Journal of Marine Science and Application (2024) 23: 689-706
https://doi.org/10.1007/s11804-024-00443-0

REVIEW

Cyberattacks on the Maritime Sector: A Literature Review

Steve Symes[1], Eddie Blanco-Davis[1], Tony Graham[1], Jin Wang[1] and Edward Shaw[1]

Received: 11 March 2024 / Accepted: 30 July 2024

Abstract

This study is an investigation into cyberattacks on autonomous vessels, focusing on previous "real-world" cyberattacks and their consequences. The future of commercial and noncommercial shipping is moving toward autonomous vessels. Autonomous ships can provide significant financial and logistical benefits for shipping companies and their stakeholders. However, these vessels suffer from shortcomings concerning cybersecurity. Previous cyberattacks are investigated to understand how the command system of an autonomous ship is infiltrated, the consequences of an attack, and the shortfalls of the security of the vessel. This aim is achieved via a literature review concerning cyberattacks on autonomous vessels with a focus on sources indicating how the security systems of previous vessels were breached, the consequence of said cyberattacks, and their capability for recovery. Sources used include Web of Science, Scopus, Google Scholar, Mendeley, Zotero, SciFinder, broadsheet, and newspaper articles. The results of the literature review showed that autonomous vessels are significantly vulnerable to cyberattacks. Autonomous vessels were determined to have relatively easy-to-breach security systems. In most cases, the consequences of a cyberattack had a negative financial impact, a loss of cargo, and a potential breach of oceanic airspace, resulting in military action. The vessels analyzed were left "dead in the water" until they were recovered, and after a severe attack, the affected shipping company servers suffered potential weeklong incapacitation. This study also aims to fill the gaps in the transport industry and maritime market concerning the security of autonomous vessels and viable recovery procedures.

Keywords Autonomous vessels; Cybersecurity; Survivability; Artificial intelligence; Hacking

Article Highlights

- Increased vulnerability of autonomous ships: The study finds that autonomous vessels are significantly more susceptible to cyberattacks compared to traditional ships. This is likely due to their reliance on complex interconnected systems and potentially weaker cybersecurity measures.
- Consequences of cyberattacks: The research the severe consequences of cyberattacks on autonomous ships. These can include financial losses, cargo theft, disruption of maritime traffic, and even military intervention. In some cases, attacks have left vessels disabled and required lengthy recovery times.
- Weak security systems: The study identifies shortcomings in the security systems of autonomous ships investigated. These weaknesses make them easier targets for attackers, highlighting the need for improved cybersecurity measures in this evolving domain.
- Filling the knowledge gap: This research aims to address the lack of knowledge within the maritime industry regarding cybersecurity for autonomous vessels. By investigating past attacks and their impact, the study seeks to inform the development of robust recovery procedures and improved security protocols for the future of autonomous shipping.

✉ Steve Symes
s.w.symes@ljmu.ac.uk

[1] School of Maritime Engineering and Technology, Liverpool Logistics Offshore and Marine Research Institute (LOOM), Faculty of Engineering and Technology, Liverpool John Moores University, Liverpool, L3 3AF, United Kingdom

1 Introduction

This paper is an investigation into the literature on cyberattacks in the maritime sector with a specific onus on the complexities of autonomous ships. The first part of the literature search will analyze the different types of cyberattack techniques and describe each of the most common methods used to target the maritime sector. The second part of the literature search will focus on previous attacks that the industry has faced, the timeline of the attack, and the impact of the attack. The third and final part of the literature search will examine the current techniques used to mitigate these risks to help ensure ship survivability. Then, the aforementioned aspects will be discussed in the "Discussions and Recommendations" section of this study. The main reason for this investigation is that autonomous vessels are still under development, and their widespread adoption faces several challenges. These challenges include; a regulatory framework, the vessels reliability and safety, the ethical considerations and cyber security threats. However, cyber security interlinks with all other viables mentioned above, as, developing a comprehensive international regulatory framework for autonomous vessel operation remains an ongoing process. Ensuring the reliability of onboard systems and guaranteeing the safety of crewless operations is paramount. Questions surrounding liability in case of

accidents and the ethical implications of autonomous decision-making need to be addressed and lastly, Autonomous vessels are susceptible to cyberattacks, requiring robust cybersecurity measures. Therefore, it is crucial that we have a good understanding of the cyber security risks to autonomous vessels prior to the mass production of these vessel types as the cyber threats may be able to be mitigated at the build stage.

In recent years, the maritime industry has witnessed a monumental shift with the emergence of autonomous ships (Gkioulos and Ahmed, 2021). These revolutionary vessels, equipped with cutting-edge technology and artificial intelligence, promise increased efficiency, reduced costs, and improved safety (Ahmed and Gkioulos, 2022). However, as the world embraces this transformative technology, a concerning issue looms on the horizon, i.e., the threat of cyberattacks on accessible high-tech systems implemented by the maritime sector (Ahvenjarvi et al., 2019). This paper delves into the intricacies of this emerging challenge, exploring the potential vulnerabilities and consequences that cyberattacks could pose.

The Rise of Autonomous Ships: Autonomous ships have rapidly gained traction as a viable solution for various maritime operations. Through the use of advanced sensors, machine learning algorithms, and real-time data analysis, these vessels have the potential to revolutionize the industry (Alop, 2019; Martelli et al., 2024; Kayisoglu et al., 2024) by reducing human error, increasing navigational accuracy, and enhancing operational efficiencies. However, with increased reliance on technology comes the inherent risk of cyberattacks (Amro and Gkioulos, 2023b).

Understanding Cyberattacks: Cyberattacks encompass a broad range of malicious activities aimed at compromising the security and integrity of computer systems and networks. Attackers, often referred to as hackers, employ various techniques to exploit vulnerabilities and gain unauthorized access to sensitive information or disrupt critical operations (Amro and Gkioulos, 2023a). These attacks can take many forms, including malware infections, phishing attempts, denial of service (DoS) attacks, and ransomware campaigns (Amro et al., 2023).

