Journal of Infrastructure, Policy and Development 2024, 8(8), 4146.
https://doi.org/10.24294/jipd.v8i8.4146

Article

Impending maritime cyberspace threats: An educational research perspective

Ahmed Yusuf Mai-inji[1], Kingsley Eghonghon Ukhurebor[2,*], Longe Olumide Babatope[3,4], Adeyinka Oluwabusayo Abiodun[1], Esosa Enoyoze[5], Beauty Oboghelu Olumhense[6], Idemudia Edetalehn Oaihimire[7], Udochukwu Chidiebere Nwankwo[1]

[1] Africa Centre of Excellence on Technology Enhanced Learning (ACETEL), National Open University of Nigeria, Abuja 900001, Nigeria
[2] Department of Physics, Edo State University Uzairue, P.M.B. 04, Auchi 312001, Nigeria
[3] West Midlands Open University, Ikeja 100001, Nigeria
[4] Faculty of Computational Sciences and Informatics, Academic City University College, Accra P.O. Box AD 421, Ghana
[5] Department of Mathematics, Edo State University Uzairue, P.M.B. 04, Auchi 312001, Nigeria
[6] Department of Computer Science, Edo State University Uzairue, P.M.B. 04, Auchi 312001, Nigeria
[7] Faculty of Law, Edo State University Uzairue, P.M.B. 04, Auchi 312001, Nigeria
*** Corresponding author:** Kingsley Eghonghon Ukhurebor, ukeghonghon@gmail.com, ukhurebor.kingsley@edouniversity.edu.ng

CITATION

Mai-inji AY, Ukhurebor KE, Babatope LO, et al. (2024). Impending maritime cyberspace threats: An educational research perspective. Journal of Infrastructure, Policy and Development. 8(8): 4146. https://doi.org/10.24294/jipd.v8i8.4146

ARTICLE INFO

Received: 9 January 2024
Accepted: 7 March 2024
Available online: 12 August 2024

Abstract: The ability to take advantage of new digital solutions and technology will give companies a competitive edge, and operational optimization remains a major concern. A significant area of risk is cyber security because software-based technologies are integral to ship operations. Particular emphasis has been placed on the vulnerabilities of the Global Navigation Satellite System (GNSS), since it is an essential part of many maritime facilities and hence a target for hackers. Presently, research has shown that increased integration of new enabling technologies, like the Internet of Things (IoT) and big data, is driving the dramatic proliferation of cybercrimes. However, most of the attacks are related to ransomware attacks and/or with direct attack to the information technology (IT) and infrastructure. Nevertheless, there is a strong trend toward increased systems integration, which will produce substantial business value by making it easier to operate autonomous vessels, utilizing smart ports more, reducing the need for labour, and improving economic stability and service efficiency. Cybersecurity is becoming more and more important as a result of the quick digital transformation of the offshore and maritime sectors, which has also brought new dangers and laws. The marine sector has started to take cybersecurity seriously in light of the multiple documented instances of cyberattacks that have exposed business or personal data, caused large financial losses, and caused other problems. However, the body of existing research on emerging threats in maritime cyberspace is either inadequate or ignores important variables. Based on the most recent developments in the maritime sector, the article presents a classification of the most serious cyberthreats as well as the risks to cybersecurity in maritime operations and possible mitigation strategies from an educational research perspective.

Keywords: cyberattacks; cybersecurity; maritime sector; data protection; technologies

1. Introduction

The modern maritime industry is reliant more and more on automation, operational integration, and technological advancement. Cyberthreats and fresh possibilities both appear. Cyber technologies are now essential, even critical, for many reasons, such as the management and operation of several systems and procedures in ports and aboard ships, as well as the safety, security, and protection of the ship, the crew, the cargo, and the maritime environment (Andrej et al., 2020). Like every other

