An Exploration on Advanced Persistent Threats in Biocybersecurity and Cyberbiosecurity

Xavier-Lewis Palmer^{1,2}, Lucas Potter¹ and Saltuk Karahan²

¹Department of Biomedical Engineering, Old Dominion University, Norfolk, VA, USA

²School of Cybersecurity, Old Dominion University Norfolk, VA, USA

xpalm001@odu.edu

lpott005@odu.edu

skarahan@odu.edu

Abstract: Novel and complex digital threats that are increasingly interwoven with means and products of biology that can affect society. Much work in Biocybersecurity/Cyberbiosecurity (BCS/CBS) discuss vulnerabilities, but few deeply address malicious actor varieties as attacks at this intersection are new. The path to those attacks remains mostly theoretical, presenting considerable difficulty to accomplish in practical scenarios. In terms of advanced persistent threats (APTs) this of course needs to change as biomanufacturing facilities are at risk, considering Covid-19 and other potential pandemics. Further attacks are not out of reach and thus we must start to imagine how BCS APTs may appear. This paper in progress aims to open discussion regarding the definition of the concept BCS/CBS APTs and their implications, as well as create call to action for increased attention.

Keywords: Biocybersecurity, Cyberbiosecurity, Covid-19, Cybersecurity, Biosecurity, Biomanufacturing,

1. Introduction: BCS/CBS and Security Studies

Cybersecurity has already found its place within security studies and is explicitly stated in several national security documents with an increasing level of emphasis for the past two decades (Berger and Roderick, 2014). The most recent Interim National Security Strategic Guidance of the Biden administration lists cyber and digital threats along with pandemics and biological risks after stating that “recent events show all too clearly that many of the biggest threats we face respect no borders or walls, and must be met with collective action.” (Biden, 2021). It is also stated in the same document that cybersecurity is to be made “a top priority, strengthening our capability, readiness, and resilience in cyberspace”.

As the cyber domain has an increasing presence in security studies, new subdomains gain significance as well. Social Cybersecurity defined as “an emerging scientific area focused on the science to characterize, understand, and forecast cyber-mediated changes in human behaviour, social, cultural, and political outcomes” has been seen as an emerging subdomain (Carley et al, 2018). Similarly, biocybersecurity is another such subdomain which has the potential to influence our understanding of warfare with its unique nature encompassing several aspects of biology and information technology. While there is still not a clear explanation for the rare use of biological warfare throughout history, the risk of attribution and only a few state actors’ access to the technology (considering these were accountable actors) were among the possible explanations for this rare use (Carus, 2017). However, the advancement in biotechnology has the potential to change this fact when the effects of biocybersecurity is considered. This fact has become even more prominent as we started to see the use of biological components as a target by APTs. APTs are often associated with state actors who can fund such sophisticated attacks and could have long term political goals to be gained from these attacks. The trend in the conduct of APTs further reinforces the necessity to reconsider BCS/CBS as influential subdomains within cybersecurity. While early attempts within bio-cyber APTs were limited to the disinformation campaigns, the recent trends include interventions into biotechnological systems and the conduct of these interventions at scale is looming in the horizon. Furthermore, the access to the biocyber attack capabilities by rogue states and terrorist organizations has significantly increased due to the nature of all cyber-attack capabilities. In the next section, we will look further into the world of APTs in biocybersecurity.

2. BCS/CBS and APTs

Moves of APTs are rather easy on the behalf of state actors because they have the resources to supply for multiple, well-outfitted, and long-lasting teams. Establishing control can take place through the deployment of a combination of moves in social media or bioeconomic systems from social engineering. From there, teams can establish their place within a system and use it as a launching point. Well placed malware, social media campaigns, and or employees can be used to deepen presence and permanence in society. Eventually, the APT

finds a groove in a consistent system for examining the network, extracting or attacking assets, and keeping its footing more securely. However, some APTs can re-attack in coming in the form of a different group or at a different time, with better resources. The persistent nature cannot be understated. This is a general workflow and is something to be contended with by more of the bioeconomy, and this became apparent in 2021 with the finding of Tardigrade, a metamorphic, semi-autonomous APT used to target biomanufacturing facilities as revealed by Bioeconomy Information Sharing and Analysis Center (Newman, 2021).