Vulnerabilities in Shipping: Despite their advanced technological systems, new high-tech and autonomous ships are not immune to cyber threats (Amro et al., 2020). Their vulnerability derives from their interconnectedness and reliance on complex software and hardware components (Amro et al., 2022). These vulnerabilities can arise from inadequate cybersecurity measures, insecure communication protocols, outdated software, or even human error during the design and implementation phases (Anatoliy et al., 2018). The potential consequences of cyberattacks on the maritime sector and autonomous ships are far-reaching and alarming (Bakdi and Glad, 2021).

Consequences of Cyberattacks on the Maritime Sector: The consequences of successful cyberattacks on the maritime sector can be catastrophic (Ahmed and Gkioulos, 2022). They can range from financial losses due to disrupted operations and compromised cargo to compromised safety and environmental risks (Ahvenjarvi et al., 2019). For instance, a hacker gaining control of the navigation system of an autonomous ship could redirect it toward hazardous areas, leading to collisions or oil spills as acts of terrorism (Anatoliy et al., 2018). Moreover, cyberattacks can undermine public trust in automation (Bakdi and Vanem, 2022).

Since this literature review focuses on autonomous vessels, below is an explanation of the core components and working principles of autonomous vessels.

The core components of autonomous vessels, also known as Maritime autonomous Surface Ships (MASS), include; The navigation systems, decision making and control systems, propulsion systems and communication systems. The navigation system forms the heart of an autonomous vessel. It relies on a combination of sensors, including Global Navigation Satellite Systems (GNSS), radars, Light Detection and Ranging (LiDAR), and cameras, to provide real-time information on the vessel's position, orientation, and surrounding environment (Alop, 2019). The decision making and control system processes data from the navigation system and other onboard sensors. Employing artificial intelligence (AI) and machine learning algorithms, it analyzes the environment, detects obstacles, and determines the optimal course of action for the vessel. This system plays a critical role in collision avoidance, path planning, and adherence to maritime regulations (Boudehenn et al., 2023). The propulsion systems translate the decisions made by the control system into physical actions. They include electric or diesel-powered engines, rudders, thrusters, and other actuators that maneuver the vessel according to the planned course (Loukas, 2019). Autonomous vessels require robust communication capabilities. They can utilize satellite communication for remote control, data transmission, and communication with other vessels and shore-based operations centers (Epikhin and Modina, 2021).

The working principles of MASS can be described informally as a feedback loop which includes the following stages; data acquisition, data processing and analysis, route planning and decision making, command execution, monitoring and feedback. Sensors continuously gather data on the vessel's position, surrounding environment, and internal systems. The decision-making system processes this data using AI and machine learning algorithms. Based on the analysis, the system determines the optimal course of action, including route planning, obstacle avoidance, and speed adjustments. The control system translates these decisions into commands for the propulsion and control systems. The system continuously monitors the vessel's performance and surrounding environment, feeding data back into the loop for ongoing adjustments (Gkioulos and Ahmed, 2021).

2 Objectives

The purpose and scope of this literature review are to answer the following research questions:

1) What cyberattacks have happened previously, and what techniques were used?

2) What were the impact and consequence of each identified cyberattack?

3) What options are available to mitigate the risk of a cyberattack, and what are their shortcomings?

4) What are the recommendations for future research to address their potential shortcomings?

The research hypothesis is that the maritime sector has limited optimally secure practices in place, more specifically, with vessels that have a high degree of tech or are autonomous. It is hypothesized that this review will find that the maritime sector is behind in having technology in place to mitigate cyber threats and that this will be at a great cost to the sector and shipping companies.

3 Methodology

The methodology used in this literature review is preferred reporting items for systematic reviews and meta-analyses (PRISMA). PRISMA provides a standardized checklist, ensuring that the reporting of systematic reviews is transparent and complete. This framework is also applicable to various intervention-based reviews (intervention is the cornerstone behind the reason for conducting this research, as this review will pave the way for the development of a concept, assessment, demonstration, manufacture, in-service, and disposal/termination cycle to tackle the issues faced by cybercriminals targeting the maritime sector). PRISMA also ensures a clear, critical evaluation of methods, assesses potential biases and ultimately presents reliable review outcomes (Liberati et al., 2009).

Section 4 involves a review of previous cyberattack techniques and protection models used in the maritime sector. This review aims to improve the understanding of how the security of a vessel is breached to determine mitigation measures. Moreover, the consequences of cyberattacks on the maritime sector were evaluated to substantiate the benefit of investment to solve this problem. Furthermore, the recovery processes were evaluated to identify any shortcomings of the current procedures.

4 Literature review

The scope of the literature review involves recent case studies of cyberattacks on the maritime sector, new technology related to and including autonomous vessels, and their vulnerability to cyberattacks. The literature will be

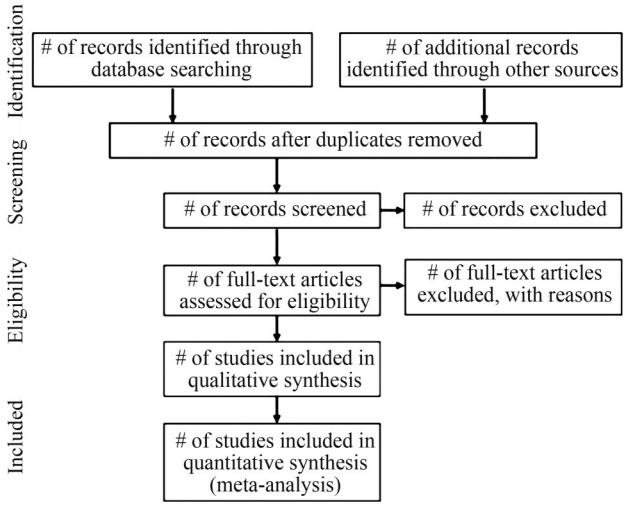

Figure 1 Shows a flowchart of the methodology used in this review (# = Number)

sourced from Web of Science, Scopus, Liverpool John Moores University's internal library services, Google Scholar, and various news sources (e.g., Rules of engagement issued to hacktivists after chaos—BBC News (Tidy, 2023), Royal Navy contractor forced to pay off cybercriminals—The Telegraph (Corfield, 2023), SeeByte to develop secure drone swarm operation methods for Royal Navy (Manuel, 2023), A comprehensive guide to maritime cybersecurity (Mission Secure, 2023), and maritime cyber risk (IMO, 2019). Additional sources included expert knowledge from the coauthors of this review paper.

