2024

Different Visions from BiosView: A Brief Report

Lucas N. Potter
Old Dominion University, lpott005@odu.edu

Xavier-Lewis Palmer
Old Dominion University, xpalmer@odu.edu

Original Publication Citation

Potter, L. N., & Palmer, X.-L. (2024). Different visions from BiosView: A brief report. In D. N. Burrell (Ed), *Change Dynamics in Healthcare, Technological Innovations, and Complex Scenarios*. IGI Global. https://doi.org/10.4018/979-8-3693-3555-0.ch008

Chapter 8
Different Visions From BIOSView:
A Brief Report

Lucas Potter
Old Dominion University, USA

Xavier-Lewis Palmer
BiosView Labs, USA

ABSTRACT

In this collaborative research endeavor at the intersection of biological safety and cybersecurity for BiosView labs, the authors highlight their engagement with a diverse student cohort. The chapter delves into the motivation behind collaborations extending beyond traditional academic research environments, emphasizing inclusivity. The meticulous examination of student demographics, including gender, self-reported ethnicity, and national origin, is detailed in the methodology. A student-centric approach is central to the exploration, focusing on aligning teaching and management styles with unique student needs. The chapter elaborates on effective teaching methodologies and management practices tailored for BiosView labs. A dedicated section emphasizes the purpose of joint endeavors, featuring a thoughtfully crafted questionnaire that guides collaborations towards both educational and personally meaningful outcomes for students.

INTRODUCTION

Agriculture, bioenergy, pharmaceuticals, industrial biomaterials, and more – items that are fundamental to sustaining humanity comprise the economic subjects that researchers call the Bioeconomy. Since the end of the 20th century, societies have witnessed an increasing convergence of digital interfacing with the bioeconomy for improved processing, logistics, and commerce of biological products (Murch, So, Buchholz, Raman, & Peccoud, 2018). This was fantastic for both consumers and providers, as the benefits of digitization and digital interfacing begat many new and innovative features for both parties.

DOI: 10.4018/979-8-3693-3555-0.ch008

There was the creation of better means to monitor the quality of products, track, interact, and trade them. Faster speeds or deeper resolutions would become available. However, with increasing digitization and digital interfacing of elements of the bioeconomy comes the increasing vulnerability of said systems to malicious agents operating on digital platforms to cyber-attacks (Potter & Palmer, Human factors in biocybersecurity wargames, 2021; Murch & DiEuliis, 2019). Realizations of this are apparent through growing attacks on bioeconomic supply chains and researchers provide demos of additional problematic bases that could potentially occur.

Contemplation of cybersecurity cases involving the bioeconomy having their own, hybrid section has deeply prompted considerable discussion and debate. Further, as links of chains in biological cyberattacks became more realistic, these discussions intensified resulting in the terms "Cyberbiosecurity" and "Biocybersecurity," and hyphenated alternative versions, appearing in literature within the 2010s. The initial works trickled in, and the field would see publication titles bearing the aforementioned names towards the late 2010s, with the first recognized paper being release in 2017 (Peccoud, Gallegos, Murch, Buchholz, & Raman, 2017; Murch, So, Buchholz, Raman, & Peccoud, 2018).

A key practical work to show that a hybrid field was necessary versus couching concerns of biosecurity concerns within the domain of all current cybersecurity practitioners would be helpful. A pivotal work among several that changed this, became just that, "Computer Security, Privacy, and DNA Sequencing: Compromising Computers with Synthesized DNA, Privacy Leaks, and More" by Ney et al, 2017, energized plenty in the research community in showing that biological materials could be a meaningful interlock in cybersecurity attacks, among other findings through demonstration of DNA, a biomaterial, being useful for execution of a remote cyber-attack (Ney, Koscher, Organick, Ceze, & Tadayoshi Kohno, 2017).

This work enhanced the seriousness of discussion; several works followed to expand on work that needed to be done to account for the expanded attack surfaces that were now possible in the world cybersecurity. Works by Murch (Murch, So, Buchholz, Raman, & Peccoud, 2018) (Murch & DiEuliis, 2019), Duncan (Duncan, et al., 2022), Reed and Dunaway (Reed & Dunaway, 2019), Schabacker (Schabacker, Levy, Evans, Fowler, & Dickey, 2019), DiEuliis (DiEuliis, 2019), Millet and Dos Santos (Millett, Santos, & Millett, 2019), and many others would both map and deeply expand on the nature and importance of the widened attack surface to the bioeconomy that was presented, prompting calls to secure it. George (George, 2019) and Reed and Dunaway (Reed & Dunaway, 2019) would expand on the national security implications. Many, also from Virginia Polytechnic Institute and State University, would highlight additional critical needs for novel education drives to expand audiences and practitioners, as well as bridge gaps between biological and cybersecurity related domains (Adeoye, et al., 2023). During this same period, the authors, while PhD Candidates in Biomedical Engineering and having backgrounds in cybersecurity and human-factors engineering between them, were also working on potential contributions to the field as well. Two points were captured early on by them that were important, reflecting on the national security implications of having an intellectually and view-point diverse coalition: 1) Biological materials and signatures as interlocks in cybersecurity chain of attacks are underexplored, greatly expand (and dwarf) the attack surfaces available in traditionally cybersecurity attack libraries, and their inclusion might eventually require their own category from a mission POV 2) Considerable cybersecurity foci are primarily aimed at populations with traditional access to infrastructure and thus can be ignorant of approaches engaged by "underground", under-resourced/underrepresented/intentionally excluded group; the second of these points was further recognized in part and given further depth by Burrell and McAndrew (Burrell & Mcandrew, 2023). Their preferred focus was thus Biocybersecurity

