A Commentary and Exploration of Maritime Applications of Biosecurity and Cybersecurity Intersections

Michaela Barnett[1], Issah Samori[2], Brandon Griffin[3], Xavier-Lewis Palmer[1-4] and Lucas Potter[4]
[1]Blacks In Cybersecurity Headquarters, Inc., VA, USA
[2]Minohealth AI Labs, Accra, Ghana
[3]CySecSol, Franklin, VA, USA
[4]BiosView, Oswego, KS, USA

michaela@bichq.org

Abstract: Prior work has discussed the emerging fields of Biocybersecurity (BCS) and Cyberbiosecurity (CBS) in multiple forms. These include the definition, mission-awareness, general applications, and policy (Murch et al, 2018; Peccoud et al, 2019; Potter et al, 2020). One area that has received relatively little attention are unique BCS/CBS vulnerabilities with maritime theaters, which refers to ocean and littoral-based commercial and military ventures. There is considerable ground for both bioeconomies and militaries to be placed at risk of degraded capacity for activity due to maritime-specific BCS/CBS attacks presently in the future. This is especially the case where aforementioned vulnerabilities are used to disrupt logistics through targeting of personnel and means of transport. This paper discusses the growing relevance of CBS/BCS in maritime space, aspects of maritime environments that can be exploited for BCS attacks, possible BCS/CBS attacks in the near future, possible BCS/CBS means of defense and pre-emptive positioning, and discussion of BCS/CBS relevance in international policy, and differences in application. This paper aims to facilitate and accelerate discussion of BCS to spur helpful action in this area.

Keywords: Biocybersecurity, Cyberbiosecurity Maritime, Biosecurity, Ecology, Military

1. Introduction

War and criminal activities change over time. This is especially true considering that new technologies find their way into offensive actions taken against other parties. Humanity has used sticks and stones from thousands of years back only to investigate new means today through artificial intelligence enhanced malware and remote attacks through DNA in recent times (Ney 2017; Chen et al, 2022). This novelty falls under the scopes of Biocybersecurity (BCS) and Cyberbiosecurity (CBS), which constitute two associated fields at the intersection of biological security and cybersecurity take into account novel biodigital attacks that lean on biospecific knowledge and digital systems (Duncan et al, 2019; Murch et al, 2018; Peccoud et al, 2019; Potter et al, 2020). Prior work by Potter, Powell, Palmer has covered the use of cybercrime and the escalation of such as corollaries of war (2021). In the most basic respect, logistics and supply chains are required for the basic operation of a nation state - and the disruption of maritime shipping through cyberattacks has been very well explored (Crosignani et al, 2023). One specific field of interest to this extrapolation is maritime shipping, which has been facing an increased level of cyberattacks for several years (*Report: Maritime Cyberattacks up by 400 percent*). “seven of the world’s top ten container carriers have publicly acknowledged they have been victims of cyber attacks, with all of the leading four carriers being among the victims” (Chubb, 2022). One particular cyberattack caused more than 300 million USD in losses (and frustratingly the victimized company has not been forthcoming with details of the attack in order to prevent similar ones - all interviewed only spoke on the condition of anonymity) (Greenberg, 2018; Lord, n.d.). The types of cyberattacks on modern maritime industry tend to align with three specific types - “traditional computer systems, industrial control systems and the communications protocols that control the most critical functions on a ship.” (*Are you mitigating maritime cybersecurity risks? | Industryweek*). These systems may include IoT (Internet of Things) technologies in addition to the biological assets that are at risk or are acting as an interlock within bio-digital authentication interfaces (Mileski et al, 2018). A short review of the specific cyber-enabled tools has previously been completed here. One of the most basic tools required for modern shipping AIS (Automatic Identification System) could conceivably be used to remotely interact with air-gapped systems on a modern shipping vessel (Leite Junior et al, 2021). At time of writing, an ongoing cyberattack was being conducted on a Norway-based shipping firm (Treloar, 2023). The physical security of maritime systems has been noted as a vulnerability as the physical security of a cybersystem can often be related to BioCyberSecurity, so we require a review of maritime affairs through the lens of BCS (Tam and Jones, 2018).