The keywords or phrases used in the literature search were "autonomous vessels" "cyberattack" "threats to safety" "hacking" "autonomous vessel security" "maritime cybersecurity" "cyberattack techniques" and "cyberattack prevention".

A preliminary literature search indicated that the literature detailing cyberattacks on autonomous ships is currently scarce because of the early stages of the implementation of this type of vessel. Therefore, this literature review primarily investigates cyberattacks on different types of vulnerable vessels and the maritime sector as a whole (for which relevant literature is still more available). It is assumed that cyberattacks on shipping companies and nonautonomous vessels will be conducted similarly against autonomous ships (Gkioulos and Ahmed, 2021). The main difference is the potential consequences, as an autonomous vessel will likely be unmanned (Alop, 2019).

First, the literature search on the Web of Science using the keywords "maritime" "cybersecurity" and "autonomous vessels" showed 30 results. Second, the literature search on Scopus using the same keywords showed 26 research papers. Third, the literature search on Google Scholar resulted in 27 500 academic journals. Therefore, the keywords "ship survivability" "artificial intelligence" and "hacking techniques" were added and produced 717

documents. To further filter the found documents, all documents older than 2019 were omitted, with specific onus on the most recent publications. This final filter resulted in 255 documents (older publications were still read to gauge the concept of the evolution of maritime cyber technology). From the literature search, 76 documents were used because of duplicate publications (Fang et al., 2022) and duplicated cybersecurity techniques. The 76 documents resulted in the identification of six different techniques used in most of the cyberattacks to infiltrate the security system of a ship.

4.1 Cyberattack methods

This subsection of Section 5 describes the six different types of cyberattack techniques and answers the research question: "1) What cyberattacks have happened previously, and what techniques were used?"

4.1.1 Phishing attacks

Phishing attacks involve an attacker's attempt to manipulate human victims into revealing sensitive information, such as login credentials or financial data (Bolbot et al., 2023).

Phishing attacks often involve malicious emails, messages, or even phone calls that appear to come from legitimate sources. In a phishing attack in the maritime sector, a hacker may maliciously claim they represent a shipping company, port authorities, or a maritime enterprise. These messages may contain urgent requests, enticing offers, or false information designed to trick recipients into acting (Bolbot et al., 2020). For example, a phishing email might masquerade as a communication from a shipping company, asking the user to click on a link or download an attachment. Once clicked, the link or attachments can install malware, granting the attackers access to sensitive information or systems (Boudehenn et al., 2023). A common cycle of phishing attacks is illustrated in Figure 2.

4.1.2 Malware attacks

Malware, in the context of maritime cyberattacks, refers to malicious software designed to disrupt, damage, or gain unauthorized access to computer systems and networks within the maritime industry (Chiu et al., 2001). Malware is a broad term encompassing various types of harmful software, such as viruses, worms, trojans, ransomware, and spyware (Dittman et al., 2021).

In maritime cyberattacks, malware can be introduced to systems through various means, such as infected email attachments, compromised websites, or removable media. Once inside a system, malware can execute malicious actions, such as stealing sensitive information, disrupting operations, or granting unauthorized access to attackers (Ehlers et al., 2022). The common types of malware include the following:

1) Ransomware: software that leverages data or access to software until the hacker's demands are satisfied;

2) Spyware: software that monitors other software for data (and, in some instances, the victim through an integrated camera) without the victim's awareness;

3) Adware: software that sends its victims adverts, often leading to false product or service interfaces inviting its victim to provide payment details;

4) Worms: software that spreads automatically through the files of a computer or to other computers within a network;

5) Trojans: named after the Trojan Horse, it is software that appears to be a trusted file that often spreads via malicious emails;

6) Botnets: software that connects a victim's computer to a hacker's network, preventing the victim from using the infected computer.

4.1.3 Denial of service

DoS, in the context of maritime cyberattacks, refers to a type of cyberattack that disrupts or disables the availability of critical systems or networks within the maritime industry (Li and Yu, 2020). A DoS attack overwhelms targeted systems with a flood of illegitimate traffic or resource requests, rendering them unable to function correctly (Liou, 2011).

In the maritime sector, a DoS attack can have severe consequences, affecting vital systems such as navigation, communication, or operational control. By overwhelming these systems with massive amounts of traffic or resource requests, attackers can disrupt vessel operations, impede communication between vessels and shorelines, or even cause safety risks (Li and Yu, 2020).

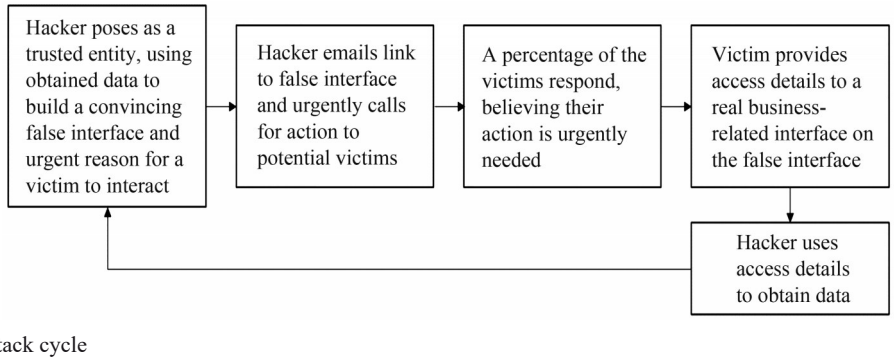

Figure 2 Phishing attack cycle

The two primary forms of DoS attacks are as follows:

1) Network-based DoS: In this attack, the attacker floods the target network or servers with a high-traffic volume, often from multiple sources. This flood of traffic exhausts the resources of the network, leading to service degradation or complete unavailability (Liou, 2011);

2) Application-based DoS: In this attack, specific applications or services within the maritime infrastructure, such as web servers, communication platforms, or control systems, are overwhelmed. Hackers exploit vulnerabilities in these systems or flood them with malicious requests to exhaust their resources, rendering them unresponsive. DoS attacks can be launched by individuals or organized groups with malicious intent, including hacktivists, competitors, or state-sponsored actors. These attacks can be challenging to mitigate, as they often involve high traffic volumes from multiple sources, making it difficult to distinguish legitimate requests from malicious requests (Loukas, 2019).