major industry, shipping grows in tandem with technological advancements. As more and more tasks are automated, ships get bigger while their workers get smaller. These days, the crews have access to the Internet, and certain onboard devices receive updates while sailing. The risk of external interference and disruption of critical systems increases significantly with the increased reliance on automation. Hackers have the ability to disrupt navigation systems, interfere with ship operation, cut off the vessel's external communications, or steal sensitive data. However, a lot of those working in the marine business are used to working in an "almost invisible" field that is hidden from the general public; hence, not all information concerning successful attacks is made public (Nwankwo et al., 2020a, 2020b). Business owners frequently have the option to remain silent about it out of concern for negative effects on their reputation, claims from clients and insurance providers, and the start of inquiries by outside parties and governmental bodies (Nwankwo et al., 2023a, 2023b; Nwankwo et al., 2021a, 2021b, 2021c). Rizika (2020) reported that there were fifty major overtime hacks in 2017, 120 in 2018, and over 310 in 2019. Following the cyberattacks against the ports of Barcelona and San Diego, the NotPetya virus that cost Maersk suffered $300 million in losses in 2017, and the assault against the Australian shipbuilder Austal in 2018. Due to lost, damaged, or interrupted data or systems, this may lead to operational, safety, or security issues in the shipping industry (Desiana and Prima, 2022). The necessity of providing risk assessment analysis for maritime cybersecurity was elucidated by Haugli et al. (2022). Afenyo and Caesar (2023) recommend further study on risk analysis using a qualitative method approach to fully comprehend the main elements impacting risks and threats to marine cybersecurity.

System-based technology in the littoral nations is vulnerable to emerging maritime cyber threats. Ports and ships are becoming increasingly interconnected thanks to the internet. While increased connectivity improves many areas of the maritime business, it also introduces new threats, such as outages and hackers, for maritime operators and administrations. Due to its delayed recognition of the implications of the new operating environment, the marine sector currently lags behind other industries in terms of cyber risk mitigation and regulation (Hopcraft and Martin, 2018). A crucial aspect of safe and secure shipping operations is the awareness of potential cyber hazards, which is necessary to combat cyberattacks in the marine sector. The marine industry now needs more cyber risk management due to its increased reliance on digitalization, automation, integration, and network-based technologies. Traditionally, cyber risks have mostly targeted operations in other domains as contained in the "2017 of the International Maritime Organization (IMO) guidelines on maritime cyber risk management". Studying cybersecurity in the maritime business is less common than in other sectors like the military, finance, or aviation, e.g., behind other computer-related industries by ten to twenty years (Caponi and Belmont, 2015). In light of the aforementioned data, Consequently, it is imperative to perform a contemporary cyber threat study in order to address the cyber dangers that the marine industry faces. Hence, the purpose of this study is to determine the risks to cybersecurity in maritime operations and possible mitigation strategies from an educational research perspective. For the remainder of the paper, this format will be applied. A brief recap of earlier papers, cybersecurity definitions, and the dangers of cyberattacks in the maritime environment. Cyber threats are facing the maritime sector

currently. Data precautions and mitigating factors. Conclusions and recommendations are provided.

2. Literature section

Determine Cyber risk threats and vulnerabilities must be made more widely known in order to promote safe and secure shipping that is operationally resilient to cyber risks. In order to protect shipping from present and future cyber threats and vulnerabilities, administrations, classification societies, ship owners and operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and other maritime industry stakeholders should step up their efforts as contained in the "resolution MSC.428 (98) of 2017 of the Maritime Cyber Risk Management in Safety Management Systems". The IMO anticipated the arrival and severity of cyber-related threats six years ago; yet, what measures are in place to address these impending concerns? The way different parties behave and interact affects maritime security (Putra et al., 2023). Maritime security can be divided into two categories: those that employ non-traditional security frameworks and those that employ conventional security frameworks (Susilo et al., 2019). Putra et al. revealed four dangers to maritime security in their paper: dangers from resources (like pollution and harm to the sea and its ecology), dangers to navigation, dangers from violence (such as piracy, sabotage, and vital objects of terror), and dangers to sovereignty. Infrastructure security is adversely affected by connectivity via navigation technologies such as GNSS, Radio Detection and Ranging (RADAR), and Automatic Identification System (AIS). Additionally, extremely sophisticated and novel cyberattacks that target in-port information systems and harm on-vessel critical equipment have been directed at shipping companies (Androjna et al., 2020). The likelihood of a successful cyber-attack is further increased by crews' reliance on the Internet, use of unsecured computers, and lack of proper security training. There is ample evidence that one of the main causes of vulnerabilities in the supply chain is the lack of systematic security awareness training for workers; as a result, hackers can successfully access systems using traditional methods like spam emails and Denial-of-Service (DoS) attacks (Goudosis and Katsikas, 2020). In the near future, it will be necessary to have a security plan that offers suggestions for safeguarding the maritime supply chain and a coordinated approach with international marine organizations (Papastergiou et al., 2020). The risk of identity theft and in-port data is increased when software is updated by removable media. Real-time information sharing through new technologies, including the IoT, further raises the risk because of inadequate authentication or unsecured network services.