3. Insights Taken from Leading Experts Across Academia, Government, and the Private Sector

In addition to Peccoud et al's (2018) and Murch et al's (2018) initiation and spurring of the conversations on the blurred territory of cybersecurity, biosecurity, and cyber-physical security, Reed and Dunaway (2019) delivered a further exploration of labs of the future, finding that governments still face significant challenges in preparation for the unique threats that Cyberbiosecurity presents. This is in agreement with George (2019) who reflected on posed national security implications as these core technologies continue to converge in use. This concern is amplified through findings of Millett et al (2019) who explored perceptions of risk in the Biotech sector through a study which surveyed anonymized leaders in biotechnology and biosecurity, concerning perceived risks. Their work revealed that a considerable number of the participants had difficulty assessing risks to their organizations in the face of cyber-related threats. Some experts surveyed were unaware of dedicated resources that could be used to mitigate risks in biotechnology, and many believed that more time and resources are needed to be dedicated. A broader picture revealed that there are considerably wide gaps for malicious actors to take advantage of. As the poll was online and limited, further research is necessary; however, concerns reliably exist among the question of who is most unprepared. This altogether, indicates need for a closer look at the state of biomanufacturing and need for surgical reassessments of infrastructure.

Mueller (2020) discussed at length challenges that COVID--19 introduced, highlighting bioeconomy diversity and that they contain unique elements that require further assessment. It's important to note that the networks and interactions of components of vital elements such as agriculture, animal husbandry, restaurants, pharmacies, and processing plants will differ by locale and subjected policies. These are each further open to compromise in part due to varying pressures that pandemics impose on the relevant populations. Mueller gave recommendations on responding to cyber-bio convergences, which benefit from cross-discipline insights; follow through on these recommendations are vital given that allowed incomplete public awareness of relevant cyber-bio convergent potential and their potential routes to affect key public institutions and businesses, combined with wide gaps in expertise across fields that comprise BCS /CBS can sustain vulnerabilities that can be exploited by malicious actors. This is especially critical in the ongoing management of Covid-19, considering shifting vaccine availability and heightened importance of the facility capacity available to administer care. Jordan et al (2020) expanded security conversation in this space through artificial intelligence as bioeconomies are open to novel AI/ML threats. When considering AI, one needs to consider competing ethics at play within computing, and biological data. Threats using cyber and bio databases, along with focus on emergent functions require even more careful analysis as grey areas using such research are many and the impact of the threat is not easy to see. Jordan et al (2020) lists low to high-risk national security phenomena relating to data, using demonstrated and possible cases of exploits, which show a wide field open to defend. Proper application of AI algorithms can boost efforts of detecting CBS/BCS threats, but also improve the quality of malware created, morphing and accelerating the BCS/CBS landscape. This altogether enhances APT risks for biomanufacturers and as actors apply this technology with increasing efficiency. Tardigrade may just be only the APT successfully detected, with many others out there potentially in development. Questions of when biocomputing aided APTs may emerge within biological systems are valid as relevant technique and capacity become increasingly available.

4. Proposed Approach to BCS/CBS and Concluding Thoughts

Starting from the understanding of biocyber threat, there are several measures that can be taken to secure ourselves from threats within BCS/CBS subdomain. These measures extend from BCS/CBS advocacy to further study of means of detection and building capacity (and resilient infrastructure) within this subdomain. Examining the security implications of big data in life sciences, "vulnerabilities of datasets to cyber intrusion and design of biological weapons derived from the integration and analysis of Big Data in the life sciences" has been listed as one of the risks associated (Berger and Roderick, 2014). Considering the fact that "computers can be compromised by encoding mal-ware in DNA sequences, and bio-logical threats can be synthesized using publicly available data" as stated by Peccoud et al., there needs to be further research in policy guidelines and detection

mechanisms (Peccoud et al, 2018). Considering the intrinsic link between biotechnology and computing, advanced infrastructure investment and capacity building remain necessary steps. There have already been recommendations for this including incentivizing biotech companies, cyber-centers for disease control and prevention, mandating gene guard systems, and consumer education (Pauwels and Vidyarthi, 2016). While the foundational contribution of existing approaches in disciplines linked to biocybersecurity are recognized, their incompetency in capturing particularly “the emergent features related to biological and biomedical systems” necessitates a genuine approach (Schabacker et al, 2019). Further infrastructure development should include education and reassessment that focuses knowledge on both modern and emergent cyber-bio gaps and policies in terms of incentives, along with updated regulation in infrastructure designs and deployment, where most critical to national security. Beyond these measures at the detection or infrastructure or regulation levels, a stronger and wider awareness campaign highlighting increased cyber-bio convergence is needed regarding BCS/CBS subdomain when the increasing potential APT attacks to occur in this field are considered. This awareness can only be accomplished with further advocacy in the recognition of the field as a significant subdomain of cybersecurity, increasing discussion of vulnerabilities, threats and policy topics in academic circles and government entities.

