A Snapshot of the Biocybersecurity/Cyberbiosecurity Landscape (2017-2024)

Saurabh Ranjan[1], Lucas Potter[2,3] and Xavier-Lewis Palmer[2,3]
[1]Shaheed Sukhdev College of Business Studies, University of Delhi, India
[2]School of Cybersecurity, Old Dominion University, USA
[3]BIOSView, Oswego, USA

28saurabhranjan@gmail.com

Abstract: The global bioeconomy is extremely valuable, comprising healthcare, agriculture, logistics, and biotechnology, and more (Murch et al, 2018; Kircher, 2019; Khandekar & Ghosh, 2023). The increased integration of digital systems within biological domains within the modern bioeconomy has exposed vulnerabilities that exist at the intersection of cybersecurity, cyber-physical security, and biosecurity, referred to as "Cyberbiosecurity" (CBS) or "Biocybersecurity" (BCS) (Murch et al, 2018; Potter and Palmer, 2023). These respectively focus on protecting biological data and systems from cyber threats and addressing the security of cyber systems that interact with biological entities. Their landscape has evolved considerably and vulnerabilities found pose risks to infrastructure and human lives, as cyberattacks could disrupt essential bio-based and related systems such as medical supply chains, food systems, research, and all connected to it (Murch et al, 2018; Potter and Palmer, 2023). Given the complexity and interconnectedness of these domains, the need for interdisciplinary collaboration between experts in cybersecurity, biosecurity, and biotechnological innovation is more pressing than ever. Addressing these emerging threats requires a multifaceted approach combining technical safeguards with policies that enhance resilience across the bioeconomy. There is considerable benefit to viewing what work is mapped over the combined landscape. In order to map the research landscape and track the progess and explorations of this work, research publications were compiled and analyzed using search operators including "Cyberbiosecurity," "Biocybersecurity," "Digital Biosecurity," and "Cyber-biosecurity" to identify critical trends and contributions over the past seven years. In this we have found many different players and trends by year. This work finds that the intersections of Cybersecurity and Biosecurity presents an evolving landscape with significant benefits, novel applications, but also heightened global risks. When properly examined, our communities can meet the emerging challenges.

Keywords: Cyber security, Biocybersecurity, Digital biosecurity, Bioeconomy, Research

1. Introduction

Biocybersecurity (BCS)/Cyberbiosecurity(CBS) reflect hybrid field intersections in the early stages. They have a wide scope and necessitate a multidisciplinary approach to tackle the risks linked to current and emerging technologies in the bioeconomy (Potter & Palmer, 2023). BCS and CBS combine the principles of cyber security with the life sciences, such as biology and biotechnology, while incorporating other disciplines, such as engineering, data science, and law. Overall, it concerns the security of biological systems such as genetic engineering and synthetic biology, as well as the security of biologically relevant data and infrastructures such as data centers and agricultural and water systems (Mantle et al., 2019; Murch et al., 2018; Duncan et al., 2019; Batarseh et al., 2023; DiEuliis, 2023; Sobien et al., 2023) It also addresses the security of biological resources such as crops and livestock and the security of biological processes such as the production of pharmaceuticals (Duncan et al, 2019; Mantle et al, 2019). For those wanting deeper in-depth views, collections of works within “Mapping the Cyberbiosecurity Enterprise” (Murch & DiEuliis , 2019) and “Cyberbiosecurity: A new field to deal with emerging threats.” (Greenbaum, 2023) are great resources to improve one’s depth in the field. As a disclaimer, this exploration paper itself is not a substitution. Instead, it briefly re-examines the research landscape in BCS/CBS by scanning and skimming the publications 7 years in, building on prior work looking at the intersections (Potter and Palmer, 2023). For those interested in BCS and CBS, read the works listed in the references for greater understandings of BCS and CBS. This work is a supplementary companion piece to the works that exist. Biocybersecurity and Cyberbiosecurity have significant potential to impact every critical industry.

2. Methodology

The research utilized multiple databases, including PubMed, IEEE Xplore, Google Scholar, Web of Science, and Scopus. The search terms were meticulously chosen to ensure a focused exploration of the topic, encompassing phrases such as "cyberbiosecurity," "cyber-biosecurity," "biosecurity cyber threats," "cybersecurity in biotechnology," and "digital biosecurity." Inclusion criteria centered on peer-reviewed articles in English from 2017 onwards, specifically addressing the convergence of cybersecurity and biosecurity with full-text availability. Exclusion criteria removed non-peer-reviewed articles, studies not emphasizing the cyber aspects of biosecurity,

publications in languages other than English, and articles published before 2017 or without full-text access. Challenges encountered included the interdisciplinary nature of cyberbiosecurity, leading to variations in terminology, a limited number of publications, keyword discrepancies, incomplete database coverage, and restricted access to some full-text articles behind paywalls. This process is illustrated in Figure 1, below., and resulted in 359 published research elements.