as a term but would oscillate on focus and value throughout various uses not limited to publishing, and workshops. Unpublished works began in 2018, followed by their first poster at the 2019 CEPE (Computer Ethics—Philosophical Enquiry) conference in 2019, in Norfolk, Virginia through collaboration with a faculty member.

Published works would soon follow as confidence was built, pulling in collaborations with willing parties who were both traditionally and non-traditionally in cybersecurity. Their first non-conference-based book chapter would be published in 2023 (Potter & Palmer, Mission-Aware Differences in Cyberbiosecurity and Biocybersecurity Policies: Prevention, Detection, and Elimination, 2023). They would eventually discuss Cyberbiosecurity and Biocybersecurity within Community Bio Conferences and Summits, one of which being the Global Community Bio Summit, in aims of helping Community Biologists sharpen their digital foci on security, within their works. As discussions of Cyberbiosecurity became more common and accessible, they would attend some of these events and integrate into discussions with the community attending events held at universities and research institutes in Virginia, Georgia, Massachusetts, and virtually abroad, connecting to researchers from various nations. An unofficial virtual lab called BiosView Labs was formulated that would pursue collaborative projects, preferably with those who had unique, non-traditional perspectives and backgrounds. In their collaborative research efforts within the multitude of collaborations at the nexus of biological safety and cybersecurity for BiosView labs, the authors of this chapter have had the privilege of working with a diverse group of students. In this comprehensive exploration, their aim is to paint a vivid picture of several features of these collaborations.

For a further exploration into the definitional issues associated with bio-cybersecurity and cyberbiosecurity, please refer to previous work (Potter & Palmer, Mission-Aware Differences in Cyberbiosecurity and Biocybersecurity Policies: Prevention, Detection, and Elimination, 2023). For additional knowledge on specific BCS and CBS threat domains and vectors, refer to the following publications (Palmer, Potter, & Karahan, COVID-19 and biocybersecurity's increasing role on defending forward, 2021), (Potter, Ayala, & Palmer, Biocybersecurity: A Converging Threat as an Auxiliary to War, 2021), (Samori, Palmer, Potter, & Karahan, 2022), (Affia, et al., 2023), (Palmer, Potter, & Karahan, An Exploration on APTs in Biocybersecurity and Cyberbiosecurity, 2022), (Palmer, Powell, & Potter, Biocyberwarfare and Crime: A Juncture of Rethought, 2021), (Palmer, Powell, & Potter, 2021), (Stephen, Alexander, Potter, & Palmer, 2023), (Griffin, Alexander, Potter, & Palmer, 2023), (Finch, Affia, Jung, Potter, & Palmer, 2023), (Potter, Powell, Ayala, & Palmer, 2021), (Powell, Akogo, Potter, & Palmer, 2022), (Potter, Mossburg, & Palmer, A Reflection on Typology and Verification Flaws in Consideration of Biocybersecurity/Cyberbiosecurity: Just Another Gap in the Wall, 2023), (Potter & Palmer, Post-LLM Academic Writing Considerations, 2023), (Westberry, Palmer, & Potter, 2023), (Barnett, Samori, Griffin, Palmer, & Potter, 2023), (Samori, Odularu, Potter, & Palmer, 2023), (Potter, Shetty, Karahan, & Palmer, 2024). These works are not exhaustive of all past, current, submitted, accepted, and projected works. Literature is to follow this case report in a separate work when the authors or others deem the hybrid field matures enough for a thorough analysis.

The efforts to contribute to another pipeline of cybersecurity professionals is part of an ongoing program to fill in the gap left behind by conventional educational establishments, as seen previously (USA DHS-CISA, 2024). One sub-type of educational programs, referred to as "Bootcamps" are an alternative to traditional educational institutions. To wit: "Furthermore, bootcamps take a relatively shorter time to complete and, in many instances, part-time bootcamp solutions can be completed while the participants continued their full-time jobs" (Caliskan & Vaarandi, 2020). The very content imparted during the typical cybersecurity curriculum is being questioned (Erickson & Kim, 2021). Additionally,

the proposed "High-Impact Practices" of teaching cybersecurity at academic institutions (Payne, Mayes, Tish, Wu, & Xin, 2021) are clearly flawed, considering the evidence of cybersecurity breaches in higher education (Ulven & Wangen, 2021).