To that end, the following paper explores the following topics in series. Foremost, we present the scope of the issue, including a brief summary of the bioeconomy of the US and the globe (section 2). In the next section (section 3) we detail the prime BCS and CBS) issues. Section 4 further evaluates the scale of shipping to the

international bioeconomy. Section 5 explores the threat landscape of the modern maritime environment. Section 6 dives deeper into the autonomous shipping threats that might be prescient in the coming years. Section 7 concludes with an evaluation of ontological security in the context of shipping. Section 8 extends this discussion into policy considerations that may be relevant for future cybersecurity advances. Section 9 details limitations of this study, before concluding. This paper serves as both an exploration and commentary. It is the belief of the authors that there is much depth to be explored in the combination of maritime activities and BCS/CBS policy. Namely, with the rise of ubiquitous computing services and the lowering cost point of cyber-enabled technologies, the goods that we receive for our day-to-day lives will become more at threat than ever: both from actively malicious actors and from improperly vetted measures of automation.

2. Review of the International Bioeconomy vs the United States Bioeconomy

The bioeconomy, which refers to the production of goods and services from biological resources, is heavily dependent on sea-based logistics for the transportation of raw materials, intermediate goods, and finished products. The bioeconomy includes sectors such as agriculture, forestry, fisheries, and food and beverage production, as well as biotechnology and bioenergy. These sectors rely on the transportation of goods by ship to move products to domestic and international markets. According to the United Nations Conference on Trade and Development (UNCTAD) estimates, around 80% of global trade by volume and over 70% by value is carried by sea, therefore, sea-based logistics play a significant role in the bioeconomy (Piñeiro et al, 2021). For example, in the agriculture sector, a large proportion of food exports are transported by sea, and the forestry sector also relies heavily on sea transport for the export of wood products (Rodriguez Franco, 2020). In the fishing industry, much of the catch is transported by sea to processing and distribution centers. The bioenergy sector also relies on sea-based logistics for the transport of biomass and biofuels. In summary, sea-based logistics plays a crucial role in the bioeconomy, as it enables the transportation of raw materials, intermediate goods, and finished products to domestic and international markets, which is essential for the growth and development of the bioeconomy sectors.

In the United States, a significant portion of the bioeconomy is dependent on sea-based logistics, particularly for the export of goods. Considerable exports, such as soybeans, corn, and wheat, are transported by sea to foreign markets (Xavier and Reis, 2020; Gerval, 2022; 김찬우, 2020. The U.S. is also a leading exporter of forest products, practical for export by sea (Rodriguez Franco, 2022). In the fishing industry, much of the catch is transported by sea to processing and distribution centers. In the bioenergy sector, the US is a leading producer of biofuels such as ethanol and biodiesel, and these products are also transported by sea to domestic and international markets. Overall, sea-based logistics plays a significant role in the US bioeconomy, enabling the transportation of raw materials, intermediate goods, and finished products to domestic and international markets, which is essential for the growth and development of the bioeconomy sectors in the US.

3. Cyberbiosecurity & Biocybersecurity Considerations

Cyberbiosecurity and biocybersecurity are related fields, but they have slightly different focuses. In terms of mission specific differences, this is further addressed in Potter and Palmer (2021). Cyberbiosecurity is the practice of protecting biological systems, information, and infrastructure from cyber threats. This includes protecting research facilities, laboratories, and other biological systems from cyber attacks, as well as ensuring the integrity and confidentiality of data generated by biological research. It also includes protecting the critical infrastructure that supports biological research, such as power systems, water supplies, and communication networks. Biocybersecurity, on the other hand, focuses on the intersection of cybersecurity and the life sciences. It deals with the protection of biological systems and organisms from cyber threats, including the protection of biological systems from malicious use, and the protection of organisms from malicious manipulation of their genetic code or other characteristics. Biocybersecurity also includes the protection of the information and data that is generated by biological research, including the protection of intellectual property and proprietary information. In summary, Cyberbiosecurity is focused on protecting biological systems, information, and infrastructure from cyber threats, while Biocybersecurity is focused on the intersection of cybersecurity and the life sciences.