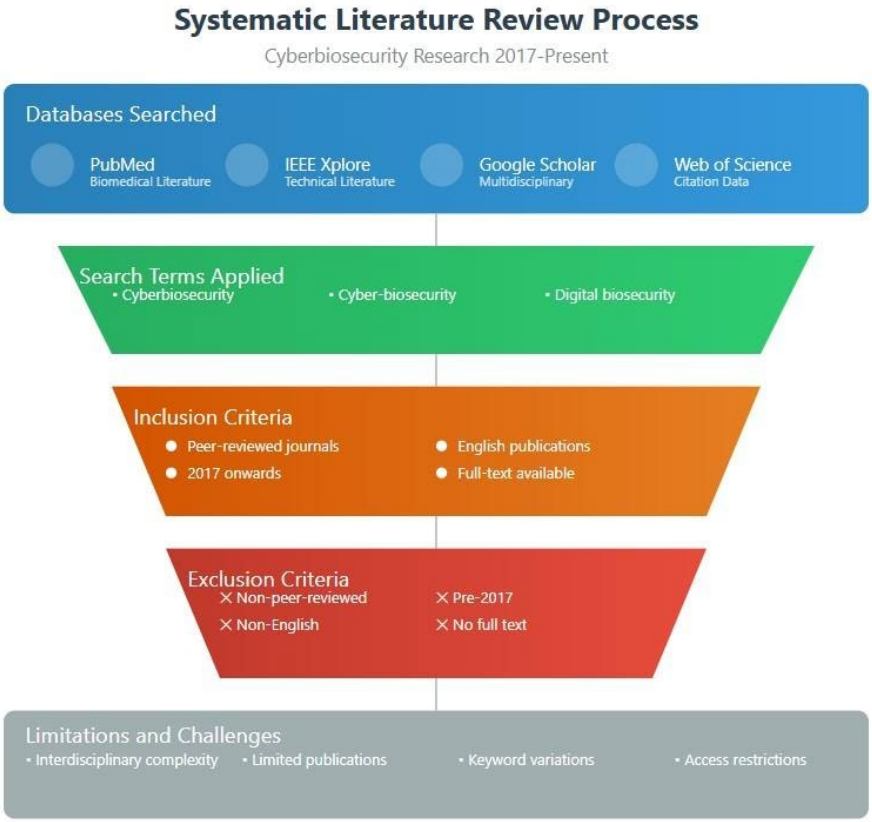

Figure 1: Graphical representation of the Literature Review Process on Biocybersecurity/Cyberbiosecurity Research between 2017 and 2024

The objective was to track papers from 2017 to August 2024 containing the terms "cyberbiosecurity," "biocybersecurity," and "digital biosecurity." The process involved searching these terms in various databases and analyzing specific parameters to track relevant papers in a spreadsheet. However, as the search extended to the 20th page of results, relevance decreased, making this effort more of a sample than a comprehensive collection. Despite this, the methodology reflects a genuine attempt to capture as much relevant literature as possible. Any articles or other research elements left out are not intentional. It is important to note that there are several research elements that were presentations and excluded from our records. Any exclusion of significant works is not intentional. For practical purposes, deep dives on dossiers or any documents critical to national security requiring clearance were not sought and not included. The authors expected that some publications and other relevant documents may slip their attention and welcome suggestions to include in the following works.

3. Mapping Concepts, Institutions, and Contributions

Our scan of nearly 360 research elements has revealed that at least 53 countries are actively contributing to cyberbiosecurity research. The United States leads with 129 contributions, followed by the United Kingdom (28), Australia (27), India (15), and China (14). The research shows strong representation from North America, Europe, and Oceania, while Asian countries contribute significantly. Although South America and Africa have more limited involvement, it's important to note that smaller countries are also making significant contributions. Ecuador, for instance, has emerged as a notable contributor with five contributions, and Iran leads in the Middle East with three contributions. The global reach of cyberbiosecurity research extends across all continents, except

Antarctica, with contributions from both large nations like China and India and smaller countries such as Qatar and Estonia.

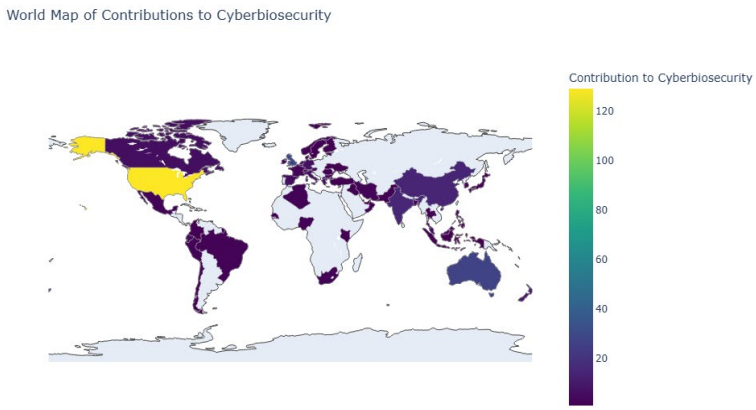

Figure 2: Geographical Mapping of Contributors to Biocybersecurity/Cyberbiosecurity Research between 2017 and 2024, by note of published research elements found

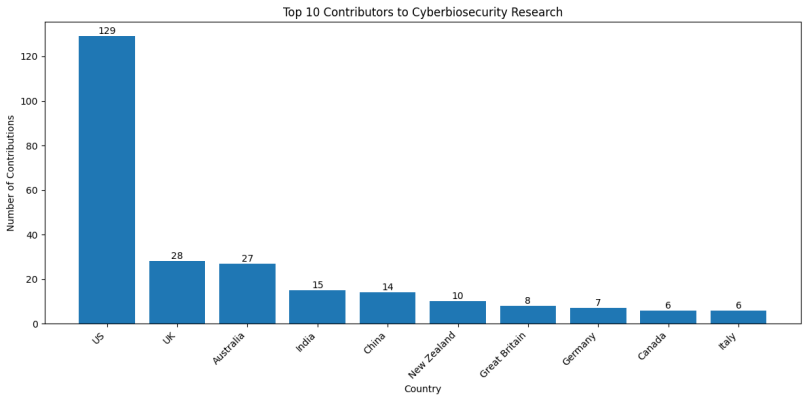

Figure 3: Charting of Contributors to Biocybersecurity/Cyberbiosecurity Research, by country, between 2017 and 2024, by note of published research elements found

Figure 3 above visualises the top 10 contributing countries, highlighting the significant contributions from the US and the notable efforts of other leading nations. This data suggests that while Cyberbiosecurity research is a global endeavour, it is currently led by a few key countries with the US at the forefront. The wide range of contributing countries indicates growing global awareness and interest in this field. It is expected that this distribution will change as facilities that enable quality Biocybersecurity/Cyberbiosecurity research proliferate, especially among the Global South.

