A Reflection on Typology and Verification Flaws in Consideration of Biocybersecurity/Cyberbiosecurity: Just Another Gap in the Wall

Lucas Potter[1], **Kimberly Mossburg**[1-2] **and Xavier-Lewis Palmer**[1-2]
[1]BiosView, Oswego, USA
[2]Cyber Solutions Academy, Franklin, USA

lpott005@odu.edu
kmorring@gmail.com
xpalm001@odu.edu

Abstract: Verification is central to any process in a functional and enduring cyber-secure organization. This verification is how the validity or accuracy of a state of being is assessed (Schlick, 1936; Balci, 1998). Conversely, breakdown in verification procedures is core to the interruption of normal operations for an organization. A key problem for organizations that utilize biology as an interlock within their systems is that personnel lack sufficient ability to verify all practically relevant biological information for procedures such as a nurse logging a blood draw, or a molecular biology technician preparing agar to culture microbes for study. This has several implications, one of which is our diminished ability to approximate and defend against emerging biologically-linked cyberthreats. These could be in the form of mis- or dis-information, contaminants, or calculated threats to vital supplies. Two important questions to ask are: "What may be the implications of diminished ability to undergo strict verification measures (such as triple redundancy and technological distancing)." And "how does this impact our ability to anticipate and make changes for verification of biological processes?" This paper aims to discuss key areas where verification gaps exist and how to bridgethos gaps. Towards this, we cover data integrity, implications of the lack of verification, triple redundancy, technological distancing, biosafety concerns, and more. All of this will factor into the ability of organizations with proximity to biosecurity to anticipate national changes to biological processes that are nationally relevant.

Keywords: Verification, Typology, Biocybersecurity, Cyberbiosecurity, Vulnerability, Ontology

1. Introduction

There exists a key problem within biosafety among corporate and national officials, and in the general population (including community biolab members) in which many do not fully understand or appreciate the ability to verify biological information. This leaves us with gaps to address in the field on multiple fronts. Namely: in industry, community bio labs, and government. This has several implications, including a diminished ability to approximate and defend against emergent threats, be they mis or disinformation, or contaminants. An important question to ask is what the implications of the lack of ability may be to undergo strict measures such as triple redundancy and technological distancing. Further, how does this impact our ability to anticipate and make national changes for biological processes?

Previous papers have explored the idea of the future of threats at the nexus of both biological and cyber domains (Bevilacqua et al, 2022; Duncan et al, 2019; Griffin, 2023; Palmer, 2021; Peccoud et al, 2018; Reed et al, 2019; Richardson et al, 2019). Now is a relevant moment to explore how that nexus can be bridged with other avenues of aggression, and how those can be effectively defended against. Through the polymorphisms that biology presents in data processing, storage, and presentation, these potential avenues increase appreciably as prior demonstrations and advancements within the last 10 years have demonstrated, as stated by Murch (2018). Potter & Palmer demonstrated that the early threats can be approximated, and wargaming has been shown to be extendable to biocybersecurity (2021).

In cybersecurity and its offshoot, cyberbiosecurity, typology refers to the classification and categorization of different types of malicious cyber activities that can pose a risk to the security of biological systems and data. This includes identifying the different types of cyber threats that can target these systems, such as malware, phishing, and ransomware, as well as the tactics, techniques and procedures used by attackers. Understanding the different types of cyber threats that can target biological systems is important for several reasons. It allows organizations to better identify and defend against specific types of cyber threats that can target these specific types of data. It helps organizations prioritize their cyberbiosecurity efforts by focusing on the types of cyber threats that are most likely to occur and have the greatest potential impact. It allows for the development of more effective cyberbiosecurity tools and strategies by providing a better understanding of the tactics, techniques, and procedures used by attackers. It can help in detecting and responding to cyber incidents that may compromise biological systems and data. It also allows organizations to stay up-to-date on the latest trends and innovations in the field of cyberbiosecurity.

