due to the widespread use of Internet-of-Things (IoT) devices and cloud-based services in biological research [40]. In addition to enabling real-time data monitoring and remote access to research facilities, IoT devices expand the attack surface for cyberattacks [41] (Figure 3).

Figure 3 Market size of the IoT in healthcare.



This figure illustrates the market size of the IoT in the healthcare sector from 2022–2024 and the expected size from 2025–2027 [42]. The chart shows that the market size has increased by $100 billion between 2022 (about $400 billion) and 2024 (about $500 billion).

Mutual Impact of Cyber and Biological Threat

The intricate interactions between digital technology and biological systems and their possible convergence outcomes are reflected in the joint effects of cyber and biological threats. Cyberattacks targeting biological systems, such as ransomware attacks, data breaches, and supply chain intrusions [43], may significantly impact public health, biosafety, and biosecurity.

For example, stolen or altered genomic data from biobanks or research institutes may jeopardize the privacy and confidentiality of a person's genetic information. This might result in genetic discrimination [44] or identity theft [45]. On the other hand, biological risk may also affect cybersecurity

because threat actors might use biological vulnerabilities to conduct cyberattacks or disseminate false information. Examples of these threats include bioterrorism and infectious disease epidemics [46]. For instance, state-sponsored actors or cybercriminal organizations may use public worries and uncertainty about contagious illnesses to conduct malware distribution campaigns to gain an advantage over other countries [47]. The confluence of biological and cyber risks raises concerns over dual-use research and technology. For example, advances in gene editing technologies, such as CRISPR-Cas9, can potentially improve agricultural yields and ameliorate genetic illnesses [48]. Nevertheless, they also raise ethical and security concerns about its abuse for bioterrorism or biowarfare [49].

Synergies in Developing Integrated Security Measures

Organizations may strengthen their resistance to new threats and vulnerabilities by using the synergies between cybersecurity and biosafety procedures and fostering a security awareness and readiness culture. The following sections discuss aspects that add to local and worldwide preparedness to address cyber attacks [23, 50].

1. Risk assessment and mitigation, where organizations may assist in choosing which security controls, resilience measures, and incident response capabilities to invest in first by conducting thorough risk assessments that consider biological and cyber risks, vulnerabilities, and repercussions.

2. Secure-by-design principles in which research projects can reduce vulnerabilities and mitigate risks at every stage of the process, from data collection and analysis to distribution and storage, could be implemented by incorporating cybersecurity and biosafety considerations into the design and development of digital and biological systems.

3. Cross-training and collaboration: Offering cybersecurity and biosafety professionals cross-training opportunities and promoting cooperation between research labs, cybersecurity companies, and government agencies can improve information exchange, the sharing of best practices, and coordinated responses to cyberbiosecurity threats.

4. Regulatory harmonization and alignment: Data protection laws, laboratory safety guidelines, export control regulations, and other regulatory frameworks and standards for cybersecurity and biosafety can be harmonized to simplify compliance requirements and foster a unified strategy for risk management across industries and jurisdictions.

5. Public education and outreach: Spreading knowledge about the potential repercussions of cyberbiosecurity threats and the synergies between cybersecurity and biosafety among researchers, policymakers, and the general public can encourage a proactive risk management culture within and outside the scientific community.

By acknowledging the reciprocal effects of biological and cyber threats and capitalizing on the synergies between biosafety and cybersecurity protocols, organizations can fortify themselves against intricate and dynamic security challenges.

Future Trends and Emerging Challenges

Anticipated Evolution of Cyber Threats in the Biological Domain

The growing digitalization and interconnectivity of biological systems and infrastructure is one trend propelling the emergence of cyber risk in the biological realm. The attack surface for cyber threats grows as biotechnology develops and combines with digital technologies, covering various networked platforms, devices, and data repositories.

Another trend is the rise of complex cyber threats, such as nation-state-sponsored cyberespionage operations [51], ransomware-as-a-service (RaaS) activities [52], and advanced persistent threats (APTs) [53]. Because these threats require sophisticated detection and response skills to identify and neutralize successfully, they present severe problems for cybersecurity and biosafety specialists. Cyber-physical assaults, which combine cyber- and physical security concerns, also present new difficulties for enterprises trying to protect themselves from various dangers. For example, attacks on critical infrastructure and Internet of Things (IoT) devices can predominantly affect biomanufacturing facilities [54] and biological research facilities.