It is a well-established fact that over 85% of global commercial transportation occurs via maritime means. The majority of products traded internationally are transported by water, and for the majority of developing nations, this percentage is much higher. According to Parka et al. (2019), approximately 80% of global trade is shipped by sea. Simultaneously, growing concerns about cyberattacks as a new threat to maritime operations are brought on by increased communication in international trade (United Nations Conference on Trade and Development (UNCTAD, 2016). For instance, a cyberattack in 2017 cost Maersk, the biggest container shipping firm in the

world, between $200 and $300 million (Svilicic et al., 2019). The Port of Long Beach COSCO facility was the target of a cyberattack in 2018 (Novet, 2017).

According to Mraković and Vojinović (2019), a comprehensive strategy is necessary for managing marine cyber security due to the growing complexity, digitization, and automation of systems within the maritime sector. Every day, the number of networked ship-to-shore systems grows. These systems require special attention in the context of the internet. Cyberattack susceptibility is becoming a big problem in marine computing. Cyber events in the maritime sector have the potential to result in fatalities, loss of control over vessels or confidential information, and abduction of ships or cargo (Mraković and Vojinović, 2020).

The fact that these hacks caused monetary losses in addition to breaches of private or corporate information and harm to a company's reputation emphasizes the importance of cybersecurity in the marine industry. Thus, highlight the pressing necessity to comprehend the entire scope of cyberattacks in the maritime sector and take appropriate measures to tackle the obstacles to economic growth (Mraković and Vojinović, 2020; Mraković and Vojinović, 2019). Hence, the rationale and implications (motivation) for considering this study are due to the fact that cybersecurity is becoming more and more important as a result of the quick digital transformation of the offshore and maritime sectors, which has also brought new dangers and laws, as earlier stated. In light of the numerous recorded cases of security breaches that have revealed corporate or personal data, resulted in significant financial losses, and created other issues, the maritime industry has begun to take cybersecurity seriously. But the amount of study on new dangers in maritime cyberspace that has already been done is either insufficient or leaves out crucial factors. Therefore, this article offers a categorization of the most dangerous cyberthreats, along with information on the dangers to cybersecurity in marine operations and potential mitigation techniques from the standpoint of educational research, based on the most current advancements in the maritime industry.

The article is structured as follows: Section one is the introduction section, comprising the background of the study; Section two is the literature section; Section three discusses an overview of cybersecurity in the maritime domain; Section four highlights the looming cyber threats in the maritime environment; and Section five summarises the mitigating factors. Section six, which is the last section, is centred on the conclusion and recommendations.

3. An overview of cybersecurity in maritime domain

Cybersecurity: The protection of users, devices, and networks should be the cornerstone of any cyber security policy, according to the Piracy International Organization, even though there is no one definition of cybersecurity that is accepted by all. According to the "guidelines on cyber security onboard ships", cyber security is the safeguarding of data, information, and operational technology (OT) from disruption, tampering, and unauthorized access. The term "collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment, organization, and user's assets" is the definition attached to

cybersecurity (Lagouvardou, 2018). Malicious, intentional actions directed at ports, ships, or other organizations in the marine sector are referred to as maritime cyberattacks (maintenanceandcure.com/maritime-blog). Cybersecurity is concerned with maintaining the availability and integrity of data and systems, as well as guaranteeing business continuity and the continued usefulness of digital assets and systems. It goes beyond simply preventing access to systems and data by hackers, which could result in a loss of availability, confidentiality, and integrity.

The proliferation of OT and IoT networks on vessels increases the vulnerability of the marine sector to cyberattacks. Hackers find fertile ground in these digital transformations. The potential dangers included the possibility of financial exploitation, disruption of corporate operations, harm to vital systems, and even fatalities. The biggest worry, however, is how easy it is for an adversary (a hacker) to interrupt operations. The industry saw the pandemonium that ensued from the grounding of the EverGreen in early 2021, affecting the global supply chain. The average cost of a cyberattack in the maritime sector has tripled from $182,000 in 2022 to $550,000, according to a recent analysis by Thetius, law firm Holman Fenwick Willan (HFW), and maritime cybersecurity startup CyberOwl. Here's the depressing reality: Also, the average ransom price has increased to $3.2 million from $3.1 million the previous year, a more than 350% increase in ransom requests. A marine cyberattack could have serious and wide-ranging effects on the sector, affecting a number of different aspects, including but not limited to the following, as summarized in **Table 1**.