4. Scale of biological imports and relation to Biocybersecurity and Cyberbiosecurity

These features lack an obvious link to BCS. Until the following is considered: an estimated 80% of the world's population relies on imported foods (Dunphy, 2020). In fact, local grown crops can only fulfill the demand for

less than one third of the global population (Kinnunen, 2020). Cost of food importing are projected to reach 2 trillion USD in 2023 (not all of this cost is associated with maritime shipping, but the point remains as to its important link to supplying the world with nutrition) (*Global food imports on track to reach all-time high: FAO | UN News*). Some countries are concerned with the safety of imported food, particularly the US (Center for Food Safety and Applied Nutrition, *FDA strategy for the safety of imported food*).

The unique aspects of the shipping industry that relate to BCS are 1) The use of multiple cyber platforms for various tasks (such as verifying contents, navigating, control of the ship itself, and crew registration), 2) the ability of biologically active components to be shipped, to 3) the exploration and protection of biologically important environments (Grafi, 2022). The first and latter is especially important considering that international trade has led significantly to invasions of unwanted species (Grafi, 2022; Hulme, 2021).

Biocybersecurity refers to the security of biological materials, information, and systems, including measures to protect against the theft, loss, release, or misuse of dangerous pathogens or toxins, as well as the protection of sensitive information related to these materials, from the perspective of biology as an interlock (Potter and Palmer, 2021). Long term goals of those working at this intersection include protecting against accidental releases, as well as intentional ones such as bioterrorism, and also includes protection against cyber attacks on systems and networks used in the handling and transportation of biological materials. Biocybersecurity is an interdisciplinary field that involves collaboration between the biological sciences and information technology to ensure the safety and security of biological materials and information. Biocybersecurity in shipping refers to the security of biological systems, such as those used in cargo or supply chain management, against cyber attacks. These attacks can target the systems used to track and monitor cargo, as well as the systems used to control and operate the ships themselves. Some possible problems that biocybersecurity presents in shipping include: Disruption of cargo tracking and monitoring systems, which can lead to lost or stolen cargo. Tampering with or manipulating the data used to control and operate ships, which can lead to accidents or collisions. The release of harmful biological agents, such as pathogens or toxins, as a result of a cyber attack on cargo systems or ship systems. Overall, biocybersecurity is a growing concern in the shipping industry as it becomes increasingly reliant on digital systems and connected devices. Addressing these risks requires a multi-disciplinary approach that brings together experts in biology, cybersecurity, cyber-physical systems involved and shipping.

5. Threat Landscape of BioCybersecurity in the Maritime Environment

The threat landscape of BioCybersecurity related to the maritime environment includes the exploration, exploitation or manipulation of key systems in navigation, port facilities, maritime infrastructure and their accompanying assets; especially when transporting and maintaining the condition of perishable food or supplies, fuel and maintaining agriculture.

The particularly pertinent attack surfaces here are the information technology systems supporting corporate networks in day-to-day operations through more advanced or crucial systems. This includes navigation and autonomous shipping capabilities. The attacks of these systems commonly involve the use of malicious software to gain unauthorized access to systems and the contained data. In particular, ransomware attacks have become more prevalent (as mentioned in the introduction) and also have combined other elements to increase their effectiveness such as social engineering, that can ultimately lead to the effective phishing of key staff and personnel.

Social engineering attacks can be especially effective in the context of Maritime environments (Guidelines on Cyber Security Onboard Ships, Version Four, n.d.). It can be inferred that threat actors are able to triangulate the element of an individual's emotions and leverage feelings of isolation, home sickness or simply fatigue. Personnel who are responsible for food preparation, water sanitation and any potentially dangerous materials would also be likely to present as a target, as they may overcompensate for any suggested compromise to the communal safety of those aboard.

Ransomware in these systems can be particularly devastating to operational software in maritime environments as they involve encrypting data and demanding payment in exchange for the decryption key, this can delay and augment vital systems. The accompanying phishing technique, typically allows for a malicious link to be triggered by an unknowing end-user to kick off the software used to compromise the user or their system. The delivery medium is usually by SMS (text messages) or email. In 2019, leading into 2020 The United States Coast Guard released a safety alert to inform that a phishing email had led to a facility's network being compromised. This Ryuk Ransomware attack “further burrowed into the industrial control systems that monitor and control cargo transfer and encrypted files critical to process operations" (Gatlan, 2019).