The average cost of a breach for a university was 3.5 million USD (IBM Security, 2023). As astounding as it may sound, it is somewhat less than the salary of at least 50 of the highest paid football coaches in the US (USA Today), The privacy of the university and student body data should arguably take precedence over a football program. There should be a call to invest in the security of data within our universities which could be significantly lower than the cost of a breach. However, further discussion of economic analysis of data breaches concerning college informational infrastructure is reserved for potential future work.

Despite the lack of CBS and BCS relevant education in typical institutes of higher learning, to the author's knowledge, only three universities offer studies or coursework on BCS. Those being Colorado State University (Colorado State University, 2024), Virginia Polytechnic Institute and State University, and Old Dominion University (Johnston, 2021). The motive behind collaborations outside of the typical research environments of academia is demographics. The authors' commitment to inclusivity and student success is underscored by a meticulous examination of the gender, self-reported ethnic breakdown, and national origin of the individuals the authors have collaborated with (reported in methodology). Diversity is approached to ensure that more helpful perspectives are sought which is essential for both national and international security The authors took care to align their teaching and management style with the unique needs of the students in a way that imparts valuable knowledge and skills, while fostering a conducive learning environment. This section of the authors' exploration will provide a detailed account of the teaching methodologies employed, shedding light on the intricacies of the authors' management style that has proven to be effective in the dynamic landscape of BiosView labs.

As part of the authors' commitment to student-centric collaboration, the authors have integrated an extended section focusing on the purpose of the authors' joint endeavors. Central to this exploration is a questionnaire meticulously crafted to gauge the authors' students' goals, to ensure that the authors' collaborative efforts are not only educational but also aligned with the individual aspirations of each student. The questionnaire serves as a compass, guiding the authors' collaborative efforts towards outcomes that are not only academically enriching but also personally meaningful to the authors' students.

PROBLEM STATEMENT

There appears to be a public perception in the US. that research can only be done at an academic institution. This is false. There are scientists that may openly and at length admit that their curiosity and love of knowledge came prior to obtaining a higher education or enjoying the academic environment. However, due to the current constraints on academic positions in the US - namely a 'Cult of Ignorance' (Asimov, 1980), and a marked decrease in local and state funding for US universities considering the additional massive increase in tuition charged (US Bureau of the Census, 2022), many students with little or no background in how research is conducted find themselves trapped in research holes that offer the illusion of research with no real scientific validity (Ballantyne, 2022). That is of course, if they can find any research on the topic which can in fact be replicated (Ioannidis, 2005). And when one does attempt to make it past the extant hurdles into academia, they are met with a morass of ill-defined goals with precious little oversight of neigh-unfireable professors and a famously toxic work environment (Henkle,

2021) which has lead in recent years to historic and much needed labor strikes in academia (Langin, 2023). Graduate school in the US then rewards those dedicated enough for navigating a byzantine structure of toxic workplaces and aristocratic professors (Burke, 2021) with historically bad job prospects (Malloy, Young, & Berdahl, 2021). Meanwhile, there has existed concerning level of burnout among PhD students for years – who will lift them, and those earlier on the ladder, up? (Woolston, 2017; Nagy, et al., 2019). A well-meaning, kind person in these situations will help another person, but a kind person in a toxic environment will soon find their kindness rejected by the perpetrators of that environment. For the benefit of improving learner outcomes, different paths of mentorship are encouraged.

Increased funding for biocybersecurity researchers should be considered as academia is currently formulated. It could increase the speed of the current course of study, help replication of research, and promote a workplace conducive to producing value. The current climate does not appear to be true. Earlier works identified some of these issues as a problem of demographics (Burrell & Mcandrew, 2023). The significance of this issue cannot be overstated: A solid cybersecurity strategy at a national level must include diverse perspectives from different populations in order to defend forward (Palmer, Potter, & Karahan, COVID-19 and biocybersecurity's increasing role on defending forward, 2021) to defend against the converging threats of biosecurity and cybersecurity (Potter, Ayala, & Palmer, Biocybersecurity: A Converging Threat as an Auxiliary to War, 2021). Ideas from areas with undiscovered biological assets (Samori, Palmer, Potter, & Karahan, 2022) and unique cybersecurity considerations (Samori, Palmer, Potter, & Karahan, 2022) must be fully integrated into a coherent Biocybersecurity strategy in order to formulate a complete protection strategy in the context of BCS.

METHODOLOGY

The authors' solution was to seek students in retraining or alternate training pipelines, giving them a crash course in research, and showing them how to produce novel and valid research in a supportive environment while permitting them to work at their own pace, schedule, and execution. We definitively rejected hierarchies based on seniority and were amenable to changing research topics as desired by the collaborator. This will be expanded on in the discussion section below. The authors reported the demographic breakdown of the authors' student population. The following data was gathered via self-reporting. Each instance of a collaborative work (i.e., authorship on a conference or academic proceeding) was counted separately. Despite only having twelve collaborators, there are twenty-four total entries. The two authors of this work were excluded from this report. Entries additionally excluded from this report are ones with only senior collaborators (who were all male and from non-US origins) and works in the process of being published.