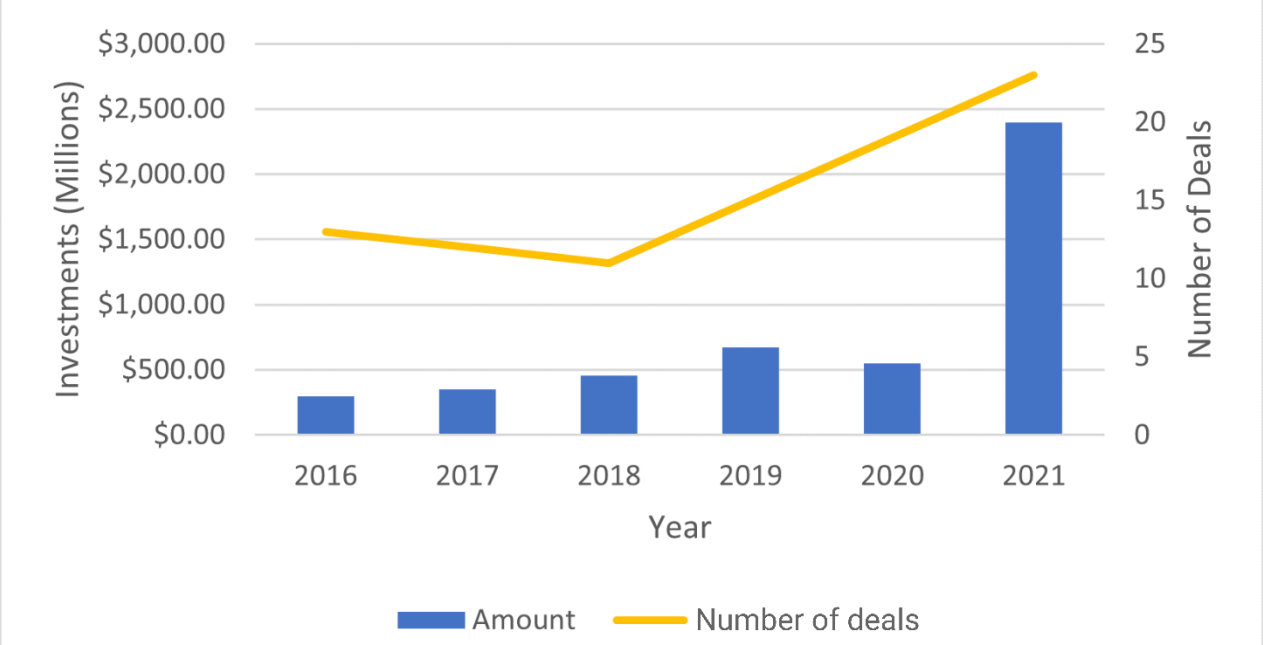
Foreseen challenges and potential solutions

Critical difficulties when anticipating cyberbiosecurity obstacles include developing new solutions for safeguarding biological systems and data, which require interdisciplinary expert teams to work together and continuously invest in the research and development of advanced cybersecurity technologies. This is necessary to keep up with rapid technological advancements and the emergence of cyber threats. Policymakers and regulators trying to foster a unified strategy for managing cyberbiosecurity risk across sectors and jurisdictions face difficulties harmonizing disparate regulatory frameworks and standards for sharing. Careful consideration of cybersecurity and biosafety and ongoing dialogue and engagement with stakeholders is necessary to balance security imperatives, ethical research practices, and individual privacy rights [55].

On the other hand, promoting cooperation among stakeholders from various fields, such as academia, business, and government, can help exchange best practices, lessons learned, and threat intelligence, which will help organizations better understand and reduce the risks associated with cyberbiosecurity. Building capacity and developing the workforce: Financial investments in cybersecurity education, training, and professional development programs can contribute to the development of a workforce with the necessary skills to address the intricate problems of

cyberbiosecurity and to foster a resilient and security-aware culture within and outside of the scientific community (Figure 4).

Figure 4. Interest in investing in cybersecurity



Large companies such as Google, Apple, and Meta have invested in cybersecurity [56]. The chart shows that the number of deals has increased over the years, which led to the number of millions invested in the development of cybersecurity.

Case Studies and Examples

Highlighting Successful Cyberbiosecurity Implementation

Genomic research facilities utilize secure computer systems and encryption techniques to prevent unauthorized access to or disclosure of sensitive genetic data. Using homomorphic encryption and trusted execution environments (TEEs), researchers may perform computations on encrypted genomic material without first decoding it [57]. This promotes cooperative analysis and research while guaranteeing privacy and confidentiality.