4.1.4 Man in the middle

In maritime cyberattacks, the term "man in the middle" (MITM) refers to an attack where an unauthorized entity intercepts and potentially alters communication between two legitimate parties without their knowledge. The attacker positions themselves between the sender and the recipient, intercepting.

In the maritime setting, an MITM attack occurs when an attacker gains unauthorized access to the communication channels or systems used for exchanging information between vessels, ports, and other maritime entities. The attacker can then eavesdrop on the communication, modify the data being transmitted, or even inject malicious content to disrupt or manipulate the exchange of information (Sepehri et al., 2022).

An MITM attack in the maritime industry can have serious consequences. For example, an attacker intercepting communication between a vessel and a port authority could modify navigational data, leading to potential safety risks or redirecting the vessel to unauthorized locations. Similarly, intercepting communication between shipping companies and ports could result in cargo misdirection or unauthorized access to sensitive information (Serru et al., 2023). An MITM attack is illustrated in Figure 3.

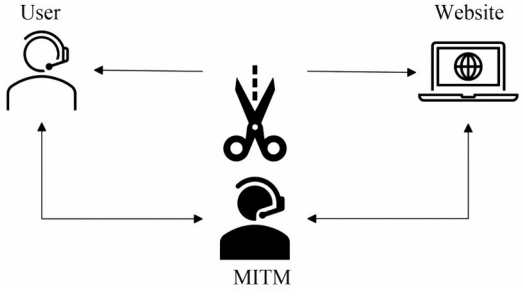

Figure 3 MITM attack

4.1.5 Social engineering

Social engineering in the context of the maritime industry refers to a cyberattack technique where attackers exploit human psychology to manipulate individuals within the sector into divulging sensitive information or performing actions that compromise security (Solnor et al., 2022).

Phishing is a type of social engineering attack that typically targets its victims through emails. The attackers pose as a trusted source, such as a colleague, a client, or even someone from a regulatory authority (Silverajan et al., 2018). The message could ask the recipient to provide confidential information, such as login credentials, financial details, or ship-related data (Tam and Jones, 2018).

To make the attack more convincing, the attackers might research the maritime industry to personalize their messages and increase the likelihood of success. For example, the attackers could mention specific vessels, recent regulatory changes, or industry-specific jargon to gain the trust of the target (Titov et al., 2019).

If an unsuspecting employee falls for the phishing attempt and shares the requested information, then the attackers can gain unauthorized access to critical systems, compromise sensitive data, or even cause disruptions to maritime operations (Tusher et al., 2022).

4.1.6 Physical attacks

Physical cyberattacks in the maritime industry involve exploiting physical assets, systems, or infrastructure to launch or facilitate cyberattacks (Kavallieratos et al., 2020a). These attacks blur the line between physical security and cybersecurity, leveraging vulnerabilities in both realms. Here are a few examples of physical cyberattacks in the maritime industry:

Unauthorized Physical Access: Attackers gain physical access to critical infrastructure, such as ports, ships, or offshore platforms, intending to compromise or tamper with networked systems. By connecting directly to these systems or inserting malware-infected devices, the attackers can disrupt operations, steal data, or plant malicious code (Kavallieratos et al., 2020b).

USB Drop Attacks: Attackers strategically place infected USB devices in areas accessible to maritime industry personnel. When unsuspecting employees find these devices and connect them to their systems, malware can be automatically installed, enabling attackers to gain unauthorized access or control over the compromised systems (Kavallieratos et al., 2021).

Supply Chain Attacks: Attackers exploit weaknesses in the supply chain of the maritime industry by tampering with physical components or systems before they are deployed, including introducing malicious hardware or firmware into devices used for navigation, communication, or other critical functions. Once deployed, these compromised components can be remotely controlled or used as an entry point for cyberattacks (Kavallieratos et al., 2020b).

Physical Infrastructure Tampering: Attackers physically manipulate or sabotage physical infrastructure elements within the maritime industry to cause disruption or enable cyberattacks involving tampering with communication systems, navigation equipment, or physical sensors used for monitoring and control. By compromising these systems, attackers can manipulate data, disrupt operations, or create safety risks (Kavallieratos et al, 2021).

4.2 Cyberattack cases and their impact on the maritime sector

This subsection of Section 4 examines real cases of cyberattacks in the maritime sector and the impacts of such attacks and answers the research question: "2) What were the impact and consequence of each identified cyberattack?"

Significant examples of successful phishing cyberattacks include the China Ocean Shipping Company (COSCO) Group in July 2018 (Bakdi and Glad, 2021), the Det Norske Veritas (DNV) (a leading provider of software and digital solutions predominantly for the energy maritime markets) (Manuel, 2023), and the Compagnie Maritime d'Affrètement (CMA) and Compagnie Générale Maritime (CGM) in 2021 (Mission Secure, 2023). The attack on the DNV alone resulted in the disabling of their systems for weeks, affecting 70 companies and over 1 000 vessels (Manuel, 2023). The "Ragnar Locker" ransomware attack on CMA CGM resulted in the disabling of their systems for days, costing the company 8 million US dollars (Mission Secure, 2023).