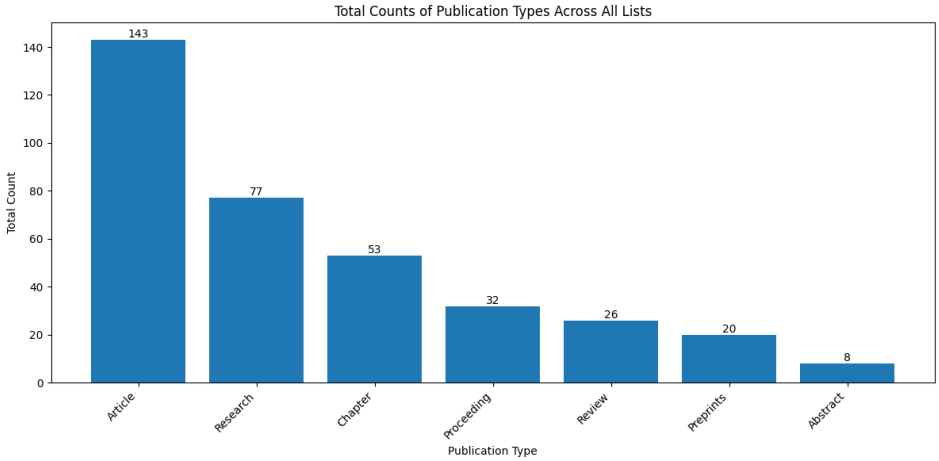

Figure 4: Charting of Contributors to Biocybersecurity/Cyberbiosecurity Research, by published research element type, between 2017 and 2024, by note of published research elements found

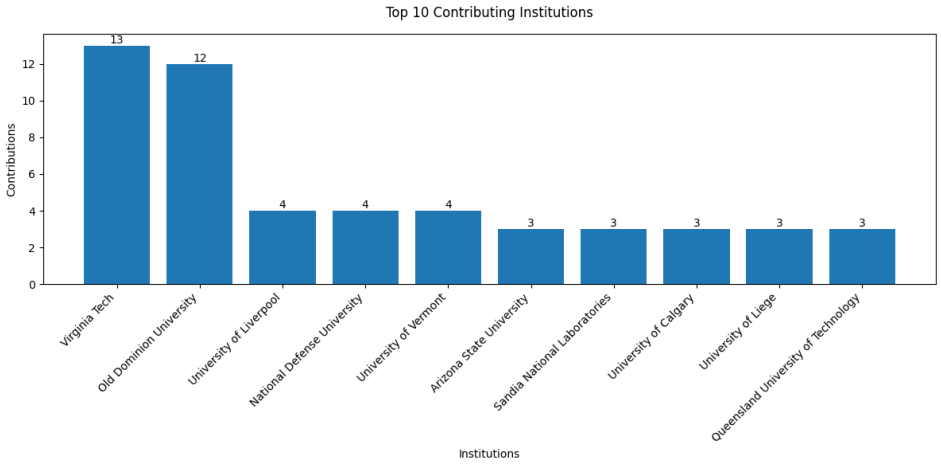

Figure 5: Charting of Contributors to Biocybersecurity/Cyberbiosecurity Research, by Affiliated Institution, between 2017 and 2024, by note of published research elements found

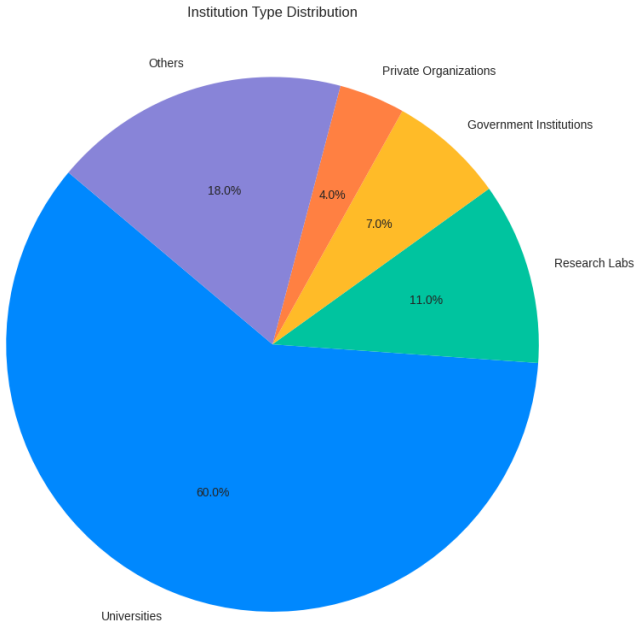

Figure 6: Pie Charting of Contributors to Biocybersecurity/Cyberbiosecurity Research, by Institution Type, between 2017 and 2024, by note of published research elements found

Most publications in the field are articles, constituting about 39.8% of the total, as revealed by Figure 4. Research papers are the second most frequent type, making up 21.4%, while chapters represent 14.8%. Proceedings, reviews, and preprints each account for between 5% and 9% of the total publications. Abstracts are the least common, comprising only 2.2% of the total. In cyberbiosecurity and biocybersecurity, the research landscape is globally distributed. Among the universities, Virginia Polytechnic Institute and State University (VPI) and Old Dominion University (ODU) stood out with member contributions. The next tier of institutions contributes only four each, but the top 10 institutions collectively account for approximately 52% of all contributions. An analysis of institutional types shows that universities represent the majority of contributors, making up 60%, followed by research laboratories (11%), government institutions (7%), and private organizations (4%). Other contributors, making up 18%, include independent researchers, research foundations, international organizations, non-profits, professional associations, think tanks, and research consortiums. Geographically, North America leads with 58% of contributions, but Europe, the Asia-Pacific region, the Middle East, and other regions also make significant contributions, accounting for 42% collectively.