The biotechnology and healthcare sectors have formed information-sharing and analysis centers (ISACs) and threat intelligence-sharing partnerships to exchange actionable threat intelligence, best practices, and incident response methodologies

Examining Cyberbiosecurity Incidents and Lessons Learned

Cyberbiosecurity events and failure analyses offer valuable insights and opportunities to enhance cybersecurity protocols and biological domain resilience. One example is the 2020 breach of the National Institutes of Health (NIH) Bioinformatics Resource Centers (BRCs), which gave unauthorized parties access to sensitive genetic data and private information (PII) stored in NIH databases [58]. The incident demonstrated the importance of monitoring systems, access controls, and encryption to protect infrastructure and sensitive research data from cyberattacks.

Another example is the 2017 WannaCry ransomware attack [59], which disrupted operations at several pharmaceutical and healthcare companies worldwide, including Merck & Co. and the UK National Health Service (NHS) [59]. The attack highlighted the threats posed by ransomware to critical infrastructure and the need for timely software patches, vulnerability management, and incident response strategies to lower cyber risk [59]. Furthermore, the 2020 SolarWinds Orion platform attack revealed concerns about software supply chain integrity and security in the biological domain [60]. Businesses must conduct thorough risk assessments, vendor due diligence, and supply chain monitoring to identify and manage vulnerabilities and dependencies in their digital ecosystems.

Recommendations for Strengthening Cyberbiosecurity

Proposed Strategies for Increasing Cyberbiosecurity Measures

Strengthening cyberbiosecurity requires a multidimensional strategy to address new risks and weaknesses, including organizational, technological, and policy approaches. Organizations may improve

their cyberbiosecurity defenses against cyberattacks by using several tactics that protect data, infrastructure, and biological systems. To provide a comprehensive understanding of cyberbiosecurity issues, risk assessments should consider both technological vulnerabilities and human aspects, such as insider threats and social engineering assaults.

Adopting a defense-in-depth strategy for cybersecurity involves deploying numerous layers of security controls, including network segmentation, access restrictions, encryption, and intrusion detection systems. Organizations may identify and repel cyberattacks more successfully by building various barriers and stacking security controls and protection methods. To improve cybersecurity education and training, increase knowledge of cyber hazards, and promote best practices for reducing attacks, laboratories, researchers, and administrators must invest in cybersecurity education and training programs.

To establish incident response capabilities to successfully identify, contain, and quickly recover from cyberattacks, companies must have robust incident response plans and processes. Incident response plans should include roles and duties, escalation processes, communication protocols, and recovery measures to guarantee a coordinated and efficient response to security issues. The exchange of threat intelligence, best practices, and learning from cyber events may be facilitated by forming cooperative relationships with peer institutions, governmental organizations, cybersecurity companies, and industry groups.

Conclusion

In conclusion, cyberbiosecurity is a crucial topic of concern in the digital age since it creates intricate risks and vulnerabilities for biological systems, data, and infrastructure due to the combination of cybersecurity and biotechnology. Organizations, decision-makers, and researchers must understand the connection between biological and cybersecurity and take proactive steps to successfully manage new risks and threats as the field of cyberbiosecurity gains momentum. Increasing funding opportunities and capacity building are crucial for developing cyberbiosecurity worldwide. By improving knowledge and understanding of the significance of cyberbiosecurity, it is possible to increase the ability of biological systems to withstand and counteract cyber dangers. Establishing international cybersecurity councils and strategic partnerships has become necessary as technology and biological research are inseparable.

Conflict of interest

All the authors declare that they do not have conflicts of interest.

Acknowledgments

The authors thank Jordan University of Science and Technology for providing administrative and technical support.

Data Availability

Not Applicable.

Ethics and Consent

Not Applicable.

Funding

Not applicable.

Author's Contribution

L.A.E conceptualized the study. L.A.E, H.J, and A.M have all contributed to the manuscript's writing, reviewing, and editing. H.J and A.M designed the figures.