In biocybersecurity typology can be used to classify different types of biological threats such as viruses, bacteria, and toxins, as well as different types of cyber threats such as malware and phishing attacks. This can aid in identifying and understanding the characteristics of these threats, and in developing appropriate countermeasures to protect against them. Additionally, typology can be used to classify different types of organisms, such as bacteria and fungi, which can be used in biotechnology applications such as the production of biofuels and other products. This can help in the development of security measures to protect against the unauthorized release or misuse of these organisms. However, in this new hybrid field of biocybersecurity typology and verification may prove to be problematic. There is no systemic method to implement the policy, standards of practice, or legal considerations for protecting the bioeconomy. It is arguable that even with the newest developments in Artificial Intelligence (AI) there may never be. Experts in the field are generally not aware of each other's expertise, perspectives and even mutually supported opportunities to work together to provide positive outcomes. It is imperative to create standards for cyberbiosecurity and establish a structured discipline that can be supported by various individuals.

In summary, typology in cyberbiosecurity (CBS) and biocybersecurity (BCS) represents ways to categorize, analyze and understand the different types of threats that can target biological systems and cyber-linked data, which can aid in better defense and incident response strategies. The paper includes a literature review concerning the typology of cybersecurity in general. The literature review delves into the incentivization of cybersecurity, as well as network considerations and the impact of human behavior on cybersecurity. This review is to be used as a means to explore how analogues of cybersecurity may exist in biocybersecurity. The review then explores why one should care about the possibility for people to exploit these openings in security. It should be noted that because BCS/CBS is a new field there are extremely limited resources available to discuss its impact in the field of cybersecurity as a whole.

This paper intended to be used as a stepping stone to begin that discussion. Considering the burgeoning expanse of the multi-trillion dollar global bioeconomy(Kacprzak et al, 2022), it is entirely likely that most typological security systems will one day be linked within the cyber-bio nexus. To dutifully cover those issues, the most pertinent subdomains and examples have been selected. Some may seem only tangentially related to BCS, but they are fields that should soon face integration with biologically relevant endeavors. We begin with a literature review on cybersecurity that discusses how a cybersecurity typology can refer to many things, but that it is only complete when that typology can be understood by all parties. The paper then moves to the incentivization of cybersecurity which delves into the incentives (economic or otherwise) that organizations look to when determining the use of cybersecurity within their organization. This is followed by a review of network considerations of security typology, which breaks down different network types and components and how they are impacted by cybersecurity typology. The final topic that is covered in the literature review is that people and their behaviors are the most common threat to keeping data secure. We follow this with a discussion of potential limitations.

2. Typology Literature Review

Within cybersecurity there are many different typologies that can be considered. In the scoping review conducted here, it was discovered that no two authors have the same point of view regarding what the typology for cybersecurity should entail.

Curwell (2022) says that a typology refers to how a system can be broken down into different parts. Current research indicates that cybersecurity typology could refer to many different things including: the governances of cybersecurity, the threats and risks that are associated with cybersecurity, economic impacts of cybersecurity, reasons why organizations do (or do not) invest in cybersecurity, different types of networks and how they are impacted by cybersecurity, how cybersecurity resources are managed within an organization, how cybersecurity policies impact parts of the network (specifically the DMZ and firewalls), and managing the impact of humans on cybersecurity. In this scoping review, the authors found that there is no agreement as to how cybersecurity should be broken up and the best ways to implement cybersecurity policies effectively in an organization's environment.