Table 1. Implications of cyberattacks.

S/N	Consequences of operation	Remarks/causes
1	Monetary losses	Cyberattacks on ships have significant and varied financial consequences.
2	System disruptions	Sophisticated attack has the potential to seriously interrupt port or ship operations.
3	Compromised security	Attackers have the ability to jeopardize security protocols in ports or on-board ships.
4	Endanger safety	Vessels can easily collide or run aground due to cyberattacks.
5	Environmental disasters	Cyberattacks on maritime systems may have detrimental effects on the environment.
6	Vessels hijacked	Cyberattacks targeting ships may make it easier to smuggle or steal cargo.

The idea, as stated in **Table 1**, outlined the severe repercussions that cyberattacks can have on livelihoods and businesses, including the possibility of environmental catastrophes. Information security needs to be treated seriously since the marine business is just as important as any other sector that propels the world economy.

For the past ten years, the maritime sector has suffered greatly from numerous cyber-related accidents. A summary of some of the recent marine cyberattacks between 2022 and 2023 is contained in **Table 2**; however, more details can be obtained from Tsoukas (2023).

Table 2. Recent maritime cyber incidents/cyberattacks between 2022 and 2023.

S/N	Organization	Date	Incident
1	Sembcorp Marine	December 2022	Sembcorp is a Singapore shipbuilder where an unauthorized user gained access to the IT network through third-party software.
2	Voyager Worldwide	December 2022	Incident occurred that brought all systems down at Voyager a Singapore-based maritime IT solutions vendor whose operations support more than 25% of shipping companies worldwide.
3	Oiltanking and Mabanaft	February 2022	The German logistics company Marquard & Bahls owns Oiltanking and Mabanaft, both of which experienced a cyberattack that rendered their loading and unloading systems completely unusable.
4	Port of Lisbon	December 2022	The Port was suspended for four days after a cyberattack on the port's website and internal computer system on the 25th of December 2022.
5	Royal Dirkzwager	January 2023	The cyberattack group "PLAY" published data of the affected companies on the dark web in January 2023.

4. Looming cyber threats in maritime environment

According to the IMO, maritime cyber risk is a gauge of how much a technological asset can be endangered by an eventuality or incident that could lead to operational, safety, or security problems in the shipping industry because of corrupted, lost, or compromised data or systems. However, despite the fact that the marine industry has been the target of assaults that have shut down supply lines, it appears from a number of indicators that the industry has not given cyber security the same priority as other sectors. The lack of cybersecurity expertise in the maritime industry, the usage of antiquated IT infrastructure, and inadequate cybersecurity awareness and training are the main causes of the high risk of cybercrime in this industry.

4.1. Lack of maritime cybersecurity expert

There is uncertainty regarding the absence of cybersecurity experts, even in the IT sector, because of a lack of funding and a lack of awareness of the significance of this emerging field. Cyber experts were either completely absent or glaringly inadequate when it came to the maritime industry, and maritime professionals lacked the understanding necessary to comprehend the consequences of ignoring this facet of the business. In an era where ships and other vital infrastructure are becoming more networked and linked to IT systems, less than half (40%) of maritime professionals believe their company is spending enough in cyber security, according to new data released by Det Norke Veritas (DNV). The industry needs to maximize the specialized knowledge that is at its disposal. Additionally, there is a need for those with specialized experience in marine cyber-security to disseminate information about dangers and best practices more widely. In shipping, what functions well in other industries could not work.

4.2. Absence of proper cybersecurity training and awareness

According to prior research, human error is the primary cause of 80%–90% of shipping accidents, both directly and indirectly (Teoh and Mahmood, 2018). Human fatigue can lead to errors that result in cyberattack events. Cyberattacks can sometimes happen accidentally by someone who knows very little or nothing about cybersecurity. As a result, people's behaviours can potentially spread malware. For example, people

may inadvertently download viruses onto their computers when they browse fraudulent websites or open unsolicited emails.