We can infer that the systems that maintain proper condition of transported goods such as refrigeration, agricultural monitoring and managing of exacting substances are at risk and able to be accessed laterally from external facing attack vectors. Maritime Operational Technology has become further ingrained in the Internet of Things (IoT) as well as maintaining infrastructure for independent connections to the wider internet such as; onboard computer systems for personnel and openly available Wifi availability for passengers (Navigating Cybersecurity Challenges in Maritime Operational Technology, 2020).

DDoS attacks involve overwhelming a system or network with traffic, making it unavailable to users. These attacks can be used to disrupt the maritime staff's network or to distract the monitoring security personnel while other attacks are launched. March 2017, in a meeting about the future of Vancouver Energy a DDoS attack occurred on the Port of Vancouver's computer system. This attack occurred as a result of a participant connecting to the port's Wi-Fi, temporarily knocking it offline (Cyber-attacks on the Ports and Maritime Industry – Secolve, n.d.). In evaluating the implications of this not only are end users jeopardizing their methods of daily corporate operation but also have the ability to potentially bridge the unauthorized access allocated by these attacks to more critical systems supporting biological systems and accompanying information.

Supply chain attacks and data breaches can involve the unauthorized access to and theft of sensitive data; involving the compromising of a third-party vendor, integrating technologies or suppliers to gain access to a target system as well as simple mishandling or misappropriation of contributing systems. In the context of Cyberbiosecurity, this might involve compromising the database used to stock and ship requested materials relevant to a nation's bioeconomy or augment their condition mid-transport. Most recently, it was cited that in an evaluation of the factors contributing to the Maritime supply chain by a consulting firm that fault could be assessed in lack of provision of security systems and their configuration versus any percieved absence (Linskey & Palmadesso, 2022). The need for further fortification of Supply chain is also highlighted by the National CounterIntellgence and Security Center (NCSC) and Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) as well as other agencies by their latest awareness initiative in a comprehensive approach to supply chain reinforcement focusing on the need for Cybersecurity and operational technology comprehsnion within procurement and execution (White House 2023).

Autonomous shipping is constructed to operate either completely autonomously or partially, to aid with certain tasks; utilizing software to manage sensors, cameras and other maritime tools (Wariishi, 2019). This emerging technology is yet another vector for exploitation and a threat to the operational technology hosting and maintaining infrastructure that BioCybersecurity systems rely on in transit.

In reviewing these definitions, scenarios and observations it is important to involve every aspect and resource in this area of security research by exploring the technology used to support the maritime industry and its BioCybersecurity systems. The threat landscape here is evolving with the introduction of Artificial Intelligence and Autonomous Systems that aid in monitoring, reporting and communications which poses a significant risk to critical systems (Navigating Cybersecurity Challenges in Maritime Operational Technology, 2020). Only through a coordinated effort across commercial, recreational and military maritime communities can we move this industry forward and mitigate the impact of threats to operations and commerce.

6. Threats of Autonomous Shipping

Let us explore a concept that is common in many avenues of transportation. The number and quantity of efforts involved in creating autonomous vehicles is growing more numerous. Cyber threats to them have been specified before and must be continually monitored (Akpan et al, 2022; Bolbot et al, 2020; Kavallieratos et al, 2019; Tusher et al, 2022).

There are already several risks associated with automation in maritime logistics, for instance: operational risks, workforce displacement, technology dependence for fundamental tasks, human errors, accidents, and risks of non-compliance with regulatory bodies.

It is important for companies in the maritime logistics industry to be aware of these risks and to implement measures to mitigate them, such as cybersecurity protocols and procedures, regular system maintenance and testing, training of personnel and ensuring that they are compliant with laws and regulations. This problem compounds with biological interlocks or matter within logistics to take into account.

However, the real scale of a compromised autonomous maritime transport system loaded with foodstuffs with a single illicitly stored unit on board which has the ability to autonomously optimize a biothreat - a method previously explored by Potter, Ayala, and Palmer (2021). Such a threat, placed on board an autonomous vessel,

would be able not only to discover the best contaminant to maximize speed of contamination, but theoretically a simple logging or transit change on a compromised logistics unit could inadvertently cause the spread of this disease to other vessels, or even countries.