Curwell (2022) states that a typology is only complete when it can be easily understood by all parties and can then be converted into a decision-making process without needing much additional clarification. This is an important note, as many cybersecurity implementations in both the national and corporate domains require substantial interpretation in order to be implemented at all, much less at an effective scale. Typologies should be written to be understood by the intended audience, whether that be data scientists, forensic investigators,

CISOs, CEOs, or cyber security analysts, and then the information should be able to be addressed on a case-by-case basis. AI is one way to automatically break some of these rules down- however this runs into substantial issues with traceability of the interpreted requirements. Curwell (2022) argues that the problem with creating a singular cybersecurity typology is that they will never be complete since there are constant changes occurring in how threat actors are working to avoid detection, as well as how the technology changes over time. Additionally, if a particular threat is not going to actually pose a risk to an organization, then that company does not require a typology for that particular cybersecurity threat. One of the primary issues with typologies in the fields of BCS and CBS is that the threats are not typically connected between cyber connections and biological materials. Since there is such a vast number of cyber threats that can impact individual organizations, it is near impossible to find one set typology that can apply across the scope of the entire field of cybersecurity.

One of the areas within cybersecurity where a typology is present is in the different governance models. Eggenshwiler (2018) states that there are three governances that are often seen in cybersecurity: hierarchical, market and multi-stakeholder. A hierarchical governance is one where there is top-down regulation (as in with specific rules, policies or laws). It is an authoritative system of command and control with strict accountability. This could be seen in military establishments, regional departments, and important in incidents that require collaboration between incidents that involve governments, private industry, and nonprofit organizations. Government policy, including international treaties (like GDPR which was adopted in 2016), on the use of cybersecurity are examples of hierarchical governance. In contrast, market governance is bottom-up regulation. Eggenschwiler (2018) argues that this accounts for decentralization and the creation of independent autonomous units. Malware defense and packet routing are some areas where market governance is appropriate. Multi-stakeholder governance is where the majority of cybersecurity governance lies. It is a combination of hierarchical and market governance and is based on an exchange relationship between stakeholders as a way to find solutions to problems. These interactions are based on trust, reciprocity, and consensus-based decisions. The management of DNS (Domain Name System) is an example of multi-stakeholder governance.

3. Incentivization of Security Typology

Further research indicates that some people believe that cybersecurity can be broken down into six separate areas that determine why organizations do (or do not) invest in cybersecurity for their company. Wessels et. al. (2021) state that the areas that cybersecurity can be broken down into are: economic, normative, historic, feasibility, network externalities, and the idea that there are competing issues & solutions within cybersecurity. The idea of topology was applied in this instance to try and analyze why cybersecurity investments are, or are not, made within an organization. Wessels, et. al. (2021) argued that the feasibility of the implementation of different security measures was a very impactful point, as organizations made estimations about proposed interventions and how they could be incorporated into the business' current infrastructure. One critical point to note is that an organization must be aware of both the cybersecurity problems and solutions that are feasible within that organization, because without that awareness it is near impossible to determine why cybersecurity is a worthwhile investment.

Wessels, et. al. (2021) also stated that there are a wide range of incentives for the use of cybersecurity within an organization and each stakeholder will look at these inceptives differently. One of the biggest incentives deals with the global economy. Economic incentives allow for the maximum profit in both reputation and operations for an organization when deciding how to invest in cybersecurity. These incentives look for the impact of cybersecurity on costs, reputation, clients and any competitive advantage that might be utilized. According to Cremer, et. al. (2022) cybercrime had a cost of almost 950 billion USD in 2020 to the global economy and also caused a rise in cybersecurity insurance. In order to better avoid negative economic impact, it is critical to have a robust cybersecurity defense system at corporate, national and global levels.

Unfortunately, there is limited data available on cyber risks to the international economy. Cremer, et. al. (2022) argued that cybersecurity is still an emerging risk and does not have a lot of historical data. When a breach occurs, institutions do not necessarily publish the incident - creating a lack of data which proves to be a challenge for research, risk management and cybersecurity. This could be an issue when it comes to the development of future cybersecurity methods or policies, as the threats to be defended against are not public knowledge until they are an onerous enough problem to cause widespread disruption. There are so many different cyber-attacks and data breaches that can occur, ranging from ransomware to DDoS attacks, that any data to help prevent future economic loss to organizations would help guide these policies that in part assure the stability of the global economy. Mandatory reporting of the details of cyber incidents could help improve understanding,

awareness and loss prevention as well as allowing cyber risks to be better understood (which in turn enables better research).