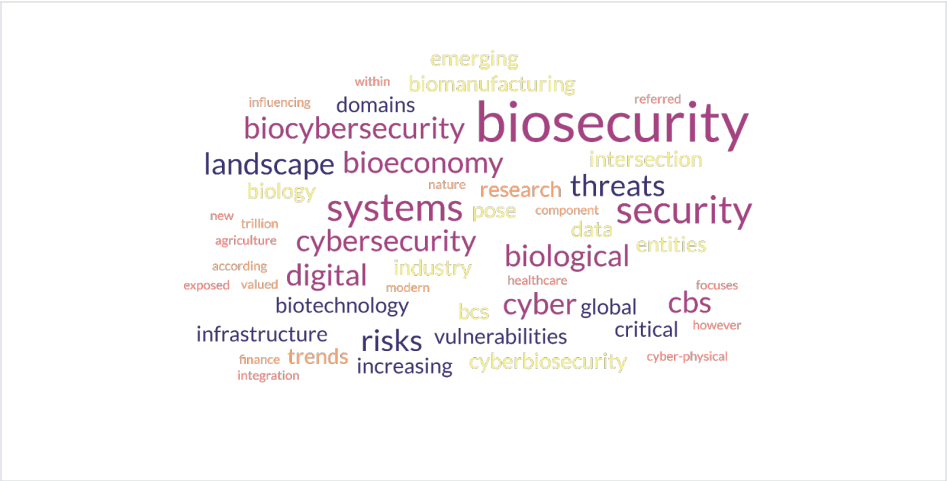

Figure 7: Word Cloud created from abstracts of research elements found, visualises the emerging landscape of biological and digital security concerns, particularly as they relate to critical infrastructure, healthcare, and the growing bioeconomy. It reflects the increasing convergence of biological and digital systems and the security challenges this integration presents

A word cloud was constructed from abstracts on published research elements involving cyberbiosecurity and biocybersecurity, highlighting critical themes between 2017 and 2024, in Figure 7. Hypothetically, a word cloud constructed on the contents of all publications would likely be much different in composition, but this provides us with a helpful starting point. Reflecting on the word cloud, more extensive terms reflect more frequent entries. The prominent terms such as 'biosecurity,' 'cybersecurity,' 'systems,' and 'risks' indicate that a significant portion of the research is dedicated to understanding and addressing vulnerabilities in integrating biological and cyber systems. Terms like 'threats,' 'vulnerabilities,' and 'security' suggest a growing recognition of the increasing risks posed by merging biological and digital technologies, particularly in domains like biomanufacturing and the bioeconomy. The frequent occurrence of 'digital,' 'biological,' and 'cyberbiosecurity' underscores the increasing interconnectedness of these domains, necessitating security experts to adopt a multidisciplinary approach. Words such as 'infrastructure,' ' entities,' and 'systems' emphasize the urgent requirement for robust defense mechanisms, such as encryption, secure access controls, and regular system audits, to safeguard biological infrastructures from cyber-attacks. However, terms like 'trends,' 'global,' and 'emerging' highlight these threats' dynamic and evolving nature, emphasizing the need for continuous adaptation and innovation in this field. For those in security capacities focusing on the bioeconomy, this word cloud indicates that the field's focus is expanding beyond abstract biosecurity and cybersecurity, encompassing fields such as biotechnology, biomanufacturing, and cyber-physical systems. It underscores the need for sustained vigilance in addressing escalating risks across various sectors but not limited to those areas such as healthcare , agriculture and finance. We must maintain a high level of vigilance, bolster interdisciplinary collaboration, enhance digital resilience in biosecurity systems, and develop comprehensive strategies to address the complexities that arise at the intersection of biology and cyber technologies.

4. Briefly Summarising the Combined BCS-CBS Research Landscape Between 2017 and 2024

Describing papers and research elements from 2017 to August 2024 was challenging; however, we attempted to summarie them. Between 2017 and 2024, research in cyberbiosecurity (CBS) and biocybersecurity (BCS) progressed significantly, responding to emerging technological advancements and growing global threats (Potter & Palmer, 2023). Early work, prior to the formalizing of the terms BCS and CBS, presented in 2017, helped accelerate discussion, deep and wide, about how cyber-attack chains need to consider biology, spurring focus on biosecurity challenges in agriculture, animal research, and environmental management, emphasizing integrating digital tools to improve surveillance and mitigate risks (Murch et al., 2018; Govindharajan et al., 2017; Net et al., 2017). Researchers additionally recognized the importance of digital technologies and citizen science in enhancing biosecurity efforts across sectors (Thomas et al., 2017). By 2018, the research landscape was paying more attention to vulnerabilities in connected biotechnology, including integrating cyberinfrastructure with biological research, which poses new risks to biodata and synthetic biology (Murch et al., 2018). Studies began emphasizing interdisciplinary approaches to addressing biosecurity challenges across various industries, such as agriculture, tourism, and marine environments (Abdo et al., 2018; Demertzis et al., 2018; Melly & Hanrahan, 2018). By 2019, Cyberbiosecurity and other forms of the name were becoming more formally accepted, and the convergence of biology and cybersecurity in modern and advanced laboratory and medical contexts were upregulated as a critical concern (Mirsky et al., 2019; Reed and Dunaway, 2019; Richardson et al., 2019). Researchers highlighted the growing threats to biotechnological infrastructures and stressed the urgent need for comprehensive risk mitigation strategies, particularly in public biological databases and advanced manufacturing sectors (Caswell et al., 2019; DiEuliis, 2019; Guttieres et al., 2019). Robust governance across sectors and through international frameworks became a central theme in addressing these evolving challenges (George, 2019). The onset of the COVID-19 pandemic in 2020 further accelerated the recognition of cyberbiosecurity as a crucial field. Studies underscored the importance of securing synthetic biology, DNA synthesis, and biological data from potential cyberattacks while reimagining public health(Adlet et al., 2021; Puzis et al., 2020; Mueller, 2021). By 2021 and 2022, some new cyberbiosecurity research focused on workforce and leadership development along with educational initiatives to prepare skilled professionals capable of addressing emerging threats at the intersection of cybersecurity and biotechnology (Dodge, 2022; Duncan et al., 2022; Kaufman et al., 2022; Powell et al., 2022). In 2023 and 2024, advancements in artificial intelligence (AI), the Internet of Medical Things, and DNA-based information security further shaped the research landscape along with conceptualizations of Bio-crime in the IoT Age (Elgabry, 2023; Liu et al., 2024). Studies focused on enhancing biosecurity in healthcare diagnostics, precision medicine, and agriculture while addressing the legislative frameworks necessary to manage emerging bio-cyber threats (DiEuliis & Giordano, 2024; Nemane & Doshi, 2024). The field of cyberbiosecurity continued to grow, with a strong emphasis on interdisciplinary collaboration, technological innovation, and policy reform to protect critical biological infrastructures from evolving cyber threats (Adeoye et al., 2024; DiEuliis & Giordano, 2024; Liu et al., 2024; Foud et al., 2024)