7. Maritime CBS Applications and Ontological Security

Cyberbiosecurity, maritime applications, and ontological security are interconnected in many ways, particularly in the context of geopolitical tensions and security threats in the South China Sea. Cyberbiosecurity refers to the protection of biological systems and related data from cyber-attacks, while maritime applications involve the use of technology and data in maritime security and navigation. Ontological security refers to the extent to which an individual or group feels secure in their understanding of the world and their place in it. It is a psychological concept that pertains to the way in which people construct their sense of self and their place in the world, and how this sense of self and place is shaped by their interactions with others and the broader social, cultural, and political context in which they live (Griffin et al., 2023). In the context of territorial disputes, ontological security is closely tied to national identity and sovereignty. For example, China's claims in the South China Sea are based on its historical and cultural ties to the region, which are central to its national identity. Taiwan also claims sovereignty over the same islands and reefs, which are a source of national pride and identity.

Maritime law governs activities in the oceans, including territorial disputes between states. The United Nations Convention on the Law of the Sea (UNCLOS) provides a framework for the use and management of ocean resources, including territorial claims, fishing rights, and shipping lanes. The South China Sea, which contains significant oil and gas reserves and important shipping lanes, is the subject of multiple territorial disputes. China claims nearly the entire South China Sea, including islands and reefs also claimed by Taiwan, Vietnam, Malaysia, Brunei, and the Philippines. The United States has contested China's claims and conducted freedom of navigation operations in the region, which has heightened tensions and raised the risk of conflict (United States Department of State Bureau of Oceans and International Environmental and Scientific Affairs Limits in the Seas No. 150 People's Republic of China: Maritime Claims in the South China Sea, 2022).

For example, in 2018, a Chinese cyber espionage group known as TA423 was found to have targeted several companies involved in the South China Sea's energy sector, including the Kasawari gas field and a wind farm in the Taiwan Strait. ("Chinese Hackers Tied to Attacks on South China Sea Energy Firms," 2022). The attack aimed to steal intellectual property and sensitive data related to offshore drilling technology, which could give China a strategic advantage in the disputed region. Such cyber attacks not only threaten the security and competitiveness of individual companies and countries, but also undermine the ontological security of the actors involved, by creating a sense of uncertainty and vulnerability in their technological and strategic capabilities.

In conclusion, the connections between cyberbiosecurity, maritime applications, and ontological security are complex and interdependent, and require a comprehensive and collaborative approach from different stakeholders, including governments, private companies, and international organizations. In the context of the South China Sea dispute, this approach should aim to promote transparency, trust, and cooperation in the use of technology, while also respecting the sovereignty and rights of all parties involved.

8. Policy Considerations, including Defend Forward

There are a number of policies that nations can implement in order to prepare for adequate biocybersecurity. Some examples include: Developing and implementing national biocybersecurity strategies: This would involve creating a comprehensive plan for identifying, assessing, and mitigating biocybersecurity risks. Encouraging public-private partnerships: Governments can work with private sector companies, such as medical device manufacturers and biotech companies, to help identify and mitigate biocybersecurity risks. Investing in research and development: Governments can fund research into new biocybersecurity technologies and techniques in order to stay ahead of emerging threats. Providing education and training: Governments can provide training and education to healthcare providers, researchers, and other stakeholders on how to identify and mitigate biocybersecurity risks. Creating oversight and regulatory bodies: Governments can create oversight and regulatory bodies to ensure that biocybersecurity guidelines and standards are being met by the organizations and companies that operate in these areas. International cooperation: Governments can work with other countries and international organizations to share information and coordinate efforts to address biocybersecurity risks on a global scale. It's important to note that the exact policies will depend on the country and the specific context and that Biocybersecurity policies are multi-disciplinary and will involve multiple actors such as government, private sector, academics, international organizations and so on.