As can be seen, the gender breakdown was roughly 1:1 male to female. Despite the authors' efforts to serve a wide-ranging population, the cybersecurity field does trend to be male, and the authors' ability to reach out to female students was limited.

Many of the students in the CySecSol (Now Cyberlinc (CyberLinc, 2024) pipeline was local to Norfolk, Virgina. As such, many were African American. Notably, all 4 Caucasian collaborators were female.

Most of the collaborators outside of the United States up until 2023 were from West Africa, among countries such as Ghana and Nigeria. They were either met as secondary connections through classes, conferences, or through by mention or collaborations with informal, but community-facing STEM professionals. Additional conference meetups resulted in an expansion of the collaborator account and

diversity largely through partnerships with professionals from The Philippines, resulting in publication between 2023 and 2024 and hopefully to be published over the course of 2024. Figure 4 shows expanded collaboration demographics by both ethnicity and gender, but it should be noted that this does not account for numerous presentations and workshops supported and engaged. In-person workshops and presentations were all conducted domestically. Some virtual workshops and presentations were conducted for community facing STEM organizations led by students and young professionals in and or from countries including, but not exhaustive of The United States of America, Ghana, India, Bangladesh, and Nigeria, for example.

Figure 1. Self-reported gender of collaborators

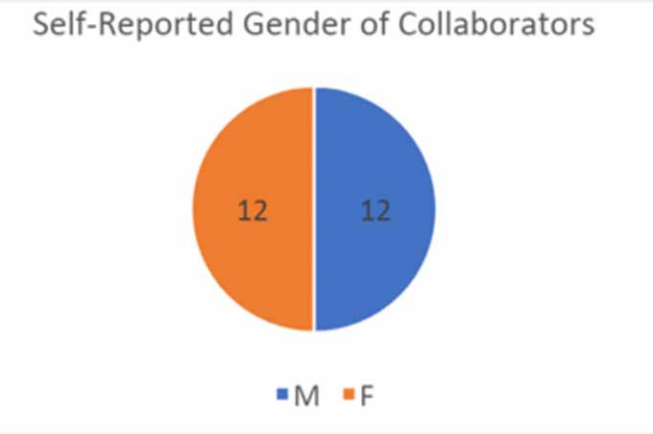


Figure 2. Self-reported ethnicity of collaborators

Figure 3. National origin of collaborators

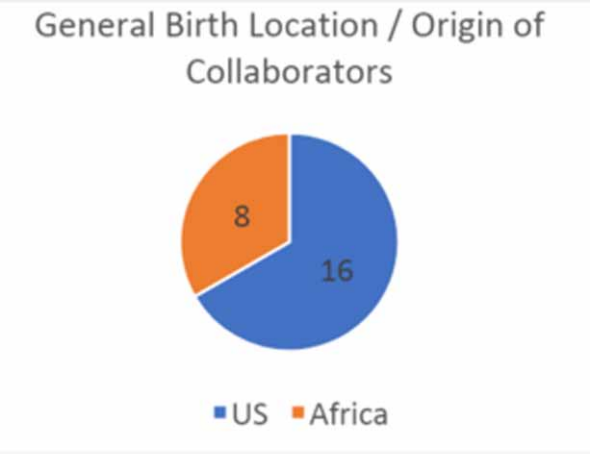
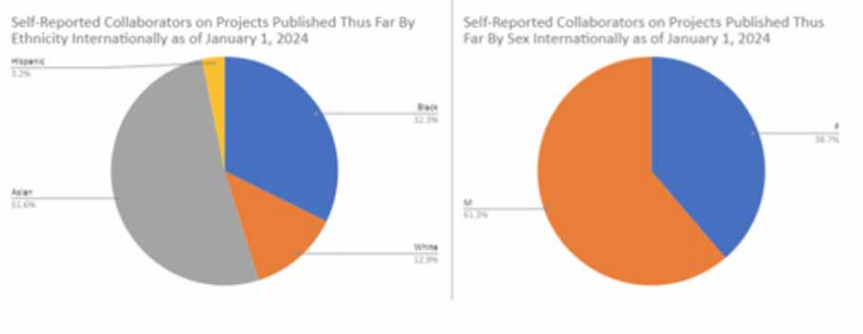


Figure 4. Self-reported ethnicity and gender of collaborators who have published with BiosView into 2024



Domestic collaborations are still set to continue and dominate over the course of 2024. Figure 5 below shows that two thirds of the authors' collaborators remain from North America, specifically the United States of America. Figure 6 shows that the Sex divide may not change significantly, but this may be addressed through improvements in networking. As it stands, BiosView's collaboration record tends to beat paid organizations with regards to STEM engagement ratios. Further, the authors remain committed to assisting underserved perspectives as the authors have the opportunity to address. The authors' meetings and collaborations reflect organic meetings and their projects have largely been at cost to them vs other sources. Outside funding could improve targeting, but for now, the authors remain committed to consenting, enthusiastic, and organic projects led by students interested in pursuing their hobby and or career interests.

The authors were able to 'meet them where they were. This allowed them to focus on helping them prepare and apply for positions outside academia with the possibility of being well-compensated for their work.