From a business standpoint, there is an investment challenge when it comes to cybersecurity. Fernandez De Arroyabe, et. al. (2023) states that organizations must determine how much of an investment in cybersecurity is needed to provide sufficient protection to their data and resources. Historically that investment has been very low - barely enough to ensure the continuity of operations. There are two perspectives that are generally taken into account when determining this. The first is the IT manager's perspective and determining what factors of the IT manager motivate them to invest in cybersecurity. These factors could be internal (attitude, self-efficacy, experience, and habits) or external, including the severity of past attacks this manager has experienced. The second perspective to consider is the financial perspective. According to Fernandez De Arroyabe, et. al. (2023) the financial perspective emphasizes the value of the investment in cybersecurity, meaning that the decision to invest is determined by the profit of the investment. The investment in cybersecurity is a decision that should be made by the organization in its entirety. All levels from senior management to the lowest cyber technology should be involved in this process.

Economics are not the only incentive that organizations look at when determining the use of cybersecurity within the organization. Wessels, et. al. (2021) argue that normative incentives can impact the use of cybersecurity within an organization as well. When decisions are made to invest in cybersecurity on the shared values and norms that are present for IT quality, a duty to contribute to society's safety, and a feeling of belonging with what everyone else is doing that would indicate a normative incentive. Those incentives include Historic incentives, Network incentives, or with competing solutions. Historic incentives, or decisions that are made to invest in cybersecurity based on past decisions and experiences, are another way that companies incentivize the use of cybersecurity. Wessels, et. al. (2021) stated that decisions made in the past to protect the organization's technology can impact current decisions and may even cause the company to act proactively to avoid past problems in the future. Network incentives are when decisions are made based on the organization's specific environment. These decisions are impacted by what other companies are doing or by the current international views on specific cybersecurity issues and is another way that cybersecurity investment decisions are made. For instance, if one Electronic Health Record (EHR) corporation has a data breach, it may drive consumers to a different company. This is not the case when a single corporate entity has captured a market (also known as monopoly) or if that industry has effectively regulated competing interests out of that field (as in regulatory capture). The feasibility of implementing specific measures in cybersecurity is another decision-making model. The final incentive model is with competing solutions and problems. Wessels, et. al. (2021) said that this is when decisions are made to invest in cybersecurity based on an organization's awareness of competitive cybersecurity issues and solutions that are complex in scope, benefit, and cost.

Fernandez de Arroyabe, et. al. (2023) stated that the investment in cybersecurity, regardless of incentive, is a strategic decision within the company. The decisions that are made must be based on a combination of cyber-capabilities of that entity, external threats that are likely to be faced, and attacks with the knowledge that attacks are becoming bigger with more sophisticated means of delivery, making them harder to mitigate. Having developed procedures, rules and resources for cybersecurity has a positive impact on investments in this area. Even though investment in cybersecurity is conditioned by the capabilities, competencies and attacks of a specific organization, the possession of developed cybersecurity procedures has reduced the severity of threats and positively impacted the entire company.

4. Network Considerations of Security Typology

Kalkman & Wieskamp (2019) state that the type of network that is being used is also impacted by the lack of a clear typology for cybersecurity in terms of challenges and outcomes of cyber intelligence. There are four network types (centralized, business, operational, and local) that all are impacted by cyber threats in different ways. However, with the frequency of change in the cyber threat landscape, it is nearly impossible for organizations to manage all of the threats on their own. Kalkman & Wieskamp (2019) argue that it is of utmost urgency to build a shared intelligence network that is collaborative. Collaboration is tricky because all of the different network types have unique characteristics which makes it both important to distinguish between network types when collaborating, and for those competing network types to collaborate. Top-down networks (centralized and business) generally have a harder time staying committed to other parties and seeing results in their collaborative efforts while bottom-up networks (operational and local) are typically less hierarchical and formal and yield more successful results. Regardless of network type, it is critical to improve cyber threat intelligence and create a unified effort against cybersecurity threats to protect global assets.

