International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 6, Issue 2, pp 75-79, February-2022
https://doi.org/10.47001/IRJIET/2022.602013

Cyberbiosecurity as the Foremost Biological Weapon to the Digital World

[1]Dr. Alex Mathew, [2]Hannah Alex

[1]Department of Cybersecurity, Bethany College, USA
[2]Brooke High School, USA

Abstract **- Cyberbiosecurity has emerged as a new field combining cybersecurity and biosecurity. The convergence of cybersecurity and biosecurity can potentially impact the digital operations of enterprises in a variety of industries, including agriculture, manufacturing, and healthcare. This systematic review summarizes and synthesizes research on the increasing importance of cyber-biosecurity threats and the importance of cyber-biosecurity measures in combating the misuse of cyberspace and bioscience technology. The author performed three distinct searches through ProQuest, Web of Science, and MEDLINE databases. The author used keywords to identify 15 articles that met the systematic review's purpose. Analysis of the 15 articles revealed that the intersection of current advancements in biosciences with conventional cyberspace security risks has promoted the awareness and discovery of threats in the cyberbiosecurity field. The author concludes that cybersecurity is the foremost biological weapon to the digital world when challenged by new technologies and security threats. As a result, cyberbiosecurity measures must safeguard the bioeconomy and address the possibility for or actual misuse of critical information, materials, and systems at the convergence of biosciences and cyberspace. Stakeholders interested in cyberbiosecurity outcomes need to be competent in its implementation.**

Keywords: Biological weapon, biosecurity, biotechnology, cyberbiosecurity, cybersecurity.

I. INTRODUCTION

Cyberbiosecurity is an emergent field that tries to understand the connection between cybersecurity and biosecurity. Consequently, cyberbiosecurity seeks to understand the emerging risks at the intersection of cyberspace and biology to develop strategies to address them [1]. Additionally, cyberbiosecurity intends to determine the vulnerabilities to unwarranted cyber-surveillance, security breaches, and malicious practices that can occur at the convergence of cyberspace and biology [2]. Consequently, cyberbiosecurity develops and implements measures to protect and mitigate threats against the cyberspace and bioscience fields.

Cyberbiosecurity has increased the potential for dealing with the damage, misuse, or exploitation of sensitive data, mechanisms, and resources at the intersection of cyberspace and bioscience [3]. It is a critical component of a broader set of policies for safeguarding the bioeconomy [4] [5]. However, the increased recognition of biotechnology innovations in the digital era has presented secondary security threats and consequently given rise to cyber-biosecurity threats [6]. Accordingly, the current research is a systematic review focused on cyberbiosecurity as the foremost biological weapon to the digital world. This systematic review summarizes and synthesizes research on the increasing importance of cyber-biosecurity threats and the importance of cyber-biosecurity measures in combating the misuse of cyberspace and bioscience technology. The author explores the increasing importance of cyber-biosecurity threats as technology continues to accelerate the digital world. Additionally, the systematic review explores the importance of cyber-biosecurity measures in preventing the misuse of cyberspace and bioscience technology, including lowering the threat of bioweapons proliferation.

II. PROPOSED METHODOLOGY

A) Study Design / Systematic Review Protocol

The author designed a protocol for a systematic review (SR) as per the Preferred Reporting Items for Systematic Review and Meta-analysis Protocols (PRISMA-P) criteria. Figure 1 depicts the SR process and the results obtained by using this SR protocol in the form of a block diagram (flowchart).

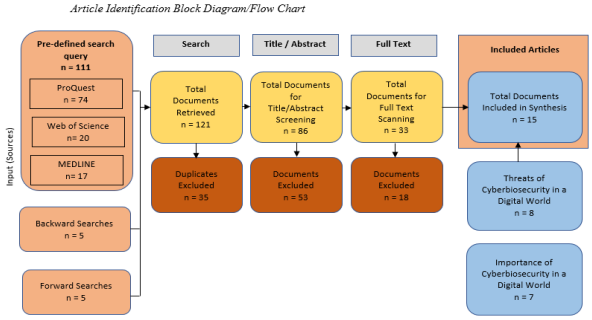

Figure 1: Article Identification Block Diagram/Flow Chart

ISSN (online): 2581-3048
Volume 6, Issue 2, pp 75-79, February-2022
https://doi.org/10.47001/IRJIET/2022.602013

B) Algorithm of Literature Search

The first step entailed identifying relevant articles using a previously defined and optimized search question. The author conducted a keyword search in ProQuest, Web of Science, and MEDLINE using combinations of the following index terms: biological weapon, biosecurity, biotechnology, cyberbiosecurity, and cybersecurity. Furthermore, the author conducted both forward and backward citation searches to discover additional relevant articles.