References

1. Laith A-E, Alnemri M. Biosafety and biosecurity in the era of biotechnology: The Middle East region. Journal of Biosafety and Biosecurity. 2022;4(2):130-45. https://doi.org/10.1016/j.jobb.2022.11.002.
2. Millett K, Dos Santos E, Millett PD. Cyber-biosecurity risk perceptions in the biotech sector. Frontiers in bioengineering and biotechnology. 2019;7:136. PubMed https://doi.org/10.3389/fbioe.2019.00136.
3. Aileni M, Rohela GK, Jogam P, Soujanya S, Zhang B. Biotechnological perspectives to combat the COVID-19 pandemic: precise diagnostics and inevitable vaccine paradigms. Cells. 2022;11(7):1182. PubMed https://doi.org/10.3390/cells11071182.
4. Mthunzi SN, Benkhelifa E, Bosakowski T, Hariri S. A bio-inspired approach to cyber security. Machine Learning for Computer and Cyber Security: CRC Press; 2019. p. 75-104.https://www.taylorfrancis.com/chapters/edit/10.1201/9780429504044-4/bio-inspired-approach-cyber-security-siyakha-mthunzi-elhadj-benkhelifa-tomasz-bosakowski-salim-hariri
5. Hanley M, Dean T, Schroeder W, Houy M, Trzeciak RF, Montelibano J. An analysis of technical observations in insider theft of intellectual property cases2011. Available from: http://www.dtic.mil/get-tr-doc/pdf.

6. Sobb T, Turnbull B, Moustafa N. Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. Electronics. 2020;9(11):1864. https://doi.org/10.3390/electronics9111864.
7. Filkins BL, Kim JY, Roberts B, Armstrong W, Miller MA, Hultner ML, et al. Privacy and security in the era of digital health: what should translational researchers know and do about it? American journal of translational research. 2016;8(3):1560. PubMed
8. Von Solms R, Van Niekerk J. From information security to cyber security. computers & security. 2013;38:97-102.https://doi.org/10.1016/j.cose.2013.04.004.
9. Srinivas J, Das AK, Kumar N. Government regulations in cyber security: Framework, standards and recommendations. Future generation computer systems. 2019;92:178-88. https://doi.org/10.1016/j.future.2018.09.063.
10. Toch E, Bettini C, Shmueli E, Radaelli L, Lanzi A, Riboni D, Lepri B. The privacy implications of cyber security systems: A technological survey. ACM Computing Surveys (CSUR). 2018;51(2):1-27. https://doi.org/10.1145/3172869.
11. Seemma P, Nandhini S, Sowmiya M. Overview of cyber security. International Journal of Advanced Research in Computer and Communication Engineering. 2018;7(11):125-8. https://doi.org/10.17148/IJARCCE.2018.71127.
12. Agbaje M, Awodele O, Ogbonna C, editors. Applications of digital watermarking to cyber security (cyber watermarking). Proceedings of Informing Science & IT Education Conference (InSITE); 2015.
13. Khari M, Shrivastava G, Gupta S, Gupta R. Role of cyber security in today's scenario. Detecting and mitigating robotic cyber security risks: IGI Global; 2017. p. 177-91.
14. Bonfanti ME. Artificial intelligence and the offence-defence balance in cyber security. Cyber Security: Socio-Technological Uncertainty and Political Fragmentation London: Routledge. 2022:64-79.
15. Sharma P. A Detailed Review on Cyber Security 2022 [Available from: https://doi.org/10.36893/JNAO.2022.V13I02.012-020.
16. ISO. International Organization for Standardization 2024 [Available from: https://www.iso.org/home.html.
17. ISO. Information security, cybersecurity and privacy protection — Information security management systems — Requirements, ISO/IEC 27001:2022 2022 [Available from: https://www.iso.org/standard/27001.
18. ISO. Information security, cybersecurity and privacy protection — Information security controls, ISO/IEC 27002:2022 2022 [Available from: https://www.iso.org/standard/75652.html.
19. Prevention CfDCa. Biosafety in Microbiological and Biomedical Laboratories 2020 [Available from: https://www.cdc.gov/labs/pdf/SF__19_308133-A_BMBL6_00-BOOK-WEB-final-3.pdf.
20. Sommerhalder M. Hardware Security Module. Trends in Data Protection and Encryption Technologies. 2023:83-7.https://doi.org/10.1007/978-3-031-33386-6_16.
21. Ashoor AS, Gore S, editors. Difference between intrusion detection system (IDS) and intrusion prevention system (IPS). Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India, July 15-17, 2011 4; 2011: Springer.
22. Deepa G, Thilagam PS. Securing web applications from injection and logic vulnerabilities: Approaches and challenges. Information and Software Technology. 2016;74:160-80. https://doi.org/10.1016/j.infsof.2016.02.005.
23. Reed JC, Dunaway N. Cyberbiosecurity Implications for the Laboratory of the Future. Frontiers in bioengineering and biotechnology. 2019;7:182. PubMed https://doi.org/10.3389/fbioe.2019.00182.
24. Usama M, Qadir J, Raza A, Arif H, Yau K-LA, Elkhatib Y, et al. Unsupervised machine learning for networking: Techniques, applications and research challenges. IEEE access. 2019;7:65579-615. https://doi.org/10.1109/ACCESS.2019.2916648.
25. Incidents ERoC. Overview of cyber incidents 2024 [Available from: https://eurepoc.eu/.
26. Neumann PG. Combatting insider threats. Insider Threats in Cyber Security: Springer; 2010. p. 17-44.https://doi.org/10.1007/978-1-4419-7133-3_2
27. Collier R. NHS ransomware attack spreads worldwide. Can Med Assoc; 2017.https://www.cmaj.ca/content/189/22/E786.
28. Ghafur S, Kristensen S, Honeyford K, Martin G, Darzi A, Aylin P. A retrospective impact analysis of the WannaCry cyberattack on the NHS. NPJ digital medicine. 2019;2(1):98. PubMed. https://www.nature.com/articles/s41746-019-0161-6.
29. Oliver JM, Slashinski M, Wang T, Kelly P, Hilsenbeck S, McGuire A. Balancing the risks and benefits of genomic data sharing: genome research participants' perspectives. Public