Violations of maritime biocybersecurity or cyberbiosecurity can have significant political ramifications. Here are a few examples: A violation of maritime biocybersecurity could occur if a cyber attacker is able to disrupt the navigation or control systems of a ship, potentially causing a collision or other maritime accident. This could lead to loss of life, environmental damage, and economic disruption, and could result in a diplomatic incident between the countries involved. A violation of cyberbiosecurity in the maritime context could occur if a cyber attacker uses a ship as a platform to launch a cyber attack on other ships or shore-based systems. This could result in a loss of confidence in the safety and security of the maritime industry, and could lead to calls for increased regulation and oversight of ships and shipping companies. A violation of biosecurity in maritime context could occur if a malicious actor uses a ship to smuggle dangerous pathogens into a country. This could lead to a public health crisis and could result in diplomatic tensions between countries. In general, violations of maritime biocybersecurity or cyberbiosecurity can have significant economic, political, and security implications, and can cause damage to the reputation and credibility of the countries and organizations involved. It is important for countries to have robust cyber and biosecurity measures in place to protect against these types of incidents.

Defend Forward is a cyber security strategy framework developed by the U.S. Cyber Command (USCYBERCOM), it is designed to proactively detect and disrupt malicious cyber activities before they can do harm to U.S. interests. This framework focuses on identifying and stopping threats at their source, rather than simply reacting to them once they have already entered the network. Defend Forward could be a suitable framework in which to include maritime applications biocybersecurity as it's a proactive approach to detecting and disrupting malicious cyber activities before they can cause harm to U.S. interests. However, incorporating maritime applications biocybersecurity into the framework would require some additional considerations. Maritime applications biocybersecurity refers to the protection of ships, ports, and other maritime infrastructure from cyber threats that could disrupt or damage these systems. This could include protecting against the hacking of navigation and control systems on ships, or the spread of computer viruses through biological vectors on ships. To include maritime applications biocybersecurity within the Defend Forward framework, the following steps could be taken:

1. Identifying the specific biocybersecurity risks associated with maritime systems
2. Developing and implementing biocybersecurity protocols and guidelines for maritime systems specifically tailored to the maritime industry, that would be in line with the overall Defend Forward strategy
3. Encouraging public-private partnerships between the maritime industry and government to share information and coordinate efforts to address biocybersecurity risks
4. Investing in research and development for maritime biocybersecurity technologies and techniques
5. Providing education and training for maritime industry workers on how to identify and mitigate biocybersecurity risks
6. Creating oversight and regulatory bodies to ensure that biocybersecurity guidelines and standards are being met by the organizations and companies that operate in the maritime industry,

`It's important to note that incorporating maritime applications biocybersecurity into the Defend Forward framework would require a comprehensive approach that involves multiple actors such as government, private sector, academics, international organizations and so on, and that the strategies and protocols need to be reviewed and updated regularly as the field of biocybersecurity is evolving.

9. Limitations

`The limitations of this paper should be acknowledged to provide a comprehensive understanding of the group research. Firstly, the study mainly relied on resources from limited outlets utilized by academic researchers versus those participating actively as full-time practitioners. The findings may not be generalizable to other maritime organizations or sectors. Secondly, the study was conducted during a specific period, and the results may be affected by the changing circumstances of the time. Therefore, the findings may not reflect the current state of the maritime industry in relation to the Cybersecurity implications. Further research is needed to validate these findings and explore other potential limitations.

10. Conclusion

Existence on earth is a fragile thing, as so many know all too well. So too are the tenuous links that connect our daily lives with the goods that we require - from the most basic foods that sustain us to the many medicines that

are required - they mainly arrive via sea through maritime shipping. So we see that through the lens of BCS and CBS, these tenuous links are far too crucial to remain both unexamined and unprotected from modern methods of attack. Even while more advanced and even autonomous methods of shipping are being explored, their attack surfaces must be continually monitored and impacts of cyberattacks to the processes of shipping estimated (Weaver et al, 2022).

Acknowledgments:

The authors would like to express their gratitude to the individuals in the Maritime Cybersecurity industry that have contributed to this research.

References:

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S. and Michaloliakos, M., 2022. Cybersecurity Challenges in the Maritime Sector. *Network*, *2*(1), pp.123-138.

Bolbot, V., Theotokatos, G., Boulougouris, E. and Vassalos, D., 2020. A novel cyber-risk assessment method for ship systems. *Safety science*, *131*, p.104908.