5. Implications and Applications for the Industrial Bioeconomy

The period spanning from 2017 to 2024 witnessed a burgeoning interest in the realm of cyberbiosecurity and biocybersecurity, shedding light on the escalating vulnerabilities at the convergence of digital and biological systems (Murch et al., 2018; Adeoye et al., 2024). This burgeoning field has progressively evolved to confront risks within pivotal domains such as agriculture, bio-manufacturing, and healthcare (Duncan et al., 2019; Mantle et al., 2019). Scholars have emphasized the imperative need for robust cyberbiosecurity frameworks to fortify biotechnological infrastructures against cyber threats, particularly considering proliferation of automation, AI-driven diagnostics, and DNA-based information security (Liu et al., 2024; Jordan et al., 2020). The merging of these technologies highlights the critical need for interdisciplinary collaboration, making it essential rather than just desirable (Richardson et al., 2019).

Immense ROI exists in workforce development, equipping professionals with the requisite skills to navigate bio-cyber risks adeptly (Richardson et al., 2019; Adeoye et al., 2024). Critical applications include safeguarding agriculture digital tools, enhancing healthcare diagnostics, and securing bio-manufacturing against threats (Duncan et al., 2022; Chatzilakou et al., 2024). As bioeconomy sectors increasingly pivot towards integrated cyber-physical systems, comprehensive policies and international cooperation stand as essential bulwarks against the burgeoning threats, ensuring the security and resilience of digital and biologically relevant infrastructures (Batarseh et al., 2023; Sobien et al., 2023). The potential dividends of such endeavors, which include enhanced productivity, improved data security, and reduced risk of bioterrorist attacks, are extensive

and reduce the chances that our national census can be excised swiftly (DiEuliis & Giordano, 2024). The findings advocate for a multidisciplinary governance approach to cyberbiosecurity (Puzis et al., 2020; Burrell et al., 2023). Theoretical frameworks are now compelled to assimilate the interconnectedness of biological and digital systems, with a pronounced emphasis on risk management within bioinformatics and synthetic biology (Puzis et al., 2020).

In practical terms, agriculture, healthcare, and bio-manufacturing industries are impelled to implement enhanced security protocols to assuage bio-cyber risks (Guttieres et al., 2019; Palmer & Palmer, 2023). From a policy standpoint, establishing global governance frameworks is imperative to regulate and safeguard biotechnological infrastructure across borders, ensuring adherence to cyberbiosecurity standards (Nemane & Doshi, 2024). Cyberbiosecurity research yields palpable applications across diverse sectors. In agriculture, precision farming and bio-manufacturing processes can seamlessly integrate cybersecurity protocols to preclude manipulation or sabotage (Carneiro et al., 2021). Healthcare systems stand to benefit from fortified patient data protection and secure AI-driven diagnostic tools, immunizing them against cyber threats (Arshad et al., 2021). In synthetic biology, fortifying DNA synthesis and bioengineering pipelines from malicious interference will undergird the integrity of bio-manufactured products (Farbiash & Puzis, 2020). Furthermore, while global supply chains cannot erect impregnable defenses against bioterrorist threats by deploying real-time monitoring and cyberbiosecurity solutions – they can reduce the chance of bad actors being successful, but time remains of the essence (Mantle et al., 2019; Mueller, 2023). Policymakers are further urged to institute international governance frameworks that delineate global standards for data protection within the domain of biotechnology (Fouad, 2024).

6. Conclusion

Over the last seven years, the field of cyberbiosecurity has evolved significantly with core themes centered around the integration of cyber and biological sciences, data protection, risk management, and interdisciplinary collaboration. Key players include leading academic institutions, government agencies, research institutes, and industry stakeholders. Emergent trends point towards increased regulation, advanced technology adoption, ethical considerations, enhanced public-private partnerships, and global collaboration. The literature on cyberbiosecurity reveals a field that is rapidly evolving, with significant progress in understanding and addressing the intersection of cybersecurity and biosecurity. However, there are still many areas that require further exploration and development, particularly in standardisation, empirical research, and cross-disciplinary integration. Addressing these gaps will be essential for creating robust and effective strategies to safeguard against the complex threats posed by cyberbiosecurity.

References

Abdo, D. A., Duggan, R. L., & McDonald, J. I. (2018). Sounding out pests: The potential of hydroacoustics as a surveillance and compliance tool in aquatic biosecurity. Biological Invasions, 20(12), 3409–3416. https://doi.org/10.1007/s10530-018-1792-2

Adeoye, S., Lindberg, H., Bagby, B., Brown, A., Batarseh, F., & Kaufman, E. (2024). Cyberbiosecurity workforce preparation: Education at the convergence of cybersecurity and biosecurity. NACTA Journal, 67(1). https://doi.org/10.56103/nactaj.v67i1.151

Adeoye, S. O., Batarseh, F., Brown, A. M., & Kaufman, E. K. (2024). Understanding the landscape of cyberbiosecurity for integrative educational programming. Journal of the ASABE, 67(1), 207–217. https://doi.org/10.13031/ja.15739

Adler, A., Beal, J., Lancaster, M. and Wyschogrod, D., 2021. Cyberbiosecurity and Public Health in the Age of COVID-19. *Emerging Threats of Synthetic Biology and Biotechnology: Addressing Security and Resilience Issues*, pp.103-115.

Akköse, M. (2017). Koyun ve keçilerde digital dermatitis. Atatürk Üniversitesi Veteriner Bilimleri Dergisi, 12(1), 99–110. https://doi.org/10.17094/ataunivbd.309782

Amiri A, Shekarchizadeh M, Shekarchizadeh Esfahani AR, Masoud GH-H. Bio-Cyber Threats and Crimes, the Challenges of the Fourth Industrial Revolution. Bioethics Journal, Special Issue on Ethical & Legal Reflections 2021; 81-97.