Figure 5. Self-reported unique collaborators in projects planned to finish, by continent in 2024

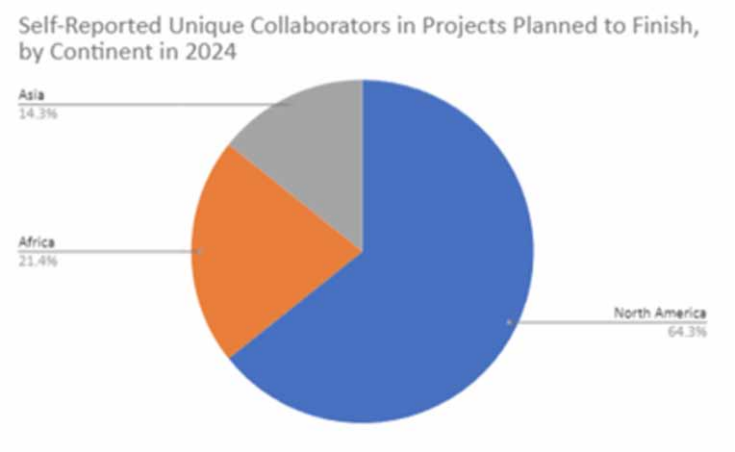
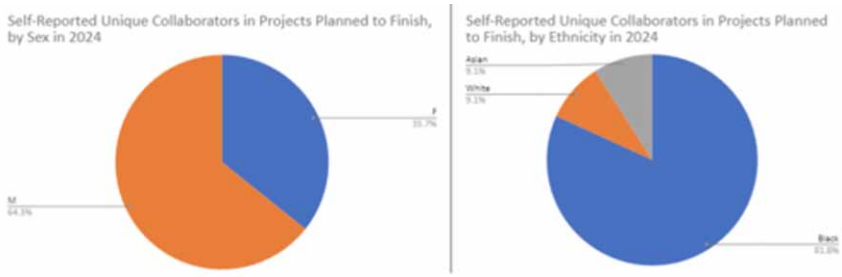


Figure 6. Self-reported unique collaborators in projects planned to finish, by in 2024



Discussion:

The process by which the authors develop research endeavors (usually culminating in a publication) includes background identification, a crucial step in laying the foundation for the authors' collaborative work. This identification involves asking the collaborator what background they have, and what kind of research they are open to doing. For example, even if a person is already an expert in one field) the authors can use that background to explore a new topic that they are interested in (like agriculture (Stephen, Alexander, Potter, & Palmer, 2023)).

The authors will detail their thought processes behind topic selection, providing insights into the considerations that shape the authors' research directions. Additionally, the authors' literature review methods will be elucidated, offering transparency into the authors' approach to staying current in relevant research in the ever-evolving field of BiosView labs. Typically, the authors' topic selection starts with finding a matter important to US National Security that is not often pondered. Further, this topic must be connected to Cyberbiosecurity (CBS) or Biocybersecurity (BCS). That is, the topic must be at the intersection of Cybersecurity, Cyber-physical Security, and Biosecurity. The authors start with free-writing to create paper nuclei by which they can create a full work from and or serve as a springboard for thought on potential collaborators. Quite often, the authors meet enthusiastic practitioners and or students in either sociology, biology/medicine, engineering, and cybersecurity. Usually, they already

have an idea and the authors' works in-progress, prior works, and works of others can be used to support these practitioners. A core principle that the authors maintain when working with collaborators is that everyone keeps an open mind and reads considerably. These practitioners and students are mostly met at Conferences, Summits, and General Meetups. The places tend to be Universities and Conference Halls. Collaborations are mostly virtual over low-cost platforms, which give the authors' teams versatility and agility. The authors' literature review tends to be a deep dive as is reasonable. Due to the lack of publications in Cyberbiosecurity and Biocybersecurity, literature dives tend to be short, unless the topic tends to be of a novel or highly slanted subject.

No collaborative effort is without its challenges, and the authors will candidly share the hurdles encountered during the authors' projects. Equally important, the authors will discuss the strategies implemented to overcome these challenges, demonstrating the authors' commitment to adaptability and resilience in the face of obstacles. The primary issues that the authors had in this endeavor were finding students with availability to learn without financial compensation. While the authors openly admit that unpaid experience or volunteering is not ideal which is not uncommon in the academic setting, all funds went towards sending and supporting collaborators to and from conferences or supporting them in publications. Emphasis was on them finding, where applicable, conferences that were local to the collaborators so that they would be able to attend and present their work if they were able to do so.

A NOTE ABOUT AI

BCS/CBS, traditionally associated with the meticulous safeguarding of technical components within engineering systems, has undergone a paradigm shift in recent years. The landscape has evolved, and the weakest links in the security chain are no longer confined to technological vulnerabilities but extend to the human elements involved. The past decade has witnessed a surge in IT-based attacks exploiting the lapses in cybersecurity hygiene and fundamental security practices; there exists deep implications for infrastructure for all nations as technological developments continue, especially with AI inclusion to the bioeconomy (Sobien, et al., 2023) This shift in focus demands a comprehensive understanding of the evolving threat landscape.