5. Future Work

2018 National Biodefense Strategy mentions the word “cyber” only twice throughout the 30 page document. Those two referrals are in the contexts of including cybersecurity in “strengthening biosafety and biosecurity practices” and “ensuring the safety, security, and reliability of supply chains to provide necessary medical countermeasures and other materiel support during bioincidents”. The authors argue that considering the increasing ransomware like attacks at medical facilities, increasing reliance on technology and increasing expectation for genetic screening to be part of preventative care, cybersecurity should be considered and essential component of biosecurity or biodefense and this should be reflected in strategy documents.

Department of Health and Human Services has the leading role in the governance of biosecurity and Presidential Memorandum on the Support for National Biodefense (NSPM-14) accompanied the issuance of the National Biodefense Strategy. As indicated in the National Biodefense Strategy, NSPM -14 “creates a dedicated mechanism to coordinate federal biodefense activities and assess the effectiveness with which the National Biodefense Strategy’s goals and objectives are being met.” While establishment of a dedicated mechanism is very promising, the increasing link between cybersecurity, biosecurity and national security requires a clear and stronger multi-agency involvement and a coordinated effort in building strategy. With its national security, economic and political dimensions, and the increasing sophistication of biocyber attacks, the sources of the attacks weigh towards intentional attacks from nation states rather than naturally occurring and accidental outbreaks. The future work in this topic would include a survey of existing mechanisms for an effective coordination and cooperation, determination of the gaps in strategy and policy and recommendations on how to approach the biocybersecurity problem.

References

- Berger, K. M., & Roderick, J. (2014). National and transnational security implications of big data in the life sciences. Washington, DC: American Association for the Advancement of Science.
- Biden Jr, J. R. (2021). Interim National Security Strategic Guidance. Executive Office of the President, Washington DC.
- Carus, W. S. (2017). A short history of biological warfare: from pre-history to the 21st century (Vol. 12). Government Printing Office.
- George, A. M. (2019). The national security implications of cyberbiosecurity. *Frontiers in bioengineering and biotechnology*, 7, 51.
- 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.
- Karahan, S., Wu, H., & Armistead, L. (2019). Evolution of US cybersecurity strategy. In *International Conference on Cyber Warfare and Security* (pp. 168-176). Academic Conferences International Limited.
- Kathleen M. Carley et al. (2018) “Social Cyber-Security,” in *Social, Cultural, and Behavioral Modeling: 11th International Conference, SBP- BRiMS 2018*, Washington, DC, USA, July 10–13, 2018, *Proceedings*, ed. Halil Bisgin et al. (New York: Springer, 2018), 389–94.
- Millett, K., Dos Santos, E., & Millett, P. D. (2019). Cyber-biosecurity risk perceptions in the biotech sector. *Frontiers in bioengineering and biotechnology*, 7, 136.
- Mueller, S. (2020). Facing the 2020 Pandemic: What does Cyberbiosecurity want us to know to safeguard the future?. *Biosafety and Health*.

- Murch, R. S., So, W. K., Buchholz, W. G., Raman, S., & Peccoud, J. (2018). Cyberbiosecurity: an emerging new discipline to help safeguard the bioeconomy. *Frontiers in bioengineering and biotechnology*, 6, 39.
- Newman, L.H., (2021) Devious 'Tardigrade' malware hits biomanufacturing facilities. *Wired*. Available at: <https://www.wired.com/story/tardigrade-malware-biomanufacturing/> [Accessed November 25, 2021].
- Pauwels, E., & Vidyarthi, A. (2016). How Our Unhealthy Cybersecurity Infrastructure is Hurting Biotechnology. *Wilson Briefs*. Washington, DC: The Wilson Center.
- Peccoud, J., Gallegos, J. E., Murch, R., Buchholz, W. G., & Raman, S. (2018). Cyberbiosecurity: from naive trust to risk awareness. *Trends in biotechnology*, 36(1), 4-7.
- Reed, J. C., & Dunaway, N. (2019). Cyberbiosecurity Implications for the Laboratory of the Future. *Frontiers in bioengineering and biotechnology*, 7, 182.
- 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, 61.