health genomics. 2012;15(2):106-14. PubMed. https://doi.org/10.1159/000334718.
30. Prevention CfDCa. Bioterrorism and Anthrax: The Threat 2024 [Available from: https://www.cdc.gov/anthrax/bioterrorism/index.html.
31. Berndt A, Ophoff J, editors. Exploring the value of a cyber threat intelligence function in an organization. Information Security Education Information Security in Action: 13th IFIP WG 118 World Conference, WISE 13, Maribor, Slovenia, September 21–23, 2020, Proceedings 13; 2020: Springer.
32. Piromsopa NNaK. How to Increase Cybersecurity Awareness 2019 [Available from: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/how-to-increase-cybersecurity-awareness#:~:text=There%20are%20various%20methods%20used,%2C%20videos%2C%20simulations%20and%20tests.
33. Li Y, Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports. 2021;7:8176-86. https://doi.org/10.1016/j.egyr.2021.08.126.
34. Rudner M. Cyber-threats to critical national infrastructure: An intelligence challenge. International Journal of Intelligence and CounterIntelligence. 2013;26(3):453-81. https://doi.org/10.1080/08850607.2013.780552.
35. Bhushan M. Cyber-biosecurity. J Defense Stud. 2023;17(2):93-119.https://idsa.demosl-03.rvsolutions.in/system/files/jds/jds-17-2_Mrinmayee-Bhushan.pdf.
36. Stoumpos AI, Kitsios F, Talias MA. Digital transformation in healthcare: technology acceptance and its applications. International journal of environmental research and public health. 2023;20(4):3407. PubMed.https://doi.org/10.3390/ijerph20043407.
37. Habich T, Beutel S. Digitalization concepts in academic bioprocess development. Engineering in Life Sciences. 2024:2300238. PubMed. https://doi.org/10.1002/elsc.202300238.
38. Torri F, Dinov ID, Zamanyan A, Hobel S, Genco A, Petrosyan P, et al. Next generation sequence analysis and computational genomics using graphical pipeline workflows. Genes. 2012;3(3):545-75. PubMed.https://doi.org/10.3390/genes3030545.
39. Arshad S, Arshad J, Khan MM, Parkinson S. Analysis of security and privacy challenges for DNA-genomics applications and databases. Journal of Biomedical Informatics. 2021;119:103815. PubMed. https://doi.org/10.1016/j.jbi.2021.103815.
40. AlSalem TS, Almaiah MA, Lutfi A. Cybersecurity Risk Analysis in the IoT: A Systematic Review. Electronics. 2023;12(18):3958. https://doi.org/10.3390/electronics12183958.
41. Rao AR, Elias-Medina A. Designing an internet of things laboratory to improve student understanding of secure IoT systems. Internet of Things and Cyber-Physical Systems. 2024;4:154-66. https://doi.org/10.1016/j.iotcps.2023.10.002.
42. Healthcare T. IoT in Healthcare Market Share and Trends by 2032 2024 [Available from: https://www.towardshealthcare.com/insights/iot-in-healthcare-market-size.
43. Mantle JL, Rammohan J, Romantseva EF, Welch JT, Kauffman LR, McCarthy J, et al. Cyberbiosecurity for biopharmaceutical products. Frontiers in Bioengineering and Biotechnology. 2019;7:116. PubMed. https://doi.org/10.3389/fbioe.2019.00116.
44. Gostin L. Genetic discrimination: the use of genetically based diagnostic and prognostic tests by employers and insurers. American Journal of Law & Medicine. 1991;17(1-2):109-44. PubMed. https://doi.org/10.1017/S0098858800007942.
45. Vieraitis LM, Shuraydi A. Identity theft 2012. Available from: https://academic.oup.com/edited-volume/41333/chapter/352358022.
46. Das S, Kataria VK. Bioterrorism: A public health perspective. Medical Journal Armed Forces India. 2010;66(3):255-60. PubMed. https://doi.org/10.1016/S0377-1237(10)80051-6.
47. Desai AN, Ruidera D, Steinbrink JM, Granwehr B, Lee DH. Misinformation and disinformation: the potential disadvantages of social media in infectious disease and how to combat them. Clinical Infectious Diseases. 2022;74(Supplement_3):e34-e9. PubMed. https://doi.org/10.1093/cid/ciac109.
48. Gostimskaya I. CRISPR–cas9: A history of its discovery and ethical considerations of its use in genome editing. Biochemistry (Moscow). 2022;87(8):777-88. PubMed. https://doi.org/10.1134/S0006297922080090.
49. Riedel S, editor Biological warfare and bioterrorism: a historical review. Baylor University Medical Center Proceedings; 2004 Oct;17(4):400–406.Pubmed.
50. Richardson LC, Lewis SM, Burnette RN. Building capacity for cyberbiosecurity training.