In 2017, the "Sea Hunter," an unmanned vessel developed by the Defense Advanced Research Projects Agency in the United States, was penetration tested using malware. In this incident, security researchers from the cybersecurity firm Fortinet employed malware to exploit weak default passwords and unpatched software vulnerabilities (Turner, 2018). In 2017, a cyberattack on the Maersk shipping company was a significant event that drew attention to the potential vulnerabilities in the cybersecurity of the shipping industry. The attack involved the NotPetya malware, which spread rapidly across computer systems worldwide, affecting various port-related industries (Greenberg, 2017). In July 2018, the COSCO Group, one of the world's largest shipping companies, also experienced a significant NotPetya cyberattack that impacted its operations globally (Goud, 2018).

As a result of the aforementioned attacks, Maersk and COSCO were forced to shut down some of their critical systems, including their website, email servers, and certain operational systems, and lost access to their data (Goud, 2018), Sea Hunter was left "dead in the water" (Turner, 2018), and the Maersk shipping company systems were disabled for weeks. The cumulative cost of these attacks is approximately 200 million US dollars (Greenberg, 2017). In April 2020, a Mediterranean shipping company also experienced a malware attack, resulting in its systems having to be reset and multiple days of delay in operations (Baker, 2020).

In 2017, the port of Antwerp, one of Europe's largest ports, experienced a cyberattack that disrupted its container operations. Although the exact details of the attack were not disclosed, it was reported that it involved a DoS component that impacted the IT systems of the port, leading to operational disruptions (Port Technology Team, 2022).

APT28 (Fancy Bear): This cyber espionage group has been linked to several cyberattacks targeting shipping and maritime companies. Their tactics include MITM attacks (National Cyber Security Centre, 2023).

Industrial Phishing Campaigns: Shipping companies have been targeted by sophisticated phishing campaigns, where attackers use social engineering techniques to trick employees into revealing login credentials or installing malicious software. Once attackers gain access, they can conduct MITM attacks to intercept and manipulate communication between shipping companies and their partners or customers (National Cyber Security Centre, 2023).

Operation Shaheen: In 2020, a threat group known as Operation Shaheen targeted shipping companies with MITM attacks. They compromised the email servers of the companies, enabling them to intercept and modify email communications, potentially leading to financial fraud or cargo diversion (Livelli et al., 2020).

The Sea Turtle cyberattack in 2018 was a highly sophisticated and targeted operation that focused on infiltrating maritime and telecom organizations, mainly in the Middle East and North Africa. The attackers employed a technique known as DNS hijacking and gained access to the DNS registrars of the targeted enterprises responsible for managing their domain names and associated IP addresses. By compromising these registrars, the attackers could manipulate the DNS resolution process. Once in control of the DNS infrastructure, the attackers redirected the legitimate traffic of the targeted enterprises to malicious servers under their control, enabling them to intercept and monitor sensitive information, such as emails, login credentials, and other communication data, passing through the compromised networks (Talos, 2018).

"Business Email Compromise" (BEC) Attack: In 2019, a maritime shipping company fell victim to a BEC attack. The attackers impersonated the CEO and sent emails to the finance department of the company, requesting urgent wire transfers to a fraudulent account. The attackers used social engineering techniques, including email spoofing and manipulation, to deceive employees into believing the requests were legitimate, resulting in significant financial losses (Agari, 2020).

"Spear Phishing" Attack on Port Operations: In 2023, a spear phishing attack targeted a major port. The hackers sent customized emails to port employees, posing as trusted

contacts or suppliers. The emails contained malicious attachments or links that, when clicked, installed malware on the victim's system. The malware granted the attackers access to internal networks, disrupting port operations and causing delays in cargo handling (EclecticIQ Threat Research Team, 2023).

"Watering Hole" Attack on Vessel Operations: In 2023, attackers compromised the website of a maritime shipping company that crew members frequently visited. The attackers injected malicious code into the website, which exploited vulnerabilities in the crew members' browsers when they accessed the compromised site, allowing the attackers to gain unauthorized access to vessel systems, compromising critical shipboard systems, and potentially enabling the attackers to manipulate navigation controls or access sensitive information (Mascellino, 2023).

"Phishing" Attack on Port Authority: In 2020, a port authority experienced a phishing attack targeting its employees. The attackers sent convincing emails claiming to be from a maritime regulatory body and requested login credentials to access a new online portal. Unfortunately, some employees fell for the scam and unknowingly provided their credentials, allowing the attackers to gain unauthorized access to the systems and sensitive data of the port (Nicaise, 2021).

Each of the aforementioned attacks had severe consequences for the companies and the maritime sector. The details of these consequences are outlined as follows:

BEC Attack: The maritime shipping company that fell victim to the BEC attack suffered substantial financial losses. The fraudulent wire transfers resulted in funds being transferred to the attacker's account, which were difficult to recover. This incident affected the financial stability of the company and damaged its reputation and customer trust (Agari, 2020).

"Spear Phishing" Attack on Port Operations: The spear phishing attack on a major port caused disruptions in its operations. The malware installed through the malicious emails allowed the attackers to gain unauthorized access to the internal networks of the port, which led to delays in cargo handling, potentially impacting supply chains, customer satisfaction, and financial losses for the port and associated businesses (EclecticIQ Threat Research Team., 2023).

"Watering Hole" Attack on Vessel Operations: The compromise of the website of the maritime shipping company led to unauthorized access to vessel systems, posing risks to vessel operations, as the attackers could manipulate navigation controls, potentially disrupting navigation, endangering crew safety, and compromising sensitive shipboard systems. The incident required extensive remediation efforts, including system restoration, network security enhancements, and employee retraining (Mascellino, 2023).

"Phishing" Attack on Port Authority: The phishing attack on the port authority resulted in unauthorized access to the systems and sensitive data of the port. The attackers exploited the compromised credentials to gain deeper access, manipulate port operations, or access confidential information. The consequences include potential disruptions in port activities, compromised data integrity and confidentiality, and the need for extensive cybersecurity investigations and remediation efforts (Nicaise, 2021).