In regard to the typology of the network and cybersecurity both the demilitarized zone (DMZ) and firewalls were discussed during the scoping review. Hawrylak, et. al. (2019) stated that while the DMZ does provide high bandwidth and throughput connectivity between computing resources it generally has minimal security. Maintaining the confidentiality and integrity of data on the DMZ is challenging. Security solutions in this instance must balance the fast speed for data processing with strong integrity and confidentiality to prevent malicious use of computing resources. Whitelists and strong SSH (Secure Shell) keys can be shared between users on the same local computer in order to help manage security on the DMZ. Data encryption on the DMZ will allow data to be protected at rest as well. Hawrylak, et. al. (2019) argued that passive security tools are another way that DMZs can remain secure. When the DMZ is part of a cybersecurity strategy (in terms of network segmentation) it cannot and should not be viewed exclusively as a performance solution. According to Anwar, et. al. (2021) firewalls are the first line of defense for security in many cases. Firewalls are critical for securing sensitive data and act as a filter between outgoing traffic from the internal network and incoming traffic coming from outside the network. The effectiveness of the firewall is dependent on environmental conditions (including the layer that the firewall is at and the nature of the data being protected). Anwar, et. al. (2021) stated that the effective use of firewalls reduces the impact of cyber threats on a company. Even with the importance of these two specific pieces of technology, there is not an agreement about how they should best be secured in order to ensure the security of the network.

5. Impact of Behavior on Security Typology

One important component of any cyber-enabled network is that people will always be involved with the security of data. People are the most common threat to keeping data secure through phishing emails, supply chain threats, threat actors, and other emerging risks. People engage in risky behavior and that needs to be addressed when looking at bio cybersecurity.

According to Buckley, et. al. (2023) there are many factors that determine how people respond to phishing emails including sociodemographics, cyber security training, phishing email typology, information processing factors and faith in the institution itself. Buckley, et. al. (2023) state that there has been a rapid increase in the number of data breaches from phishing emails as a result of the increased amount of remote work being done from the COVID-19 pandemic. When secure email behaviors are being followed, there is early detection and abatement of cyber threats which reduces financial costs and disruptions to the workplace.

Supply chain risks are also impacted by human interaction. Simon & Omar (2020) stated that a lack of coordination along the supply chain can result in either underinvestment or overinvestment from specific nodes in that chain, but there is not a lot of coordination between nodes. Breaches in the supply chain can occur quickly but may take months or even years to detect and contain. This can cause disruptions in logistics, production, and operations and may result in a loss of data. This data loss can lead to additional costs to return the supply chain to its original state. Simon & Omar (2020) argue that it should be noted that cybersecurity for a supply chain cannot be an isolated view, there has to be awareness along the entire chain as to how to mitigate cyber risks.

Additionally, Ursillo & Arnold (2019) argue that it is of utmost importance to have proper IT procedures in place to mitigate the risks associated with human error. Ongoing education to employees should be a part of all organizations' risk management framework. Policies to help mitigate risk from employees could include mandatory use of passwords on all systems (with passwords being changed regularly), encrypted USB sticks, physical security of all equipment, and multifactor authentication if possible. Maalem, et. al. (2020) stated that human error is the cause of many new cyber-attacks. Threat actors are more sophisticated and can use advanced techniques to hack into systems through human-enabled actions. Kraemer, et. al. (2009) stated that problems with passwords in particular may impact security and should be addressed to improve cybersecurity measures. Human errors may also be related to organizational factors like communication, security culture and company policy - and these mistakes may be costly for organizations to recover from.