4.3. Out-of-date information technology system

Cybersecurity research on vulnerabilities reveals that an excessive reliance on outdated IT infrastructure allows hackers easy access to the system. Sen (2016) concluded that a major problem with the cybersecurity vulnerability in the maritime industry was the over-reliance on antiquated technology and security protocols. Workers in the marine industry, for example, continue to assume that antivirus and firewall software are enough defence against cyberattacks. But malware, including viruses, may be used by hackers to launch assaults, and conventional antivirus software finds it challenging to counteract these sophisticated strikes.

4.4. Use of mobile devices and false website

The ability to operate remote IT systems from a cell phone is becoming very common; many organizations now use smart devices for operations. By visiting phony websites and clicking on phishing emails, sea crew members utilizing personal devices (such as smartphones, tablets, staff USB devices, etc.) run the risk of engaging in cyberattacks and inadvertently infecting the ship's computer system with harmful software. One well-known type of malicious software is malware, which can harm or evaluate a victim's system without the victim's knowledge. Malware can propagate by infecting email attachments or visiting phony websites that contain Trojan horses, worms, exploits, and backdoors (Teoh and Mahmood, 2018).

4.5. Maritime professionals survey on cyber incident

A cyberattack is likely to compel the closure of a vital canal, according to three-quarters of maritime professionals (76%). Over 50% of respondents anticipate that cyberattacks will result in ship collisions (60%), groundings (68%), and possibly even physical harm (injury) or death (56%). Nearly all experts (79%) believe that the sector views the dangers related to cyber security as being just as significant as those related to health and safety (see **Figure 1**).

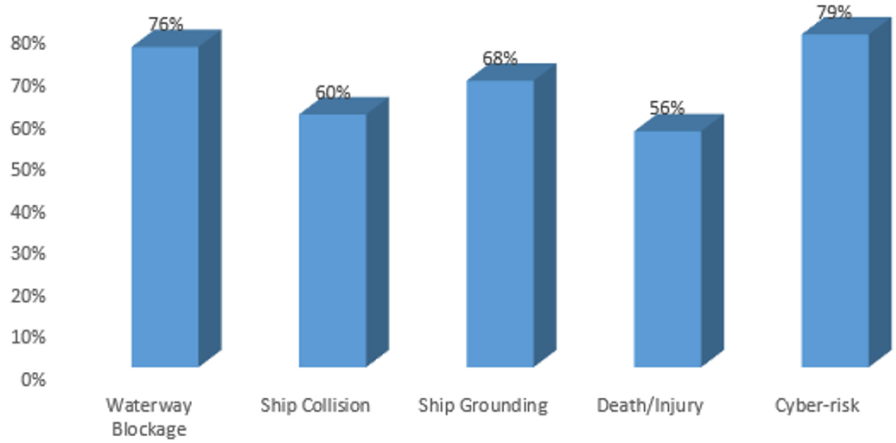

Figure 1. Maritime professionals' analysis cyber incident.

5. Mitigating factors

As reported by Mraković and Vojinović (2019), in response to an upsurge in cyberattacks, the IMO released recommendations for marine cyber risk management and adopted the "National Institute of Standards and Technology (NIST)" framework, which consists of five components: "identification, protection, detection, response, and recovery" (IMO, 2017). The NIST methodology serves as the foundation for the definition of the circular process by the Baltic and International Maritime Councils (BIMCO, 2017).

Identification: This is the process of determining dangers or vulnerabilities both outside and internally. It includes information on employees and their capacity to identify hazards, as well as information about systems, data, and other components that might jeopardise the company's regular IT operations.

Detection: This implies that actions need to be taken to identify the cyber threat promptly. Therefore, immediate threat detection results in the early identification of malicious intents, which is followed by prompt action to safeguard the remainder of the system while limiting the effects to that portion of it.

Protection: This necessitates adhering to backup plans in the event of a danger or occurrence, as well as protocols and actions to promptly recover from the attack.

Response: The creation and execution of strategies and procedures that will repair the system in the event of a cyberattack determine how to respond to threats.

Recovery: This is the final stage, which comes before the discovery of dangers and vulnerabilities and calls for the adoption of countermeasures to recover the compromised system and data.