The following are a few real examples of physical cyberattacks and their consequences experienced by the maritime industry:

Physical Infrastructure Tampering: In 2019, attackers gained unauthorized physical access to the port facility of motor vessel (MV) COSCO and tampered with its communication systems and navigation equipment, resulting in disrupted operations, compromised navigation capabilities, and potential safety risks for vessels in the port. The consequences included delays in cargo handling, financial losses, and damage to the reputation of the port (Polemi and Van-Maele, 2023).

Unauthorized Vessel Access: In May 2022, attackers managed to gain unauthorized access to the commercial vessel Nippon Maru and physically connected a device to its onboard systems, enabling them to manipulate the navigation controls of the vessel, potentially endangering the crew and jeopardizing the safety of the vessel. The consequences included compromised vessel operations, potential accidents, and the need for extensive remediation efforts to mitigate the impact (Polemi and Van-Maele, 2023).

Supply Chain Compromise: In a supply chain attack on a Mediterranean shipping company in 2021, attackers tampered with physical components or systems before their deployment in the maritime industry. For example, compromised navigation devices were deployed on vessels, enabling the attackers to manipulate navigation data remotely. The consequences included compromised navigation accuracy, potential collisions or groundings, and potential disruption to maritime traffic (Polemi and Van-Maele, 2023).

Unauthorized Physical Access to Port Facilities: In July 2022, attackers gained unauthorized access to a port facility in South America by exploiting physical vulnerabilities, such as weak access controls or inadequate surveillance systems. This unauthorized access allowed the attackers to tamper with critical infrastructure, compromise systems, or plant physical devices that facilitated further cyberattacks. The consequences included disruptions in port operations, potential breaches in sensitive data, and compromised safety and security of the port and associated assets (Polemi and Van-Maele, 2023).

4.3 Techniques available to mitigate the risk of cyberattacks and their shortcomings

This subsection of Section 4 presents a review of the current literature concerning the techniques currently and

previously used to mitigate the risk of cyberattacks and answers the research question: "3) What options are available to mitigate the risk of a cyberattack, and what are their shortcomings?"

4.3.1 Phishing

Currently, the only guidelines for the maritime sector to protect against phishing attacks are calls to be vigilant and follow best practices (Amro et al., 2020), which include verifying the sender's identity, checking email domains, avoiding clicking on suspicious links or attachments, and regularly updating and securing systems with reliable cybersecurity measures (Chang et al., 2021). In addition, maritime enterprises should prioritize employee training and awareness programs to help recognize and report potential phishing attempts (Chiu et al., 2001). Although the aforementioned protection techniques are effective in mitigating phishing attacks, they do have some potential shortcomings:

Human Error: Employees can still fall victim to sophisticated phishing tactics despite training and awareness programs. Human error, such as clicking on a malicious link or providing sensitive information, can bypass even the most robust security measures (Anatoliy et al., 2018).

Evolving Techniques: Cybercriminals continuously adapt their phishing techniques to bypass security measures and exploit new vulnerabilities (Alop, 2019). As a result, traditional email filters and spam detection systems may not always detect sophisticated phishing attempts, especially zero-day attacks that exploit unknown vulnerabilities (Ahmed and Gkioulos, 2022).

Insider Threats: Protection techniques primarily focus on external threats, but insider threats can also pose risks. Malicious insiders who have authorized access to systems may attempt phishing attacks or inadvertently compromise sensitive information (Bolbot et al., 2023).

Lack of Standardization: The maritime industry is vast and diverse, making it challenging to establish standardized security practices across all organizations. This lack of uniformity can create inconsistencies in implementing and enforcing phishing protection techniques (Boudehenn et al., 2023).

Advanced Phishing Methods: Phishing attacks are becoming increasingly sophisticated, employing techniques such as spear phishing or whaling, specifically targeting high-level executives or individuals with privileged access. Such targeted attacks can be challenging to detect and mitigate (Bolbot et al., 2020).

4.3.2 Malware

The impact of malware on maritime systems can range from relatively minor inconveniences to severe disruptions. For instance, malware may cause computer systems to slow down, display unwanted advertisements, or crash. In more serious cases, malware can compromise critical navigation, communication, or control systems, jeopardizing the safety of a vessel and its crew and cargo (Epikhin and Modina, 2021).

To protect against malware attacks, maritime enterprises are advised to implement multiple layers of defense, including:

Antivirus and Antimalware Software: Robust and up-to-date antivirus and antimalware solutions need to be deployed to detect, block, and remove malicious software (Greiman, 2019).

Regular System Updates and Patching: All operating systems and software applications need to be regularly updated with the latest security patches and updates to address vulnerabilities that malware may exploit (Fang et al., 2022).

Employee Education and Awareness: Employees need to be trained on best practices to avoid malware, such as not opening suspicious email attachments or clicking on unknown links. A culture of cybersecurity awareness needs to be encouraged throughout the enterprise (Greiman, 2019).

Network Firewalls and Intrusion Detection Systems: Network firewalls and intrusion detection systems need to be implemented to monitor and block unauthorized access attempts and suspicious network activity (Epikhin and Modina, 2021).

Secure Configuration and Access Control: Systems need to be configured securely by following industry best practices and access privileges need to be limited to authorized personnel only to prevent unauthorized installation or execution of malware (Hopcraft et al., 2023).

Regular Data Backups: Regular backups of critical data and systems need to be maintained to mitigate the impact of any malware attack. Backups need to be securely stored and can be readily restored if needed (Issa et al., 2022).

Although the aforementioned protection techniques can significantly strengthen cybersecurity in the maritime industry, they do have some potential shortfalls:

Antivirus and Antimalware Software: Although antivirus and antimalware software are essential, they rely on known signatures and patterns to detect and block threats. Advanced or recently developed malware may evade detection until the software is updated with the latest signatures (Jung et al., 2022a).

Regular System Updates and Patching: Although regular updates and patching help address known vulnerabilities, new vulnerabilities can emerge before patches are available. Enterprises must stay proactive in monitoring vulnerability disclosures and promptly applying patches when they become available (Jung et al., 2022b).