Maalem, et. al. (2020) argued that behavioral aspects of cybersecurity should be scrutinized to find a way to lessen the number of successful attacks. It is the job of the cybersecurity team to analyze security at all levels of the network and ensure defenses are present throughout. The threat to data (confidentiality) occurs when hackers attack databases, backups, application servers and try to gain system administrator access. The threat to integrity, or altering data, includes hijacking, changing financial data, stealing large sums of money and rerouting direct deposits, or damaging an organization's reputation. Denial of access to a system, or a threat to a system's availability, involves DDoS attacks and physical destruction of data. All of these have implications to

the biological field - including changing the deliveries of medical components, release of patient records, ransomware attacks on healthcare systems, or DDOS threats to publishing institutions (Mueller, 2021; Samori et al, 2022; Finch et al, 2023, Stephen, 2023). Weapons of influence (reciprocity, scarcity, authority, consistency, liking and consensus) are largely used by hackers and ignored by defenders which is a problem. If a standard topology existed for cybersecurity, this behavioral component could be included which would allow for all companies to explore human factors and how they are integrated with cybersecurity. The lack of cyber expertise within organizations that is argued by Kraemer, et. al. (2009) decreases the effectiveness of the cybersecurity policies that are in place. These cyber system vulnerabilities cannot necessarily be addressed by technical remedies, since the behaviors of individuals are what cause the problems to take place.

6. Limitations

A common admonition is not to miss the forest for the trees which compose it. Yet in an increasingly complicated threat environment, it is sometimes difficult to engage wholly with the staggering number of issues that can be present in a biology-linked cybersecurity environment. The hope of this work is to re-engage cybersecurity professionals in biologically related fields with the sum total of the meaning of and drives behind security. That being said, there is a single caveat. Sometimes institutions are named as too big to fail. Leonhardt reports that Equifax, a U.S. credit reporting agency, may be required to pay up to 700 million USD (2019). The EBITDA for Equifax in 2020 was 1.628 billion USD and in 2021 was 1.076 billion USD. The required costs of the changes required in IT infrastructure according to an Equifax press release are even less than the maximum legal penalty (2022). Thus, the lesson from legal authorities to corporate entities was that a large enough institution would not face consequences for their failures, and the message conveyed to users of the corporate entity was that their perception of cybersecurity competence was unimportant. The limits to this study and to government policy may be non-obvious - but in this case shows that there are certain institutions that may be not only resistant to change but can forestall what should be common sense regulations permanently. This grows ever more concerning when considering the impacts this phenomenon might have on a biologically relevant institution, such as a hospital network or government healthcare program.

7. Conclusion

According to Ursillo & Arnold (2019) protection from cybercrime should be a focus for all organizations and governments. The monetary and reputation risks are extremely high without proper cybersecurity procedures in place. Cybersecurity governance and management must be established for every organization, and as previously noted, there is not a lot of agreement about what a true cybersecurity typology should look like. Our literature review has found that throughout the three governance models and six broad categories of cybersecurity that the networks of threats that contribute to the perception of security is a worthy source of study that is in an interrelated relationship to the behaviors of the participants of the organization. The prime limitation of the typology of cybersecurity is that the economic costs of implementing best practices are not in line with the profit motive of a corporate entity, and some corporate entities are so large as to be beyond the ability of legal practices to effectively change. Thus, an issue that takes primacy is the reluctance of government organizations to make cyber policy a matter of jurisprudence. This is a consequential matter, as the current lack of government command of cybersecurity infrastructure often leaves government agencies “picking up the pieces” after an incident for private interests. Since many of these private interests currently are integral components of goods and services required for the daily operation of a nation (healthcare systems, research institutes, agricultural operations, etc.) the clock is ticking before this method of reactance to issues and misunderstanding of typologies leads to an incident which leaves needed components of daily life untended to.