C) Search Strategy and Inclusion Criteria

The author screened the articles against pre-set inclusion criteria in the second and third steps. As previously stated, the author derived the structure of the systematic review from the PRISMA-P. Studies were eligible for this review if published within the previous five years; if their full-text manuscript version was available on ProQuest, Web of Science, and MEDLINE, and if peer-reviewed or contained in a scientific journal. Additionally, the author included only studies that explicitly explored the increasing importance of cyber-biosecurity threats in the digital world or the importance of cyber-biosecurity measures in preventing the misuse of cyberspace and bioscience technology. The author excluded studies that discussed cyberbiosecurity in general without discussing the threats or importance of cyberbiosecurity.

D) Data Collection and Synthesis

The author initially identified 121 articles after searching for the threats and importance of cyberbiosecurity in the digital world. The author then excluded 35 articles for being duplicates, leaving 86 articles. The author then conducted an abstract review of the remaining studies, at least twice, through a SWOT analysis to evaluate whether they ought to remain in the analysis or not. The author then excluded 53 articles with more weaknesses than strengths. The author next performed a full-text scan on the remaining 33 articles in the group. A total of 18 articles were excluded due to the weak nature of the main findings reported. The final group comprised 15 studies, with which the author proceeded for a systematic review of the literature.

E) Risk of Bias

Since cyberbiosecurity is an emerging discipline that combines cybersecurity and biosecurity, researchers have not studied much in a randomized control trial. Accordingly, the non-publication of extensive research findings would limit data available for analysis.

III. RESULTS ANALYSIS

A) Study Selection and Characteristics

The first search found a total of 121 articles containing the keywords "biological weapon," "biosecurity," "biotechnology," "cyberbiosecurity," or "cybersecurity." The author identified 15 articles matching the review purpose after refining the search criteria. The author then evaluated the strength of primary findings relevant to the review purpose. The author filtered the results to English only and selected a period from 2017 to the present. However, the results in Web of Science and MEDLINE were already limited; so no extra filters had an effect. ProQuest employed similar filters as PubMed and CINAHL but necessitated an additional filter for academic papers. The “Expert Rating” filter was also chosen; however, it did not affect the results. The author studied each article to identify common themes. The author next resolved the main topic of the studies with a summary.

B) Results Synthesis

1) Cyberbiosecurity Threats in the Digital World

Cyber-biosecurity risks are challenging to characterize due to differences in threat types, targets, and possible consequences, coupled with a significant difference in the level of complexity of mitigation and response mechanisms [7]. Biology, cyberspace, and technology have evolved tremendously over the previous ten years. Their dependence on digitalization, automation, and cybersecurity has generated new vulnerabilities for unintentional effects and possibilities for intentional misuse that have gone entirely unnoticed [8].

Biotechnology’s cyber-physical nature poses unparalleled security threats. The bioscience field has conventionally functioned under an insecure system in which participants are expected to self-regulate and in most cases, doesn't monitor security threats. Cybercriminals may compromise computers by encoding malware in DNA sequences. They may also synthesize threats using data from free open sources. Trust within the biotech field causes vulnerabilities at the convergence of cyberspace and life sciences [1]. The increased digitization of information and biological material handling has made multiple market sectors vulnerable to threats at the convergence of cyberspace and biosciences [3].

The rapid digitization of bioscience has resulted in advancements that have raised fears over additional hazards not limited to cyberbiosecurity, such as cyberwar fare and malware intrusions [9]. Cybercriminals use phishing scams, viruses, virus hoaxes, and security holes that leave vulnerabilities to target industries such as agriculture, manufacturing, and healthcare [10]. Accordingly, cyber

ISSN (online): 2581-3048
Volume 6, Issue 2, pp 75-79, February-2022
https://doi.org/10.47001/IRJIET/2022.602013

attacks on infrastructure can have a cascade effect on human health and the environment due to a compromise on biotech products.

It is critical to consider the potential effects of cyberbiosecurity threats due to the increased digitization of information about products and their manufacturing in the biopharmaceutical field. Some possible effects include financial damage to the biopharmaceutical field due to the lack of integrity in the digitization of information and exposure of workers in biopharmaceutical industries to hazardous agents, such as by intentionally introducing pathogens into the manufacturing process [11]. Mechanical designers, software developers, and end-users must consider challenges associated with cyberbiosecurity vulnerabilities. Individuals and organizations must ensure privacy, fairness, and respect for their data. Organizations must train end-users on looking at laboratory equipment and digital systems from a cyberbiosecurity point of view [12]. This approach not only mitigates cyberbiosecurity vulnerabilities but has the potential to completely eradicate them, which benefits employees, bioscience enterprises, and national security.