Despite the broad nature of these features, they offer firms clear guidance; they are free to develop their own protocols and solutions to meet their own demands (Mraković and Vojinović, 2020; Mraković and Vojinović, 2019). As a result, it is thought that cyber security measures need to be based on three fundamental factors (Mraković and Vojinović, 2019).

Human resources: Personnel need to comprehend potential hazards and possess the necessary training and credentials. Additionally, staff members must to be well-versed in risk response and knowledgeable about the protocols, permission levels, and physical security obstacles.

Technology: A suitable system architecture is necessary. Additional testing, authentication, and evaluation processes should be satisfied by the software setup.

Process: The administration of networks and systems, regulations and guidelines for management, audits, agreements with third parties, etc. are examples of processes.

These factors mean that IT is not the only factor in the fight against cyber security. As a result, the business's top executives should be the ones to adopt cyber security protocols via SMS (Mraković and Vojinović, 2019). That is the most crucial prerequisite for developing future plans, educating and training seafarers, and setting up the right environment for effective defence against vulnerabilities and assaults (Mraković and Vojinović, 2019).

Summarily, the maritime industry can reduce cyberattacks in a variety of ways by implementing the following:

- Funding research on cybersecurity.

- Having a team of experts in maritime cybersecurity.
- Training and awareness campaigns.
- Conduct vulnerability assessments.
- Conduct patches and updates when they are due.
- Implementation of modern firewalls (intrusion/detection systems).
- Routine penetration testing.
- System audit and incident logins.
- Having an organized incident response plan.
- Cyber incidents related drills.
- Partnership and information sharing.
- Cybersecurity policy.

The marine sector can greatly increase its resistance to cyberattacks and protect vital systems that enable safe sailing, cargo handling, port operations, logistics, and general efficiency by taking proactive preventive measures.

6. Conclusion and recommendations

Emerging marine cyber risks can affect littoral nations' system-based technology. The internet is increasing the connectivity of ports and ships. Although this connectivity is very beneficial to the maritime sector, it also poses new risks to operators and governments, such as outages and cyberattacks. Understanding the need to educate people about cyber risk threats and vulnerabilities in order to enable safe, secure shipping that is operationally resistant to cyber risks. It is also important to recognize that all stakeholders in the maritime sector, such as administrations, classification societies, ship owners and operators, agents, equipment manufacturers, service providers, ports, and port facilities, should step up efforts to safeguard maritime transportation against cyberthreats and vulnerabilities, both established and emerging. This study describes several mitigating factors and the extent of cybersecurity threats in the maritime industry.

Port terminals, ships, cyberthreats, and other marine systems are all evolving at the same time. The detrimental consequences of cyberattacks are seen not just on board the targeted ship but also in a much larger industry, encompassing interconnection systems, port terminals, shipping businesses, etc. By considerably more than typical expenditures, the GPS signal blockage that caused the crude oil tanker to ground in thick fog is significantly more dangerous than the grounding itself. An ecological disaster will undoubtedly result from the oil leak in such a situation.

In addition to GPS errors and abuse, this article has discussed additional unpleasant experiences that have, for the most part, dire repercussions. Much more work has to be done in addition to the considerable attention that is now being paid to marine cyber security. Regulation is only a first step towards realising the objective. But it appears that crew members offer a greater issue than the rule itself since, in many cases, they carry out certain activities unintentionally and with little to no expertise of the subject, leaving the system vulnerable to assault.

Every aspect of company operations requires awareness; for example, all awareness on board a ship will be ineffective if personnel in the company's

headquarters lack awareness. Business enterprises that are prosperous will eventually be distinguished from those that are not by how resilient they are to cyberattacks.

Future research should focus on enhancing the effectiveness of maritime education in order to reduce the quantity of successful cyberattacks that occur on board ships. The many types of training that will soon be required should get extra consideration. Assuming that businesses comply with the recently enacted "General Data Protection Regulation" from the European Union, comparative analysis should reveal the degree to which the marine sector has effectively addressed the emerging threat of cyberattacks.

This article could serve as a basis for threat modelling. However, there should be further studies that differentiate the threats to the maritime environment and then recommend more specific mitigation measures. It is therefore recommended that the maritime industry kindly consider the following recommendations:

- Examine cyber security as a crucial component of the marine sector.
- Make the cybersecurity policy in the maritime sector more precise.
- Invest in significant cybersecurity awareness initiatives.
- Cooperation in research and development with academic institutions.