Carballo Piñeiro, L., Mejia Jr, M. Q., & Ballini, F. (2021). Beyond COVID-19: the future of maritime transport. *WMU Journal of Maritime Affairs*, *20*(2), 127-133.

Center for Food Safety and Applied Nutrition (no date) *FDA strategy for the safety of imported food*, *U.S. Food and Drug Administration*. FDA. Available at: https://www.fda.gov/food/importing-food-products-united-states/fda-strategy-safety-imported-food (Accessed: January 22, 2023).

Chen, Z., Liu, J., Shen, Y., Simsek, M., Kantarci, B., Mouftah, H. T., & Djukic, P. (2022). Machine learning-enabled iot security: Open issues and challenges under advanced persistent threats. *ACM Computing Surveys*, *55*(5), 1-37.

Chinese Hackers Tied to Attacks on South China Sea Energy Firms. (2022, August 30). Bloomberg.com. https://www.bloomberg.com/news/articles/2022-08-30/chinese-hackers-tied-to-attacks-on-south-china-sea-energy-firms#xj4y7vzkg

Chubb, N. (2022) *Cyber attacks: Who targets the Maritime Industry and why?*, *Thetius*. Available at: https://thetius.com/cyber-attacks-who-targets-the-maritime-industry-and-why/ (Accessed: January 22, 2023).

Crosignani, M., Macchiavelli, M. and Silva, A.F., 2023. Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, *147*(2), pp.432-448.

Dunphy, S. (2020) *Majority of the world's population depends on imported food*, *European Scientist*. Available at: https://www.europeanscientist.com/en/agriculture/majority-of-the-worlds-population-depends-on-imported-food/ (Accessed: January 22, 2023). Tam, K. and Jones, K.D., 2018. Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, *3*(2), pp.147-164.

Gatlan, S. (2019, December 27). U.S. Coast Guard Says Ryuk Ransomware Took Down Maritime Facility.

Gerval, A., 2022. US Agricultural Trade Showed Resiliency Through COVID-19 Pandemic. Amber Waves: The Economics of Food, Farming, Natural Resources, and Rural America, 2020.

Global food imports on track to reach all-time high: FAO | UN News. (2022, November 11). News.un.org. https://news.un.org/en/story/2022/11/1130467

Grafi, A. (2022) Why ports are at risk of cyberattacks, Dark Reading. Available at: https://www.darkreading.com/attacks-breaches/why-ports-are-at-risk-of-cyberattacks (Accessed: January 22, 2023).

Greenberg, A. (2018) The untold story of notpetya, the most devastating cyberattack in history, Wired. Conde Nast. Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (Accessed: January 22, 2023).

Griffin, B., Alexander, K., Palmer, X.-L., & Potter, L. (2023). Social-Engineering, Bio-economies, and Nation-State Ontological Security: A Commentary. International Conference on Cyber Warfare and Security, 18(1), 111–118. https://doi.org/10.34190/iccws.18.1.1021

Guidelines on Cyber Security Onboard Ships, Version Four. (n.d.). Www.ics-Shipping.org. https://www.ics-shipping.org/publication/guidelines-on-cyber-security-onboard-ships-version-four/

Hulme, P.E., 2021. Unwelcome exchange: International trade as a direct and indirect driver of biological invasions worldwide. *One Earth*, *4*(5), pp.666-679.

Are you mitigating maritime cybersecurity risks? | Industryweek (no date). Available at: https://www.industryweek.com/technology-and-iiot/cybersecurity/article/21216344/are-you-mitigating-maritime-cybersecurity-risks (Accessed: January 23, 2023).

Kavallieratos, G., Katsikas, S., Gkioulos, V. (2019). Cyber-Attacks Against the Autonomous Ship. In: , et al. Computer Security. SECPRE CyberICPS 2018 2018. Lecture Notes in Computer Science(), vol 11387. Springer, Cham. https://doi.org/10.1007/978-3-030-12786-2_2

김찬우, 2020. *Environmental Impacts of International Crop Trade on Supply Chain from Farm to Market* (Doctoral dissertation, 서울대학교 대학원).

Kinnunen, P., Guillaume, J.H., Taka, M., D'odorico, P., Siebert, S., Puma, M.J., Jalava, M. and Kummu, M., 2020. Local food crop production can fulfil demand for less than one-third of the population. *Nature Food*, *1*(4), pp.229-237.