2) Importance of Cyberbiosecurity Measures in the Digital World

Mechanical designers, software developers, and end-users must seize the opportunity to mitigate cyberbiological risk and security gaps before their enemies do [13]. Cyberbiosecurity will be a crucial factor in essential systems associated with the digitalization of life, as biotechnologies become more sophisticated over time [2]. Comprehensive, multidisciplinary assessments can help biomanufacturing enterprises discover security vulnerabilities and develop strategies to mitigate or resolve them [4].

The U.S. bioeconomy allows for the development of unique and creative products and the attainment of objectives such as reduced carbon footprint and high-quality healthcare. It has also created new opportunities for innovation, the creation of jobs, and the growth of the economy [5]. Other innovative developments resulting from the bioeconomy in the United States include artificial photosynthesis and carbon sequestration for the production of biofuels, as well as breakthrough technologies to combat emerging infectious diseases such as Ebola and Zika Virus [14].

Developing a complete awareness of vulnerabilities is a critical first step in effectively managing cyberbiosecurity threats. Stakeholders should then determine the cost-effective and practicable mitigation alternatives to mitigate vulnerabilities. Individuals and organizations must mitigate cyberbiosecurity threats like bioweapon proliferation by implementing standard biosecurity measures. In this case, vulnerabilities should be identified and mitigated through regular training, policy updates, and increased physical security [6]. Considering cybersecurity's interdisciplinary nature, the security team responsible for assessing, protecting, and mitigating cyberbiosecurity vulnerabilities should be competent in both biosciences and information technology [15].

IV. CONCLUSION

Cyberbiosecurity is a relatively new discipline that focuses on the convergence of cybersecurity and biosecurity. This convergence potentially impacts the digital operations of enterprises in a variety of fields, including agriculture, manufacturing, and healthcare. The intersection of current advancements in biosciences with conventional cyberspace security risks has promoted the awareness and discovery of threats in the cyberbiosecurity field. Therefore, cyberbiosecurity becomes the foremost biological weapon to the digital world when challenged by new technologies and security threats. In this regard, cyberbiosecurity measures should focus on safeguarding the bioeconomy and dealing with the possibility for or definite misuse of critical information, materials, and systems at the convergence of biosciences and cyberspace. Stakeholders interested in cyberbiosecurity outcomes need to be competent in its implementation.

REFERENCES

[1] J. Peccoud, J. E. Gallegos, R. Murch, W. G. Buchholz and S. Raman, "Cyberbiosecurity: From naive risk to awareness," *Trends in Biotechnology*, vol. xx, no. yy, pp. 1-4, 2018, doi: 10.1016/j.tibtech.2017.10.012.

[2] R. Murch and D. DiEuliis, "Editorial: Mapping the cyberbiosecurity enterprise," *Frontiers in Bioengineering and Biotechnology*, vol. 7, no. 235, pp. 1-2, 2019, doi: 10.3389/fbioe.2019.00235.

[3] L. C. Richardson, N. D. Connell, S. M. Lewis, E. Pauwels, and R. S. Murch, "Cyberbiosecurity: A Call for Cooperation in a new threat landscape," *Frontiers in Bioengineering and Biotechnology*, vol. 7, no. 99, pp. 1-5, 2019, doi: 10.3389/fbioe.2019.00099

[4] R. S. Murch, W. K. So, W. G. Buchholz, S. Raman, and J. Peccoud, "Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy," *Frontiers in Bioengineering and Biotechnology*, vol. 6, no. 39, pp. 1-6, 2018, doi: 10.3389/fbioe.2018.00039.

[5] National Academies of Sciences, Engineering, and Medicine, "Safeguarding the Bioeconomy," *The National Academies Press, Washington*, DC, 2020, doi:10.17226/25525.

ISSN (online): 2581-3048
Volume 6, Issue 2, pp 75-79, February-2022
https://doi.org/10.47001/IRJIET/2022.602013

[6] D. S. Schabacker, L.-A. Levy, N. J. Evans, J. M. Fowler, and E. A. Dickey, "Assessing cyberbiosecurity vulnerabilities and infrastructure resilience," *Frontiers in Bioengineering and Biotechnology*, vol. 7, no. 61, pp. 1-12, 2019, doi: 10.3389/fbioe.2019.00061.

[7] K. Millett, E. d. Santos and P. D. Millett, "Cyber-biosecurity risk perceptions in the biotech sector," *Frontiers in Bioengineering and Biotechnology*, vol. 7, no. 136, pp. 1-4, 2019, doi: 10.3389/fbioe.2019.00136.

[8] S. Mueller, "Facing the 2020 Pandemic: What does cyberbiosecurity want us to know to safeguard the future?," *Biosafety and Health*, vol. 3, no. 1, pp. 11-21, 2020, doi: 10.1016/j.bsheal.2020.09.007.