Author contributions: Conceptualization, AYM, KEU and LOB; methodology, AYM, KEU and LOB; software, AYM, KEU and LOB; validation, KEU; formal analysis, AYM, KEU and LOB; investigation, AYM, KEU and LOB; resources, AYM, KEU, LOB, AOA, EE, BOO, IEO and UCN; data curation, AYM, KEU and LOB; writing—original draft preparation, AYM, KEU, LOB, AOA, EE, BOO, IEO and UCN; writing—review and editing, AYM, KEU, LOB, AOA, EE, BOO, IEO and UCN; visualization, AYM, KEU and LOB; supervision, KEU and LOB; project administration, AYM, KEU and LOB; funding acquisition, AYM, KEU, LOB, AOA, EE, BOO, IEO and UCN. All authors have read and agreed to the published version of the manuscript.

Acknowledgments: The authors appreciate the authors and publishers, whose articles were used as guides for this study. Also, the authors express gratitude to their respective institutions and the Africa Centre of Excellence on Technology Enhanced Learning (ACETEL), National Open University of Nigeria, Abuja, for supporting this study.

Conflict of interest: The authors declare no conflict of interest.

References

Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. Ocean & Coastal Management, 236, 106493. https://doi.org/10.1016/j.ocecoaman.2023.106493

Androjna, A., Brcko, T., Pavic, I., et al. (2020). Assessing Cyber Challenges of Maritime Navigation. Journal of Marine Science and Engineering, 8(10), 776. https://doi.org/10.3390/jmse8100776

BIOCO. (2009). The guidelines on cyber security onboard ships. BIMCO, Chamber of Shipping of America, Digital Containership Association, Intercargo, Intertanko, Ics, Iumi, Ocimf, Sybass and WSC.

BIMCO. (2017). The guidelines on cyber security onboard ships, version 3. Available online: http://www.ics-shipping.org/docs/default-source/resources/safety-security-andoperations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16 (accessed on 1 December 2023).

Caponi, S., & Belmont, K. (2015). Maritime cybersecurity: A growing threat goes unanswered. Intellectual Property and

Technology Law Journal, 27(1).

COSCO. (2018). Cosco's pre-cyberattack efforts protected network, 2018. Available online: https://www.joc.com/maritime-news/container-lines/cosco/cosco%E2%80%99s-pre-cyber-attack-efforts-protected-network_ 20180730.html (accessed on 1 December 2023).

Desiana, R., & Prima, S. C. (2022). Cyber security policy in Indonesian shipping safety. Journal of Maritime Studies and National Integration, 5(2), 109–117. https://doi.org/10.14710/jmsni.v5i2.13673

Goudosis, A., & Katsikas, S. (2020). Secure AIS with Identity-Based Authentication and Encryption. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, 14(2), 287–298. https://doi.org/10.12716/1001.14.02.03

Haugli, M., Soldal, M., Larsen, M. H., Lund, M. S., & Bjørneseth, F. B. (2022). A model of factors influencing deck officers' cyber risk perception in offshore operations. Maritime Transport Research, 3, 100065. https://doi.org/10.1016/j.martra.2022.100065

Hopcraft, R., & Martin, K. M. (2018). Effective maritime cybersecurity regulation—the case for a cyber code. Journal of the Indian Ocean Region, 14(3), 354–366. https://doi.org/10.1080/19480881.2018.1519056

IMO. (2017). Guidelines on maritime cyber risk management, 2017. MSC-FAL.

Lagouvardou, S. (2018). Maritime Cyber Security: Concepts, problems and models [Master's thesis]. Technical University of Denmark.

MSC. (2018). Maritime Cyber Risk Management in Safety Management Systems. MSC.

Mohamed, B. F., Ukwandu, E., Hindy, H., et al. (2022). Cyber Security in the maritime industry: A systematic survey of recent advances and future trends. Information, 13(1), 22. https://doi.org/10.3390/info13010022

Mraković, I., & Vojinović, R. (2019). Maritime Cyber Security Analysis – How to Reduce Threats? Transactions on Maritime Science, 8(1), 132–139. https://doi.org/10.7225/toms.v08.n01.013

Mraković, I., & Vojinović, R. (2020). Evaluation of Montenegrin Seafarer's Awareness of Cyber Security. Transactions on Maritime Science, 9(2). https://doi.org/10.7225/toms.v09.n02.005

Novet, J. (2017). Shipping Company Maersk says June Cyberattack could cost it up to $300 million, 2017. Available online: https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html (accessed on 1 December 2023).