Anand, M. (2018). A systems approach to agricultural biosecurity. Health Security, 16(1), 58–68. https://doi.org/10.1089/hs.2017.0035

Arshad, S., Arshad, J., Khan, M. M., & Parkinson, S. (2021). Analysis of security and privacy challenges for DNA-genomics applications and databases. Journal of Biomedical Informatics, 119, 103815. https://doi.org/10.1016/j.jbi.2021.103815

Batarseh, F. A., Kulkarni, A., Sreng, C., Lin, J., & Maksud, S. (2023). ACWA: An AI-driven cyber-physical testbed for intelligent water systems. Water Practice & Technology, 18(12), 3399–3418. https://doi.org/10.2166/wpt.2023.197

Burrell, D. N., Nobles, C., Cusak, A., Jones, L. A., Wright, J. B., Mingo, H. C., Ferreras-Perez, J., Khanta, K., Shen, P., & Richardson, K. (2023). Cybersecurity and cyberbiosecurity insider threat risk management. In Handbook of Research

on Cybersecurity Risk in Contemporary Business Systems (pp. 121–136). IGI Global. https://doi.org/10.4018/978-1-6684-7207-1.ch006

Carneiro, R., Duncan, S., Ramsey, F., Seyyedhasani, H. and Murch, R. 2021. Cyber attacks in agriculture: protecting your farm and small business with cyberbiosecurity.".

Caswell, J., Gans, J. D., Generous, N., Hudson, C. M., Merkley, E., Johnson, C., Oehmen, C., Omberg, K., Purvine, E., Taylor, K., Ting, C. L., Wolinsky, M., & Xie, G. (2019). Defending our public biological databases as a global critical infrastructure. Frontiers in Bioengineering and Biotechnology, 7. https://doi.org/10.3389/fbioe.2019.00058

Chatzilakou, E., Hu, Y., Jiang, N., & Yetisen, A. K. (2024). Biosensors for melanoma skin cancer diagnostics. Biosensors and Bioelectronics, 250, 116045. https://doi.org/10.1016/j.bios.2024.116045

De Carolis, A., Newmark, A. J., Kim, J., Song, J., Pietropaoli, M., Manara, V., Gyorffy, A., Cazier, J., & Formato, G. (2024). A comprehensive analysis of beekeeping risks and validation of biosecurity measures against major infectious diseases in apis mellifera in europe. Agriculture, 14(3), 393. https://doi.org/10.3390/agriculture14030393

Demertzis, K., Iliadis, L. S., & Anezakis, V.-D. (2018). Extreme deep learning in biosecurity: The case of machine hearing for marine species identification. Journal of Information and Telecommunication, 2(4), 492–510. https://doi.org/10.1080/24751839.2018.1501542

DiEuliis, D., 2019. Key national security questions for the future of synthetic biology. *Fletcher F. World Aff.*, *43*, p.127.

DiEuliis, D. (2020). Parsing the digital biosecurity landscape. Georgetown Journal of International Affairs, 21, 166. https://heinonline.org/HOL/Page?handle=hein.journals/geojaf21&id=177&div=&collection=

DiEuliis, D. (2023). Revisiting the digital biosecurity landscape. In D. Greenbaum (Ed.), Cyberbiosecurity: A New Field to Deal with Emerging Threats (pp. 71–78). Springer International Publishing. https://doi.org/10.1007/978-3-031-26034-6_5

DiEuliis, D., & Giordano, J. J. (2024). Safely balancing a double-edged blade: Identifying and mitigating emerging biosecurity risks in precision medicine. Frontiers in Medicine, 11, 1364703. https://doi.org/10.3389/fmed.2024.1364703

DiEuliis, D. (2024). Bolstering biosecurity amid the biotechnology revolution. Orbis, 68(3), 361–382. https://doi.org/10.1016/j.orbis.2024.05.003

Dodge, H.D., 2022. Post Pandemic Cyberbiosecurity Threats from Terrorist Groups.

Duncan, J., Grove-White, D., & Angell, J. (2018). Understanding contagious ovine digital dermatitis. In Practice, 40(2), 60–65. https://doi.org/10.1136/inp.j4812

Duncan, S. E., Reinhard, R., Williams, R. C., Ramsey, F., Thomason, W., Lee, K., Dudek, N., Mostaghimi, S., Colbert, E., & Murch, R. (2019). Cyberbiosecurity: A new perspective on protecting u. S. Food and agricultural system. Frontiers in Bioengineering and Biotechnology, 7. https://doi.org/10.3389/fbioe.2019.00063

Duncan, J., & Angell, J. (2019). Control of infectious lameness in sheep. Livestock, 24(5), 246–251. https://doi.org/10.12968/live.2019.24.5.246

Duncan, J. S., Angell, J. W., Grove-White, D., Walsh, T. R., Seechurn, N., Carter, S., & Evans, N. (2022). Impact of research on contagious ovine digital dermatitis on the knowledge and practices of UK sheep farmers and veterinarians. Veterinary Record, 190(1), e674. https://doi.org/10.1002/vetr.674

Duncan, S., Carneiro, R., Braley, J., Hersh, M., Ramsey, F., & Murch, R. (2022). Cybersecurity: Beyond ransomware: Securing the digital food chain. Food Australia, 74(1), 36–40. https://search.informit.org/doi/10.3316/informit.279190773769187

Duncan, S., & Nobles, C. (2022). Cybersecurity risks in food sustainability and emerging technologies. Journal of Agricultural Informatics, 9(4), 321-335.

Elgabry, M. (2023). Biocrime, the internet-of-ingestible-things and cyber-biosecurity. In D. Greenbaum (Ed.), Cyberbiosecurity: A New Field to Deal with Emerging Threats (pp. 135–146). Springer International Publishing. https://doi.org/10.1007/978-3-031-26034-6_9

Farbiash, D., & Puzis, R. (2020). Cyberbiosecurity: Dna injection attack in synthetic biology (arXiv:2011.14224). arXiv. https://doi.org/10.48550/arXiv.2011.14224

Fouad, N. S. (2024). Cyberbiosecurity in the new normal: Cyberbio risks, pre-emptive security, and the global governance of bioinformation. European Journal of International Security, 1–21. https://doi.org/10.1017/eis.2024.19

Fracchia, C. (2023) 'Understanding the Cyberbiosecurity Threat', Defense Dossier, December, pp. 22-25. American Foreign Policy Council.