In this dynamic environment, the rise of generative AI models adds a layer of complexity to security concerns. As these models become more accessible, they introduce unique attack vectors, particularly through the propagation of misinformation (Palmer, Powell, & Potter, 2021), (Potter & Palmer, Post-LLM Academic Writing Considerations, 2023), (Westberry, Palmer, & Potter, 2023).

A key facet of the authors' exploration involves the examination of various methods employed to target uniquely vulnerable populations through misinformation campaigns. The authors recognize the need for tailored educational initiatives, especially for technical personnel who play a critical role in fortifying systems against evolving threats. This involves not only demographic selection but also the crafting of misinformation narratives tailored to specific technical fields. By doing so, the authors aim to shed light on the intricate challenges posed by the intersection of generative AI and cybersecurity.

The authors' inquiry extends beyond the technical realm, acknowledging economic inequality as a pivotal factor contributing to these vulnerabilities. Recognizing the lack of diversity in security-linked employment fields, the authors propose solutions to address this disparity. Exploring avenues for enhancing diversity and inclusion, they aim to fortify the sector with a workforce that brings a spectrum of perspectives to the table, thereby strengthening the overall resilience of BCS/CBS systems.

In essence, the authors' exploration navigates the multifaceted landscape of cybersecurity, acknowledging the evolution of threats and the critical role that generative AI plays in misinformation campaigns. By addressing the vulnerabilities tied to human elements, fostering education within technical communities, and advocating for diversity in security-related fields, the authors aspire to contribute to the ongoing dialogue on fortifying BCS/CBS against emerging challenges in the modern era.

ETHICAL CONSTRAINTS

The fundamental issues with engaging in cybersecurity research are relatively simple. Cybersecurity tends towards high very easily scalable problems - an issue on a single service: such as the issue at the core of the infamous Heartbleed (Durumeric, et al., 2014) or Tardigrade (HHS Cybersecurity Program, 2021) threats can rapidly affect thousands of websites, each in turn hosting millions of users. Therefore, the core ethics are immaterial. This is an example analogous to the Prisoner's Dilemma. While an ideal world could agree not to research the damaging ideas present in BCS or CBS, there is no guarantee that the current global socio-political order would agree to such a detente in research. If it were possible, there would be entire genres of weapons that would not exist.

CONCLUSION

The unique aspects of the authors' teaching approach will be highlighted, emphasizing the authors' dedication to student engagement, active participation, and the infusion of cutting-edge research into the learning experience. Moreover, the authors will delve into the feedback mechanisms established, creating a continuous loop for improvement and adaptability to the diverse and evolving needs of the authors' student population.

In presenting this comprehensive overview of the authors' collaborative efforts, the authors' aim is to contribute valuable insights into effective teaching methodologies for BiosView labs. They envision fostering an inclusive learning environment that not only aligns with the academic goals of the authors' students but also propels them toward success in their professional aspirations. Through this exploration, the authors aspire to leave an indelible mark on the landscape of collaborative education, elevating the standard for excellence in BiosView labs.

REFERENCES

Adeoye, S. O., Lindberg, H., Bagby, B., Brown, A. M., Batarseh, F. A., & Kaufman, E. K. (2023). Cyberbiosecurity Workforce Preparation: Education at the Convergence of Education at the Convergence of Cybersecurity and BiosecurityCybersecurity and Biosecurit. *NACTA Journal*, 341–351.

Affia, A.-O., Finch, H., Jung, W., Samori, I. A., Potter, L., & Palmer, X.-L. (2023). IoT Health Devices: Exploring Security Risks in the Connected Landscape. *MDPI IoT*, *4*(2), 150–182. doi:10.3390/iot4020009

Asimov, I. (1980). Cult Of Ignorance. *Newsweek*. https://aphelis.net/wp-content/uploads/2012/04/ASIMOV_1980_Cult_of_Ignorance.pdf

Ballantyne, N. (2022, January 03). Skeptics Say, 'Do Your Own Research.' It's Not That Simple. *The New York Times*. https://www.nytimes.com/2022/01/03/opinion/dyor-do-your-own-research.html

Barnett, M., Samori, I., Griffin, B., Palmer, X.-L., & Potter, L. (2023). A Commentary and Exploration of Maritime Applications of Biosecurity and Cybersecurity Intersections. *European Conference on Cyber Warfare and Security*, (pp. 65-72). IEEE. 10.34190/eccws.22.1.1283

Burke, L. (2021, March 28). *Faculty More Likely to Have Wealthier, Highly Educated Parents*. InsideHigherEd.com. https://www.insidehighered.com/quicktakes/2021/03/29/faculty-more-likely-have-wealthier-highly-educated-parents

Burrell, D. N., & Mcandrew, I. (2023). Addressing Bio-Cybersecurity Workforce Employee Shortages in Biotechnology and Health Science Sectors. US. *Science Bulletin*, *28*(2), 127–141. doi:10.2478/bsaft-2023-0014

Caliskan, E., & Vaarandi, R. (2020). Career Development in Cyber Security: *Bootcamp Training Programs. International Conference on Cyber Warfare and Security*. doi:10.34190/ICCWS.20.080

Colorado State University. (2024, January 01). *Bio-Cybersecurity at CSU*. ColoState.edu. https://www.research.colostate.edu/bio-cybersecurity

CyberLinc. (2024, January 01). *Home*. CyberLinc. https://www.cyberlinc.org

DiEuliis, D. (2019). Key National Security Questions for the Future of Synthetic Biology. *The Fletcher Forum of World Affairs*, *43*(1), 127–143.