Nwankwo, W., Adetunji, C. O., Olayinka, A. S., et al. (2021a). The adoption of AI and IoT Technologies: Socio-psychological implications in the production environment. The IUP Journal of Knowledge Management, XIX(1), 50–75.

Nwankwo, W., Adetunji, C. O., Ukhurebor, K. E., et al. (2020a). The precursory machinery of Internet of Things (IoT) in the platform for harmonizing bio-mined data. Nigerian Research Journal of Engineering and Environmental Sciences, 5(2), 786–796.

Nwankwo, W., Adetunji, C. O., Ukhurebor, K. E., Makinde, S. (2023a). Artificial Intelligence-aided bioengineering of eco-friendly microbes for food production policy and security issues in a developing society. In: Adetunji, C. O., Panpatte, D. G., Jhala, Y. K. (editors). Agricultural Biotechnology: Food Security Hot Spot. CRC Press.

Nwankwo, W., Adetunji, C. O., Ukhurebor, K. E., et al. (2023b). Sector-independent integrated system architecture for profiling hazardous industrial wastes. In: Hu, Z., Dychka, I., He, M. (editors). Advances in Computer Science for Engineering and Education VI, Proceedings of the International Conference on Computer Science, Engineering and Education Applications (ICCSEEA 2023).

Nwankwo, W., & Ukhurebor, K. E. (2021b). Nanoinformatics: Opportunities and challenges in the development and delivery of healthcare products in developing countries. IOP Conference Series: Earth and Environmental Science, 655, 012018.

Nwankwo, W., Ukhurebor, K. E., & Ukaoha, K. C. (2020b). Knowledge discovery and analytics in process re-engineering: a study of port clearance processes. In: Proceedings of the 2020 International Conference in Mathematics, Computer Engineering and Computer Science (ICMCECS 2020).

Papastergiou, S., Kalogeraki, E. M., Polemi, N., Douligeris, C. (2020). Challenges and issues in risk assessment in modern maritime systems. In: Advances in Core Computer Science-Based Technologies. Springer.

Parka, C., Shi, W., Zhang, W., et al., (2019). Cybersecurity in the maritime industry: A literature review. In: Proceedings of the International Association of Maritime Universities (IAMU) Conference the 20th Commemorative Annual General Assembly November 2019.

Putra, I. N., Octavian, A., Susilo, A. K., et al. (2023). A hybrid AHP-TOPSIS for risk analysis in maritime cybersecurity based on 3D models. Decision Science Letters, 12(4), 759–772. https://doi.org/10.5267/j.dsl.2023.6.005

Sen, R. (2016). Cyber and Information Threats to Seaports and Ships. Maritime Security, 281–302. https://doi.org/10.1016/b978-0-12-803672-3.00009-1

Susilo, A. K. (2019). Navy development strategy to encounter threat of national maritime security using SWOT-Fuzzy multi criteria decision making (F-MCDM). Journal of Maritime Research, 16(1).

Svilicic, B., Junzo, K., Rooks, M., Yano, Y. (2019). Maritime cyber risk management: an experimental ship assessment. The Journal of Navigation, 72(5), 1108–1120.

Tam, K., Moara-Nkwe, K. & Jones, K., (2021). The use of cyber ranges in the maritime context. Available online: https://pearl.plymouth.ac.uk/handle/10026.1/16067 (accessed on 1 December 2023).

Teoh, C. S., & Mahmood, A. K. (2018). Cybersecurity Workforce Development for Digital Economy. The Educational Review, 2(1). https://doi.org/10.26855/er.2018.01.003

Tsoukas, C. (2023). 2022–2023 Maritime cybersecurity attacks on the rise. Available online: https://marpoint.gr/blog/maritime-cybersecurity-attacks-on-the-rise/ (accessed on 1 December 2023).

UNCTAD. (2016), Review of Maritime Transport, 2016. Available online: http://unctad.org/en/PublicationsLibrary/rmt 2016 (accessed on 1 December 2023).

World Maritime News. (2018). COSCO Shipping Lines Falls Victim to Cyber Attack, 2018. Available online: https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/ (accessed on 1 December 2023).