References

Anwar, R. W., Abdullah, T., & Pastore, F. (2021). Firewall Best Practices for Securing Smart Healthcare Environment: A Review. Applied Sciences, 11(19), 9183. MDPI AG. Retrieved from http://dx.doi.org/10.3390/app11199183

Bevilacqua, S., Neira-Villena, J. E., & Valverde, M. (2022). La tecnología al servicio de la vigilancia y de la defensa de la vida. Estudios en Seguridad y Defensa, 17(33), 179-200.

Buckley, J., Lottridge, D., Murphy, J.G., and Corballis, P.M. (2023). Indicators of employee phishing email behaviours: Intuition, elaboration, attention, and email typology. International Journal of Human-Computer Studies. https://www.sciencedirect.com /science/article/abs/pii/S1071581923000022

Chappell, B. (2020, June 1). Protesting Racism Versus Risking COVID-19: 'I Wouldn't Weigh These Crises Separately'. Retrieved from https://www.npr.org/sections/coronavirus-live-updates/2020/06/01/867200259/protests -over-racism-versus-risk-of-covid-i-wouldn-t-weigh-these-crises-separate

Cremer, F., Sheehan, B., Fortmann, M., Kia, A., Mullins, M., Murphy, F. & Matarne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47, 698–736. https://doi.org/10.1057/s41288-022-00266-6

Curwell, P. (Aug. 2022). Typologies demystified - what are they and why are they important? @Forwarned Blog. Retrieved from https://forewarnedblog.com/2022/08/20/typologies-demystified-what-are-they-and-why-are-they-important/

Duncan, S. E., Reinhard, R., Williams, R. C., Ramsey, F., Thomason, W., Lee, K., ... & Murch, R. (2019). Cyberbiosecurity: A new perspective on protecting US food and agricultural system. Frontiers in bioengineering and biotechnology, 7, 63.

Eggenschwiler, J. (2018). A Typology of cybersecurity governance models. St Antony's International Review, 13(2), 64–78. https://www.jstor.org/stable/26501049

Equifax, (9 Feb 2022). Equifax Delivers Record Revenue and Eighth Consecutive Quarter of Double-Digit Growth. Retrieved from: https://investor.equifax.com/news-events/press-releases/detail/1214/equifax-delivers-record-revenue-and-eighth-consecutive

Evangelista, S. (2020, April 30). COVID-19: Using wastewater to track the pandemic. Retrieved from https://medicalxpress.com/news/2020-04-covid-wastewater-track-pandemic.html

FDA Workflow Improvement Toolkit. (2019, December 12). Retrieved from https://www.hhs.gov/cto/projects/fda-workflow-improvement-toolkit/index.html

Fernandez De Arroyabe, I., Arranz, C.F.A., Arroyabe, M. F., and Fernandez de Arroyabe, J.C. (2023). Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019. Computers & Security, 124. https://www.sciencedirect.com/science/article/pii/S0167404822003467

Friedersdorf, C. (2020, June 4). The Protesters Deserve the Truth About the Coronavirus. Retrieved from https://www.theatlantic.com/ideas/archive/2020/06/protests-carry-risk-even-when-theyre-justified/612652/

Finch, H., Affia, A. A., Jung, W., Potter, L., & Palmer, X. L. (2023, February). Commentary on Healthcare and Disruptive Innovation. In International Conference on Cyber Warfare and Security (Vol. 18, No. 1, pp. 77-84).Fi

Griffin, B., Alexander, K., Potter, L., & Palmer, X. L. (2023, March). Social-Engineering, Bio-economies, and Nation-State Ontological Security: A Commentary. In ICCWS 2023 18th International Conference on Cyber Warfare and Security (Vol. 42, No. 1, pp. 127-142). Academic Conferences and publishing limited.