George, A.M., 2019. The national security implications of cyberbiosecurity. *Frontiers in bioengineering and biotechnology*, *7*, p.51.

Govindharajan, V.K., Tesfaldet, K., Tesfom, S., Joseph, B. and Al Naemi, H., 2017. Biosecurity And Biosafety In LARC.

Guttieres, D., Stewart, S., Wolfrum, J. and Springs, S.L., 2019. Cyberbiosecurity in advanced manufacturing models. *Frontiers in bioengineering and biotechnology*, *7*, p.210.

Hamilton, R. A., Mampuys, R., Galaitsi, S. E., Collins, A., Istomin, I., Ahteensuu, M., & Bakanidze, L. (2021). Opportunities, challenges, and future considerations for top-down governance for biosecurity and synthetic biology. In B. D. Trump, M.-V. Florin, E. Perkins, & I. Linkov (Eds.), Emerging Threats of Synthetic Biology and Biotechnology (pp. 37–58). Springer Netherlands. https://doi.org/10.1007/978-94-024-2086-9_3

Hansen, O. H., Stang, J., & Jaiswal, V. (2024). A trustworthy digital twin for data driven verification. Day 2 Tue, May 07, 2024, D012S057R001. https://doi.org/10.4043/35081-MS

Jacobs, C., Orsel, K., Mason, S., & Barkema, H. W. (2018). Comparison of effects of routine topical treatments in the milking parlor on digital dermatitis lesions. Journal of Dairy Science, 101(6), 5255–5266. https://doi.org/10.3168/jds.2017-13984

Jordan, S. B., Fenn, S. L., & Shannon, B. B. (2020). Transparency as threat at the intersection of artificial intelligence and cyberbiosecurity. Computer, 53(10), 59–68. https://doi.org/10.1109/MC.2020.2995578

Kaufman, E., Adeoye, S., Batarseh, F., Brown, A., Drape, T., Duncan, S., Rutherford, T., Strawn, L. and Xia, K., 2022. CyberBioSecurity through Leadership-as-Practice Development.

Khandekar, P. and Ghosh, P.K., 2023. Bioeconomy: Different Countries, Different Strategies, Multiple Benefits. *Asian Biotechnology & Development Review*, *25*(3).

Kircher, M., 2019. Bioeconomy: Markets, implications, and investment opportunities. *Economies*, *7*(3), p.73.

Kitney, R. I., Bell, J., & Philp, J. (2021). Build a sustainable vaccines industry with synthetic biology. Trends in Biotechnology, 39(9), 866–874. https://doi.org/10.1016/j.tibtech.2020.12.006

Liu, T., Zhou, S., Wang, T., & Teng, Y. (2024). Cyberbiosecurity: Advancements in DNA-based information security. Biosafety and Health, 6(4), 251–256. https://doi.org/10.1016/j.bsheal.2024.06.002

Liv, N., & Greenbaum, D. (2023). Cyberneurosecurity. In V. Dubljević & A. Coin (Eds.), Policy, Identity, and Neurotechnology: The Neuroethics of Brain-Computer Interfaces (pp. 233–251). Springer International Publishing. https://doi.org/10.1007/978-3-031-26801-4_13

López Bernal, S., Perez Martins, D., & Huertas Celdrán, A. (2021). Towards the mitigation of distributed denial-of-service cyberbioattacks in bacteria-based biosensing systems. Digital Signal Processing, 118, 103241. https://doi.org/10.1016/j.dsp.2021.10324

Mantle, J. L., Rammohan, J., Romantseva, E. F., Welch, J. T., Kauffman, L. R., McCarthy, J., Schiel, J., Baker, J. C., Strychalski, E. A., Rogers, K. C., & Lee, K. H. (2019). Cyberbiosecurity for biopharmaceutical products. Frontiers in Bioengineering and Biotechnology, 7. https://doi.org/10.3389/fbioe.2019.00116

Melly, D., & Hanrahan, J. (2018). The potential role of smart mobile technology in mitigating ireland's tourism biosecurity risk. 6(6). https://doi.org/10.17265/2328-2169/2018.12.002

Millett, K., dos Santos, E., & Millett, P. D. (2019). Cyber-biosecurity risk perceptions in the biotech sector. Frontiers in Bioengineering and Biotechnology, 7. https://doi.org/10.3389/fbioe.2019.00136

Mirsky, Y., Mahler, T., Shelef, I. and Elovici, Y., 2019. {CT-GAN}: Malicious tampering of 3d medical imagery using deep learning. In *28th USENIX Security Symposium (USENIX Security 19)* (pp. 461-478).

Mueller, S. (2021). Facing the 2020 pandemic: What does cyberbiosecurity want us to know to safeguard the future? Biosafety and Health, 3(1), 11–21. https://doi.org/10.1016/j.bsheal.2020.09.007

Mueller, S. (2023). Potentials of pathogen research through the lens of cyberbiosecurity, or what threat actors can learn from the covid-19 pandemic. In D. Greenbaum (Ed.), Cyberbiosecurity: A New Field to Deal with Emerging Threats (pp. 147–171). Springer International Publishing. https://doi.org/10.1007/978-3-031-26034-6_10

Murch, R.S., So, W.K., Buchholz, W.G., Raman, S. and Peccoud, J., 2018. Cyberbiosecurity: an emerging new discipline to help safeguard the bioeconomy. Frontiers in bioengineering and biotechnology, 6, p.39.

Murch, R. and DiEuliis, D., 2019. Mapping the cyberbiosecurity enterprise. *Frontiers in Bioengineering and Biotechnology*, *7*, p.235.

Nemane, V. V., & Doshi, K. (2024). Innovate, evaluate, legislate: U. S. Senators forge a path to assess artificial intelligence's biosecurity quandary. Biotechnology Law Report, 43(2), 75–87. https://doi.org/10.1089/blr.2024.28103c.43.2

Ney, P., Koscher, K., Organick, L., Ceze, L. and Kohno, T., 2017. Computer security, privacy, and {DNA} sequencing: compromising computers with synthesized {DNA}, privacy leaks, and more. In *26th USENIX Security Symposium (USENIX Security 17)* (pp. 765-779).