Employee Education and Awareness: Human error remains a significant challenge, even with robust training programs. Employees may still fall victim to sophisticated malware techniques or inadvertently compromise security through unintentional actions, such as clicking on malicious links or providing sensitive information (Kardakova et al., 2020).

Network Firewalls and Intrusion Detection Systems: Although firewalls and intrusion detection systems provide valuable protection, they may not always detect zero-day attacks or advanced persistent threats that utilize sophisticated evasion techniques (Kavallieratos et al., 2020a).

Secure Configuration and Access Control: If access controls and configurations are not implemented correctly, then attackers may exploit misconfigurations or gain unauthorized access to critical systems. Regular monitoring and auditing of access controls are necessary to ensure that secure configurations and access controls are effectively maintained (Kavallieratos et al., 2020b).

Regular Data Backups: Although regular data backups are essential, backups need to be appropriately secured and tested for reliability. Inadequate backup processes or failure to regularly test the restoration process may result in incomplete or unusable backups when needed (Kavallieratos et al., 2021).

4.3.3 Denial of service

To protect against DoS attacks in the maritime industry, enterprises can implement the following measures:

Network Traffic Monitoring: Network monitoring tools need to be deployed to detect abnormal or suspicious traffic patterns indicating a potential DoS attack, enabling early detection and mitigation efforts (Martelli et al., 2020).

Load Balancers and Traffic Shaping: Load balancers and traffic shaping mechanisms need to be implemented to distribute network traffic evenly across systems, preventing overload and ensuring the availability of critical services during high-traffic periods (Martelli et al., 2021).

Redundancy and Failover Systems: Systems with redundant components and failover capabilities need to be designed to ensure that critical services and systems remain operational even if one component comes under a DoS attack (McGillivary, 2018).

Intrusion Detection and Prevention Systems (IDS/IPS): IDS/IPS needs to be utilized to detect and block malicious traffic or requests in real time, preventing them from reaching targeted systems (Meland et al., 2021).

Collaborative Defense: Information sharing and collaboration with industry partners, security organizations, and government agencies need to be engaged to exchange threat intelligence and best practices for DoS mitigation. By sharing information about emerging threats and implementing coordinated defense strategies, the maritime industry can enhance its resilience against DoS attacks (Onishchenko et al., 2022).

Incident Response Planning: Incident response plans need to be developed and regularly tested to ensure a swift and coordinated response during a DoS attack, which includes predefined procedures for isolating affected systems, implementing countermeasures, and restoring services to minimize disruption (Park and Kontovas, 2023).

Although the aforementioned DoS protection techniques are crucial in mitigating the impact of DoS attacks, they do have some potential shortfalls, especially in the context of the maritime industry:

Scalability and Bandwidth: Maritime systems often span large geographical areas, requiring significant bandwidth for communication and data exchange for onboard ship communication and port communication. DoS attacks targeting either the local or other bandwidth systems can generate massive amounts of traffic that may overwhelm network resources, making it challenging to scale up infrastructure to handle such high volumes (Pitropakis et al., 2020).

Zero-Day Attacks: DoS attacks can utilize new and previously unknown vulnerabilities or exploit weaknesses in specific maritime applications or systems. Traditional defense mechanisms may struggle to detect and mitigate these zero-day attacks, as there may not be known signatures or patterns to identify them (Park and Kontovas, 2023).

Distributed DoS (DDoS) Attacks: DDoS attacks involve multiple compromised devices, often forming botnets, to launch coordinated attacks. Maritime enterprises may face challenges distinguishing legitimate traffic from malicious traffic when dealing with large-scale distributed attacks (McGillivary, 2018).

Limited Control in Remote Areas: Maritime systems operating in remote areas or international waters may face limitations in terms of network connectivity, making it difficult to implement real-time traffic monitoring or rely on external mitigation services during DoS attacks (Qiao et al., 2020).

Resource-intensive Defense Measures: The implementation of robust DoS protection measures can require significant resources, such as investment in advanced hardware, software, and expertise. Maritime enterprises, especially smaller enterprises, may face challenges in implementing and maintaining these defense measures because of resource constraints (Qiu et al., 2021).

Insider Threats: Although external DoS attacks are common, insider threats within the maritime industry cannot be overlooked. Malicious insiders who have authorized access to critical systems may launch DoS attacks, making detection and prevention more challenging (Qiao et al., 2020).

Blockchain-based Detection Technologies: Blockchain industrial Internet of Things network hunters utilize a cluster-based architecture for anomaly detection combined with several machine learning models in a federated environment (Yazdinejad et al., 2022). Given the amount of new literature based on the use of blockchain technologies, it is discussed in further detail.

The advantages of these techniques in mitigating the impact of cyberattacks are as follows:

Enhanced Transparency and Traceability: Data stored on a blockchain is visible to all participants, ensuring trans-

parency and traceability in supply chains, financial transactions, and other data-driven processes, which can reduce fraud, errors, and tampering (Yazdinejad et al., 2023).

Improved Tamperproof Security: Blockchain data are cryptographically secured, making it virtually impossible to alter or delete without detection. This immutability strengthens data integrity and reduces the risk of unauthorized modifications (Sakhnini et al., 2023).

Decentralized Trust Model: In contrast to traditional centralized systems, blockchain relies on a distributed network of nodes to verify and store data, eliminating the need for a single point of failure and reducing the risk of data breaches or manipulation by a single entity (Rabieinejad et al., 2024).

Improved Efficiency: By automating processes and eliminating the need for intermediaries, blockchain can streamline data exchange and reduce administrative costs (Rabieinejad et al., 2021).

Enhanced Data Privacy: By controlling access permissions and leveraging encryption, blockchain can provide individuals greater control over their data and improve data privacy (Yazdinejad et al., 2019).

4.3.4 Man in the middle

To protect against MITM attacks, the maritime industry employs various security measures, including:

Secure Communication Channels: The implementation of secure communication protocols, such as encrypted connections using secure sockets layer/transport layer security (SSL/TLS), helps prevent unauthorized interception and manipulation of data during transmission (Sepehri et al., 2022).