Hawrylak, P.J., Louthan, G., Hale, J., and Papa, M. (2019). Practical cyber-security solutions for the science DMZ. Association for Computing Machinery, New York, 50,(1-6). https://doi.org/10.1145/3332186.3332213

Kalkman, J.P. & Wieskamp, L. (2019). Cyber intelligence networks: A Typology. The International Journal of Intelligence, Security, and Public Affairs, 21(1), 4-24. https://www.tandfonline.com/doi/full/10.1080/23800992.2019.1598092

Kacprzak, M., Attard, E., Lyng, K. A., Raclavska, H., Singh, B., Tesfamariam, E., & Vandenbulcke, F. (2022) Biodegradable Waste Management in the Circular Economy. DOI: 10.1002/9781119679523

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers and Security, 28, 509-520.

Leonhardt, M., (2019), Equifax to pay $700 million for massive data breach. Here's what you need to know about getting a cut. CNBC.com. https://www.cnbc.com/2019/07/22/what-you-need-to-know-equifax-data-breach-700-million-settlement.html

Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R. et al. (2020). Review and insight on the behavioral aspects of cybersecurity. Cybersecurity, 3. https://doi.org/10.1186/s42400-020-00050-w

McQuate, S. (2019, October 29). Popular third-party genetic genealogy site is vulnerable to compromised data, impersonations. Retrieved from https://techxplore.com/news/2019-10-popular-third-party-genetic-genealogy-site.html

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.

Palmer, X. L., Powell, E., & Potter, L. (2021, June). Biocyberwarfare and Crime: A Juncture of Rethought. In European Conference on Cyber Warfare and Security (pp. 517-XIV). Academic Conferences International Limited.

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.

Potter, L. and Palmer, X.L., 2021, April. Human Factors in Biocybersecurity Wargames. In *Future of Information and Communication Conference* (pp. 666-673). Springer, Cham.

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

Samori, I. A., Palmer, X. L., Potter, L., & Karahan, S. (2022, September). Commentary on Biological Assets Cataloging and AI in the Global South. In Intelligent Systems and Applications: Proceedings of the 2022 Intelligent Systems Conference (IntelliSys) Volume 3 (pp. 734-744). Cham: Springer International Publishing.

Simon, J. and Omar, A. (2020). Cybersecurity investments in the supply chain: Coordination and a strategic attacker. European Journal of Operational Research, 282(1), 161-171. https://www.sciencedirect.com/science/article/abs/pii/S037722171930757X

Stephen, S., Alexander, K., Potter, L., & Palmer, X. L. (2023, February). Implications of Cyberbiosecurity in Advanced Agriculture. In International Conference on Cyber Warfare and Security (Vol. 18, No. 1, pp. 387-393).

Stone, W. (2020, June 5). Tear Gassing Protesters During An Infectious Outbreak Called 'A Recipe For Disaster'. Retrieved from https://www.npr.org/sections/health-shots/2020/06/05/870144402/tear-gassing-protesters-during-an-infectious-outbreak-called-a-recipe-for-disast

Towie, M., & Gale, J. (2020, May 22). A Deadly Virus From Africa Is Killing Horses in Thailand. Retrieved from https://www.bloomberg.com/news/articles/2020-05-22/a-deadly-virus-from-africa-is-killing-horses-in-thailand

Ursillo, S., and Arnold, C. (2019). Cybersecurity is critical for all organizations - Large and small. International Federation of Accountants. https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all- organizations-large-and-small

Wessels, M., van den Brink, P., Verburgh, T., Cadet, B., & van Ruijven, T. (2021). Understanding incentives for cybersecurity investments: Development and application of a typology. Digital Business, 1(2), 1-7. https://www.sciencedirect.com/science/article/pii/S2666954421000132

Yi, Y., Lagniton, P. N., Ye, S., Li, E., & Xu, R.-H. (2020). COVID-19: what has been learned and to be learned about the novel coronavirus disease. International Journal of Biological Sciences, 16(