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.

Durumeric, Z., Li, F., Kasten, J., Amann, J., Beekman, J., Payer, M., & Halderman, J. A. (2014). The Matter of Heartbleed. *Proceedings of the 2014 Conference on Internet Measurement Conference*, (pp. 475-488). IEEE. 10.1145/2663716.2663755

Erickson, M., & Kim, P. (2021). Designing cybersecurity curriculum: Exploring the need for. *Issues in Information Systems*, *22*(4), 9–20.

Finch, H., Affia, A.-A., Jung, W., Potter, L., & Palmer, X.-L. (2023). Commentary on Healthcare and Disruptive Innovation. *18th International Conference on Cyber Warfare and Security*, (pp. 77-84). IEEE.

George, A. M. (2019). The National Security Implications of Cyberbiosecurity. *Frontiers in Bioengineering and Biotechnology*, *7*(51). PMID:30968020

Griffin, B., Alexander, K., Potter, L., & Palmer, X.-L. (2023). Social-Engineering, Bio-economies, and Nation-State Ontological Security: A Commentary. *18th International Conference on Cyber Warfare and Security,* (pp. 127-142). IEEE. 10.34190/iccws.18.1.1021

Henkle, T. (2021, February 2). Academics are toxic. We need a new culture. The Johns Hopkins University News-Letter. Retrieved from https://www.jhunewsletter.com/article/2021/02/academics-are-toxic-we-need-a-new-culture

HHS Cybersecurity Program. (2021). *BIO-ISAC Tardigrade Amplify Alert. Washington, D.C.: USA - Health and Human Services.* HHS. https://www.hhs.gov/sites/default/files/bio-isac-tardigrade-malware-alert.pdf

Ioannidis, J. P. (2005). Why Most Published Research Findings are False. *PLoS Medicine*, *2*(8), e124. doi:10.1371/journal.pmed.0020124 PMID:16060722

Johnston, R. (2021, April 29). *Eight Virginia universities announce cybersecurity workforce projects.* Workscoop. https://workscoop.com/2021/04/29/eight-virginia-universities-announce-cybersecurity-workforce-projects

Langin, K. (2023, September 5). After historic strike, UC grad students say university isn't honoring pay agreements. *Science*. https://www.science.org/content/article/after-historic-strike-uc-grad-students-say-university-isn-t-honoring-pay-agreements

Malloy, J., Young, L., & Berdahl, L. (2021, June 21). *Ph.D. Oversupply: The System Is the Problem*. InsideHigherEd.com. https://www.insidehighered.com/advice/2021/06/22/how-phd-job-crisis-built-system-and-what-can-be-done-about-it-opinion

Millett, K., Santos, E. D., & Millett, P. (2019). Cyber-biosecurity risk perceptions in the biotech sector. *Frontiers in Bioengineering and Biotechnology*, *7*(136), 136. doi:10.3389/fbioe.2019.00136 PMID:31275929

Murch, R., & DiEuliis, D. (2019). Mapping the Cyberbiosecurity Enterprise. *Frontiers in Bioengineering and Biotechnology*, *7*, 235. doi:10.3389/fbioe.2019.00235 PMID:31632957

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. doi:10.3389/fbioe.2018.00039 PMID:29675411

Ney, P., Koscher, K., Organick, L., & Ceze, L., & Tadayoshi Kohno. (2017). C*omputer Security, Privacy, and DNA Sequencing: Compromising Computers with Synthesized DNA, Privacy Leaks, and More*. USENIX Security Symposium, Vancouver, BC, Canada: USENIX.

Palmer, X.-L., Potter, L., & Karahan, S. (2021). COVID-19 and biocybersecurity's increasing role on defending forward. [IJCWT]. *International Journal of Cyber Warfare & Terrorism*, *11*(3), 15–29. https://scholar.google.com/citations?view_op=view_citation&hl=en&user=nU8B4UQAAAAJ&citation_for_view=nU8B4UQAAAAJ:d1gkVwhDpl0C. doi:10.4018/IJCWT.2021070102

Palmer, X.-L., Potter, L., & Karahan, S. (2022). An Exploration on APTs in Biocybersecurity and Cyberbiosecurity. *International Conference on Cyber Warfare and Security, 17*(1), 532-535. 10.34190/iccws.17.1.67

Palmer, X.-L., Powell, E., & Potter, L. (2021). Biocyberwarfare and Crime: A Juncture of Rethought. *European Conference on Cyber Warfare and Security*. doi:10.34190/EWS.21.073

Palmer, X.-L., Powell, E., & Potter, L. (2021). Matters of biocybersecurity with consideration to propaganda outlets and biological agents. *Proceedings of the 20th European Conference on Cyber Warfare and Security*, (pp. 525-533). IEEE.