Leite Junior, W.C., de Moraes, C.C., de Albuquerque, C.E., Machado, R.C.S. and de Sá, A.O., 2021. A triggering mechanism for cyber-attacks in naval sensors and systems. *Sensors*, *21*(9), p.3195.

Linskey, D., & Palmadesso, C. (2022, April 20). *Maritime Supply Chain Crisis: 6 Ways to Effectively Mitigate Port Security Risks*. Kroll. https://www.kroll.com/en/insights/publications/maritime-supply-chain-crisis-effectively-mitigate-port-security-risks

Lord, N. (no date) *The cost of a malware infection? for Maersk, $300 million*, *Digital Guardian*. Available at: https://digitalguardian.com/blog/cost-malware-infection-maersk-300-million (Accessed: January 22, 2023).

Mileski, J., Clott, C. and Galvao, C.B., 2018. Cyberattacks on ships: a wicked problem approach. *Maritime Business Review*.

Navigating Cybersecurity Challenges in Maritime Operational Technology. (n.d.). The Maritime Executive. https://maritime-executive.com/editorials/navigating-cybersecurity-challenges-in-maritime-operational-technology

Ney, P., Koscher, K., Organick, L., Ceze, L., & Kohno, T. (2017, August). Computer Security, Privacy, and DNA Sequencing: Compromising Computers with Synthesized DNA, Privacy Leaks, and More. In *USENIX security symposium* (Vol. 26, pp. 765-779).

Palmer, X.L., Powell, E. and 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.

Potter, L., Ayala, O. and Palmer, X.L., 2021, February. Biocybersecurity: A Converging Threat as an Auxiliary to War. In *ICCWS 2021 16th International Conference on Cyber Warfare and Security* (p. 291). Academic Conferences Limited.

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.

Report: Maritime Cyberattacks Up by 400 Percent. (n.d.). The Maritime Executive. https://maritime-executive.com/article/report-maritime-cyberattacks-up-by-400-percent

Rodriguez Franco, C., 2022. Forest biomass potential for wood pellets production in the United States of America for exportation: a review. *Biofuels*, pp.1-12.

Treloar, S. (2023) *Cyber attack hits 1,000 merchant ships as Norway firm targeted*, *Bloomberg.com*. Bloomberg. Available at: https://www.bloomberg.com/news/articles/2023-01-18/cyber-attack-hits-1-000-merchant-ships-as-norway-firm-targeted (Accessed: January 22, 2023).

Tusher, H.M., Munim, Z.H., Notteboom, T.E., Kim, T.E. and Nazir, S., 2022. Cyber security risk assessment in autonomous shipping. *Maritime Economics & Logistics*, pp.1-20.

Xavier, D.L.D.J. and Reis, J.G.M.D., 2022. Social Network Analysis on Agricultural International Trade: A Study on Soybean, Soybean Cake and Maize Exports. *Chemistry Proceedings*, *10*(1), p.37.

White House Office of the National Cyber Director. (2023, April 11). *April is Supply Chain Integrity Month*. The White House. https://www.whitehouse.gov/oncd/briefing-room/2023/04/11/april-is-supply-chain-integrity-month/

Wariishi, K. (2019, September). *Mitsui & Co. Global Strategic Studies Institute Monthly Report*. https://www.mitsui.com/mgssi/en/index.html.

Weaver, G.A., Feddersen, B., Marla, L., Wei, D., Rose, A. and Van Moer, M., 2022. Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach. *Transportation Research Part C: Emerging Technologies*, *137*, p.103423.

U.S Coast Guard Says Ryuk Ransomware Took Down Maritime Facility. (n.d.). BleepingComputer. Retrieved April 11, 2023, from https://www.bleepingcomputer.com/news/security/us-coast-guard-says-ryuk-ransomware-took-down-maritime-facility/

United States Department of State Bureau of Oceans and International Environmental and Scientific Affairs Limits in the Seas No. 150 People's Republic of China: Maritime Claims in the South China Sea. (2022). https://www.state.gov/wp-content/uploads/2022/01/LIS150-SCS.pdf