Frontiers in Bioengineering and Biotechnology. 2019;7:112. PubMed. https://doi.org/10.3389/fbioe.2019.00112.
51. Ohlin JD, Govern K, Finkelstein C. Cyber war: law and ethics for virtual conflicts: OUP Oxford; 2015.https://global.oup.com/academic/product/cyber-war-9780198717492?cc=au&lang=en&.
52. Meland PH, Bayoumy YFF, Sindre G. The Ransomware-as-a-Service economy within the darknet. Computers & Security. 2020;92:101762. https://doi.org/10.1016/j.cose.2020.101762.
53. Chen P, Desmet L, Huygens C, editors. A study on advanced persistent threats. Communications and Multimedia Security: 15th IFIP TC 6/TC 11 International Conference, CMS 2014, Aveiro, Portugal, September 25-26, 2014 Proceedings 15; 2014: Springer.
54. .Borgosz L, Dikicioglu D. Industrial internet of things: What does it mean for the bioprocess industries? Biochemical Engineering Journal. 2024;201:109122. https://doi.org/10.1016/j.bej.2023.109122.
55. Greenbaum D. Cyberbiosecurity: An emerging field that has ethical implications for clinical neuroscience. Cambridge Quarterly of Healthcare Ethics. 2021;30(4):662-8. PubMed. https://doi.org/10.1017/S0963180121000013X.
56. Insights C. The Big Tech In Cybersecurity Report: How Facebook, Apple, Microsoft, Google, & Amazon Are Tackling Cyber Threats 2022 [Available from: https://www.cbinsights.com/research/report/famga-big-tech-cybersecurity/.
57. Kockan C. Privacy-Preserving Algorithms for Secure Genome Analysis in Trusted Execution Environments: Indiana University; 2021.
58. Gutierrez JB, Harb OS, Zheng J, Tisch DJ, Charlebois ED, Stoeckert Jr CJ, Sullivan SA. A framework for global collaborative data management for malaria research. The American journal of tropical medicine and hygiene. 2015;93(3 Suppl):124. PubMed. https://doi.org/10.4269/ajtmh.15-0003.
59. Kalita E. WannaCry ransomware attack: Protect yourself from WannaCry ransomware cyber risk and cyber war. Independently published; 2017.
60. Tran C. The SolarWinds attack and its lessons. E-International Relations https://www e-ir info/2021/06/17/the-solarwinds-attack-and-its-lessons. 2021.

How to cite this article: Laith AL-Eitan1. Addressing Cyberbiosecurity Challenges in the Modern Era of Biotechnology and Artificial Intelligence. Global Biosecurity. 2025; 7(2).

Published: January 2025

Global Biosecurity is a peer-reviewed open access journal published by University of New South Wales.