Payne, B. K., Mayes, L., Tish Paredes, E. S., Wu, H., & Xin, C. (2021). Applying High Impact Practices in an Interdisciplinary Cybersecurity Program. *Journal of Cybersecurity Education, Research and Practice, 28*.

Potter, L., Ayala, O., & Palmer, X.-L. (2021). Biocybersecurity: A Converging Threat as an Auxiliary to War. *16th International Conference on Cyber Warfare and Security*, 291. IEEE.

Potter, L., Mossburg, K., & Palmer, X.-L. (2023). A Reflection on Typology and Verification Flaws in Consideration of Biocybersecurity/Cyberbiosecurity: Just Another Gap in the Wall. *ECCWS 2023 22nd European Conference on Cyber Warfare and Security*, (pp. 358-365). IEEE.

Potter, L., & Palmer, X.-L. (2023). Mission-Aware Differences in Cyberbiosecurity and Biocybersecurity Policies: Prevention, Detection, and Elimination. In D. Greenbaum (Ed.), *Cyberbiosecurity* (pp. 37–69). Springer. doi:10.1007/978-3-031-26034-6_4

Potter, L., & Palmer, X.-L. (2023). Post-LLM Academic Writing Considerations. *Proceedings of the Future Technologies Conference*, (pp. 154-163). IEEE.

Potter, L., Powell, E., Ayala, O., & Palmer, X.-L. (2021). Urban planning to prevent pandemics: Urban design implications of biocybersecurity (BCS). Intelligent Computing: *Proceedings of the 2021 Computing Conference*, (Volume 2, pp. 1222-1235). IEEE.

Potter, L., Shetty, S., Karahan, S., & Palmer, X.-L. (2024). *Biocybersecurity and Applications of Predictive Physiological Modeling*. International Journal of System of Systems Engineering. doi:10.1504/IJSSE.2024.10056103

Powell, E., Akogo, D., Potter, L., & Palmer, X.-L. (2022). Co-leadership and Cross-pollination of University and DIY Bio Spaces: An Exploration in Consideration of Biocybersecurity. *Proceedings of the Future Technologies Conference (FTC) 2021, 3*, 610-621.

Reed, J. C., & Dunaway, N. (2019). Cyberbiosecurity Implications for the Laboratory of the Future. *Frontiers in Bioengineering and Biotechnology*, *7*(182), 182. doi:10.3389/fbioe.2019.00182 PMID:31497596

Samori, I., Odularu, G., Potter, L., & Palmer, X.-L. (2023). Biocybersecurity and Deterrence: Hypothetical Rwandan Considerations. *International Conference on Cyber Warfare and Security,* (*vol. 18*, 348-354). IEEE.

Samori, I. A., Palmer, X.-L., Potter, L., & Karahan, S. (2022). Commentary on biological assets cataloging and AI in the Global South. *Proceedings of SAI Intelligent Systems Conference 2022*, (pp. 734-744).

Schabacker, D. S., Levy, L. A., Evans, N. J., Fowler, J., & Dickey, E. A. (2019). Assessing cyberbiosecurity vulnerabilitis and infrastructure resilience. *Frontiers in Bioengineering and Biotechnology*, *7*(61). PMID:31001526

Security, I. B. M. (2023). *Cost of a Data Breach Report*. IBM., Retrieved from https://www.ibm.com/downloads/cas/E3G5JMBP

Sobien, D., Mehmet, Y. O., Nguyen, M. B., Mao, W.-Y., Fordham, V., Rahman, A., & Batarseh, F. A. (2023). AI for Cyberbiosecurity in Water Systems—A Survey. In D. G. ed., Cyberbiosecurity (pp. 217-263). Springer Cham.

Stephen, S., Alexander, K., Potter, L., & Palmer, X.-L. (2023). Implications of Cyberbiosecurity in Advanced Agriculture. *International Conference on Cyber Warfare and Security*, (pp. 387-393). IEEE.

Ulven, J., & Wangen, G. (2021). A Systematic Review of Cybersecurity Risks in Higher Education. *Future Internet*, *13*(2), 39. doi:10.3390/fi13020039

US Bureau of the Census. (2022). *Survey of State and Local Government Finance, 1977–2020. Washington, D.C.: US Bureau of the Census*. Urban.org. https://state-local-finance-data.taxpolicycenter.org/

USA DHS-CISA. (2024, January 01). *Cybersecurity Education & Career Development*. CISA.GOV. https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-education-career-development

Westberry, C., Palmer, X.-L., & Potter, L. (2023). Social Media and Health Misinformation: A Literature Review. *Proceedings of the Future Technologies Conference*, (pp. 404-418). Springer. 10.1007/978-3-031-47457-6_26