[9] P. F. Walsh, C. Haggenmiller and T. Franke, "Threats, Risks, and Vulnerabilities At the Intersection of Digital, Bio, and Health," *Scientific and Academic Publishing, Walldorf, 2021*. https://www.researchgate.net/publication/352478030_Threats_Risks_and_Vulnerabilities_At_the_Intersection_of_Digital_Bio_and_Health

[10] S. R. Jordan, S. L. Fenn and B. B. Shannon, "Transparency as Threat at the Intersection of Artificial Intelligence and Cyberbiosecurity," *IEEE Computer Society, Washington,* D.C., 2020, doi: 10.1109/MC.2020.2995578.

[11] J. L. Mantle, J. Rammohan, E. F. Romantseva, l. J. T. Welch, L. R. Kauffman, J. McCarthy, J. Schiel, J. C. Baker, E. A. Strychalski, K. C. Rogers, and K. H. Lee, "Cyberbiosecurity for biopharmaceutical products," *Frontiers in Bioengineering and Biotechnology*, vol. 7, no. 116, pp. 1-7, 2019, doi: 10.3389/fbioe.2019.00116.

[12] J. C. Reed and N. Dunaway, "Cyberbiosecurity implications for the laboratory of the future," *Frontiers in Bioengineering and Biotechnology*, vol. xx, no. yy, pp. 1-27, 2019, doi: 10.3389/fbioe.2019.00182

[13] A.M. George, "The national security implications of cyberbiosecurity," *Frontiers in Bioengineering and Biotechnology*, vol. 7, no. 51, pp. 1-4, 2019, doi: 10.3389/fbioe.2019.00051.

[14] B. C. Wintle, C. R. Boehm, C. Rhodes, J. C. Molloy, P. Millett, L. Adam, R. Breitling, R. Carlson, R. Casagrande, M. Dando, R. Doubleday, E. Drexler, T. E. Brett Edwards, N. G. Evans, R. Hammond, J. Hasseloff, L. Kahl, T. Kuiken, B. R. Lichman, C. A. Matthewman, J. A. Napier, S. S. ÓhÉigeartaigh, N. J. Patron, E. Perello, P. Shapira, J. Tait, E. Takano and W. J. Sutherland, "A transatlantic perspective on 20 emerging issues in biological engineering," *Elife*, vol. 6, no. 30247, pp. 1-21, 2017, doi: 10.7554/eLife.30247.

[15] L. C. Richardson, S. M. Lewis, and R. N. Burnette, "Building capacity for cyberbiosecurity training," *Frontiers in Biotechnology and Bioengineering*, vol. 7, no. 112, pp. 1-5, 2019, doi: 10.3389/fbioe.2019.00112

AUTHOR'S BIOGRAPHIES

Dr. Alex's areas of expertise include Cybersecurity, Cybercrimes Investigations, Security in Next Generation Networks, Smart Technologies, IoT Azure solutions& security best practices/governance, wrangling the explosion of data from the Internet of Things, Unsecure cloud backend system, unsecure mobile connections, IoT of Healthcare challenges, Security Industry standards (ISO 17799, ISO 31000, ISO/IEC 27001/2 series), HIPPA, Bots and security and Digital Forensics Investigation. He is a Certified Information Systems Security Professional and the founder of several cyber security awareness initiatives and consultant in India, Asia, Cyprus and Middle East. With over 20 years, experience of consulting and training has developed a large skill set and certification set. He was instrumental initiating and organizing a number of conferences, implementation of incubation centers. He has 100+ publications with IEEE, ACM and Scopus Indexed International Journals. Dr.Alex has received a number of awards including the Best Professor, Best Presenter, Outstanding Researcher, Excellence Awards etc. He is a frequently invited speaker and panelist, reviewer at International conferences related to Cybersecurity, Technology, Innovation and education. He has a persuasive, open style with others, and develops interpersonal relationships quickly and relatively easily.

Hannah Alex, I am currently studying at Brooke high school as a junior student, in West Virginia, USA. Within the short span of 17 years, I have been studying and traveling over 8 countries/ 3 continents around the globe. I explored different cultures and initiated to learn 7 different languages. I'm a registered multiple "World Record" holder in different categories. I'm a motivated learner and ready to take on any challenges.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 6, Issue 2, pp 75-79, February-2022

https://doi.org/10.47001/IRJIET/2022.602013

Citation of this Article:

Dr. Alex Mathew, Hannah Alex, "Cyberbiosecurity as the Foremost Biological Weapon to the Digital World" Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 6, Issue 2, pp 75-79, February 2022. Article DOI https://doi.org/10.47001/IRJIET/2022.602013

****