Norton, G., Taylor, M., & Barnier, D. (2017). Swipe right for science: The digital revolution behind species identification. Wildlife Australia, 54(3), 34–36. https://search.informit.org/doi/10.3316/ielapa.022575919200401

Potter, L. and Palmer, X.L., 2023. Mission-aware differences in cyberbiosecurity and biocybersecurity policies: Prevention, detection, and elimination. In Cyberbiosecurity: A new field to deal with emerging threats (pp. 37-69). Cham: Springer International Publishing.

Potter, L., Shetty, S., Karahan, S., & Palmer, X. L. (2024). Biocybersecurity and applications of predictive physiological modelling. International Journal of System of Systems Engineering, 14(4), 349–361. https://doi.org/10.1504/IJSSE.2024.139410

Powell, E., Akogo, D., Potter, L. and Palmer, X.L., 2022. Co-leadership and cross-pollination of university and DIY bio spaces: an exploration in consideration of Biocybersecurity. In *Proceedings of the Future Technologies Conference (FTC) 2021, Volume 3* (pp. 610-621). Springer International Publishing.

Power, G. M., Renaud, D. L., Miltenburg, C., Spence, K. L., Hagen, B. N. M., & Winder, C. B. (2024). Graduate student literature review: Perceptions of biosecurity in a canadian dairy context. Journal of Dairy Science, 107(7), 4605–4615. https://doi.org/10.3168/jds.2023-24033

Puzis, R., Farbiash, D., Brodt, O., Elovici, Y., & Greenbaum, D. (2020). Increased cyber-biosecurity for DNA synthesis. Nature Biotechnology, 38(12), 1379–1381. https://doi.org/10.1038/s41587-020-00761-y

Rathod, S.A., 2023. Cyberbiosecurity: An Upcoming New Science to Help Protect the Bioeconomy. International Research Journal of Modernization in Engineering, Technology and Science, 5(6), pp.1339-1341. Available at: www.irjmets.com

Reed, J.C. and Dunaway, N., 2019. Cyberbiosecurity Implications for the Laboratory of the Future. *Frontiers in bioengineering and biotechnology*, *7*, p.182.

Rekha, P. N., Gangadharan, R., Dharshini, S., Clark, W., Ramanathan, G., Vimala, D., Panigrahi, A., & Gopal, C. (2017). Digital database on shrimp farming in coastal watershed of Cuddalore District, Tamil Nadu. Indian Journal of Fisheries, 64. https://doi.org/10.21077/ijf.2017.64.special-issue.76191-06

Renault, V., Humblet, M.F., Pham, P.N. and Saegerman, C., 2021. Biosecurity at cattle farms: Strengths, weaknesses, opportunities and threats. Pathogens, 10(10), p.1315.

Richardson, L. C., Lewis, S. M., & Burnette, R. N. (2019). Building capacity for cyberbiosecurity training. Frontiers in Bioengineering and Biotechnology, 7. https://doi.org/10.3389/fbioe.2019.00112

Richardson, L. C., Connell, N. D., Lewis, S. M., Pauwels, E., & Murch, R. S. (2019). Cyberbiosecurity: A call for cooperation in a new threat landscape. Frontiers in Bioengineering and Biotechnology, 7. https://doi.org/10.3389/fbioe.2019.00099

Sawaya, S., Kenneally, E., Nelson, D. and Schumacher, G., 2012. Artificial intelligence and the weaponization of genetic data. In Cyberbiosecurity: A New Field to Deal with Emerging Threats (pp. 265-278). Cham: Springer International Publishing.

Schabacker, D. S., Levy, L.-A., Evans, N. J., Fowler, J. M., & Dickey, E. A. (2019). Assessing cyberbiosecurity vulnerabilities and infrastructure resilience. Frontiers in Bioengineering and Biotechnology, 7. https://doi.org/10.3389/fbioe.2019.00061

Shafie, N. F., & Osman, N. D. (2024). Overview of biosecurity legislation in malaysia. Perdana: International Journal of Academic Research, 19(1), 1–12. https://www.perdanajournal.com/index.php/perdanajournal/article/view/192

Sobien, D., Yardimci, M.O., Nguyen, M.B., Mao, W.Y., Fordham, V., Rahman, A., Duncan, S. and Batarseh, F.A., 2023. AI for cyberbiosecurity in water systems—A survey. In *Cyberbiosecurity: A new field to deal with emerging threats* (pp. 217-263). Cham: Springer International Publishing.

Thomas, M. L., Gunawardene, N., Horton, K., Williams, A., O'Connor, S., McKirdy, S., & van der Merwe, J. (2017). Many eyes on the ground: Citizen science is an effective early detection tool for biosecurity. Biological Invasions, 19(9), 2751–2765. https://doi.org/10.1007/s10530-017-1481-6

Tighe, M., Forster, N., Guppy, C., Savage, D., Grave, P., & Young, I. M. (2018). Georeferenced soil provenancing with digital signatures. Scientific Reports, 8(1), 3162. https://doi.org/10.1038/s41598-018-21530-7

Trump, B. D., Florin, M.-V., Perkins, E., & Linkov, I. (Eds.). (2021). Emerging threats of synthetic biology and biotechnology: Addressing security and resilience issues. Springer Nature. https://doi.org/10.1007/978-94-024-2086-9

Vinatzer, B. A., Heath, L. S., Almohri, H. M. J., Stulberg, M. J., Lowe, C., & Li, S. (2019). Cyberbiosecurity challenges of pathogen genome databases. Frontiers in Bioengineering and Biotechnology, 7. https://doi.org/10.3389/fbioe.2019.00106

Wortzel, L. M. (2023) 'China's Evolving Thinking About Biotechnology', Defense Dossier, December, pp. 12-16. American Foreign Policy Council.https://www.afpc.org/uploads/documents/Defense_Dossier_-_December_2023_Final.pdf