Strong authentication and access controls implementing robust authentication mechanisms, such as multifactor authentication (MFA) and secure access controls, help ensure that only authorized parties can access and exchange information, reducing the risk of MITM attacks (Serru et al., 2023).

Certificate-based Encryption: The utilization of digital keys for encryption and authentication can enhance the security of communication channels, making it difficult for attackers to impersonate legitimate entities and conduct MITM attacks (Shapo and Levinskyi, 2021).

Network Monitoring: Continuous monitoring of network traffic and analysis of communication patterns can help detect any suspicious activity or anomaly that may indicate the presence of an MITM attack. Real-time monitoring enables swift response and mitigation efforts (Shipunov et al., 2019).

Regular Security Assessments: Conducting routine security assessments and penetration testing helps identify potential vulnerabilities in communication systems and protocols, allowing enterprises to address them proactively and enhance their resilience against MITM attacks (Silva et al., 2022).

Although the aforementioned MITM protection techniques are important for safeguarding against such attacks in the maritime industry, they do have potential shortfalls:

Insider Threats: MITM attacks can be challenging to detect when perpetrated by individuals authorized to access the communication systems. Insiders who have privileges to intercept or manipulate data can bypass authentication and encryption measures, making it difficult to detect their malicious actions (Shapo and Levinskyi, 2021).

Advanced Attack Techniques: Sophisticated attackers may employ advanced techniques, such as bypassing encryption or exploiting vulnerabilities in communication protocols, to conduct undetected MITM attacks. Constant vigilance and staying updated with emerging attack methods are essential to counter these advanced threats (Serru et al., 2023).

End User Vulnerabilities: Users of the communication systems may fall victim to social engineering attacks, such as phishing, which can compromise their credentials or lead to the installation of malicious software, enabling attackers to access communication channels and conduct MITM attacks (Shipunov et al., 2019).

Interoperability Challenges: The maritime industry involves various stakeholders, each using their communication systems and protocols. Ensuring interoperability and consistent implementation of MITM protection techniques across all entities can be complex, leaving potential vulnerabilities in interconnected systems (Silva et al., 2022).

Legacy Systems and Infrastructure: Maritime enterprises often rely on legacy systems and infrastructure that may have outdated security measures or limited capabilities to defend against sophisticated MITM attacks. Upgrading or replacing these systems can be costly and time-consuming (Silverajan et al., 2018).

Remote and Maritime Connectivity: Maritime operations often occur in remote and challenging environments with limited connectivity options, which makes the implementation of real-time monitoring and response mechanisms difficult, leaving a window of opportunity for MITM attacks to go undetected or unmitigated (Shipunov et al., 2019).

4.3.5 Social engineering

The following are some of the techniques used to protect against social engineering attacks:

Employee Education: Regular cybersecurity training programs need to be conducted to educate employees about social engineering techniques, phishing emails, and other common attack vectors, which will help them recognize potential threats and avoid falling victim to scams (Vagale, 2022).

Strong Passwords: Employees are encouraged to create strong, unique passwords for all of their accounts and systems. MFA needs to be implemented wherever possible to add an extra layer of security (Vagale et al., 2021).

Email Filtering: Robust email filtering systems that can

identify and block malicious emails need to be implemented to minimize the chances of phishing messages reaching employees' inboxes (Vagale, 2022).

Policy and Procedures: Clear security policies and procedures related to handling sensitive information, including guidelines on how to verify identities, report suspicious emails, and manage data securely, need to be established (Vagale et al., 2021).

Regular Updates and Patches: All software, applications, and operating systems need to be updated with the latest security patches to protect against known vulnerabilities that attackers may exploit (Vagale, 2022).

Incident Response Plan: An incident response plan specific to social engineering attacks needs to be developed. This plan should include steps to be taken in case of an attack, such as reporting incidents, isolating affected systems, and communicating with relevant stakeholders (Yoo and Jo, 2023).

Security Awareness Culture: A security-aware culture needs to be fostered within the maritime industry by promoting a mindset of constant vigilance. Open communication among employees is encouraged so they feel comfortable reporting suspicious activities or potential security breaches (Vagale, 2022).

Regular Security Assessments: Periodic security assessments and penetration testing need to be conducted to identify vulnerabilities and address them proactively, which will help identify any weakness in systems, processes, or employee knowledge that could be exploited in social engineering attacks (Vagale et al., 2021).

Verify Requests: Employees are encouraged to verify requests for sensitive information, especially if they are unusual or out of the ordinary, by contacting the supposed sender through a different channel (e. g., a phone call) to confirm the legitimacy of the request (Yoo and Jo, 2023).

Keep Up with Industry Updates: Employees are encouraged to stay informed about the latest trends and tactics in social engineering attacks within the maritime industry, which will help adapt security measures and stay one step ahead of potential threats (Yoo and Park, 2021).

Although the aforementioned points are effective in preventing social engineering attacks, it is important to acknowledge their potential shortcomings:

Human Error: Despite education and training, employees can still make mistakes and fall for social engineering tactics. Eliminating human error is challenging, as attackers continuously evolve their techniques to exploit psychological vulnerabilities (Zhou et al., 2018).

Advanced Attacks: Highly sophisticated social engineering attacks may bypass traditional email filters and security measures, making them difficult to detect. Attackers may employ advanced tactics, such as spear phishing, which targets specific individuals or groups, making it more difficult to identify and prevent (Zhou et al., 2021).

Lack of Awareness: Some employees may not pay sufficient attention or take cybersecurity seriously even with regular training, which can lead to complacency and increase the risk of falling victim to social engineering attacks (Zhou et al., 2018).

Insider Threats: Social engineering attacks can also be conducted by malicious insiders who have legitimate access to systems and sensitive information. Preventing such attacks requires a combination of technical controls, employee monitoring, and strong access management policies (Vagale, 2022).

Rapidly Evolving Tactics: Attackers continuously adapt their social engineering tactics to exploit new vulnerabilities and technological advancements. To stay ahead, enterprises must keep up with the latest trends and invest in updated security measures (Vagale et al., 2021).

False Sense of Security: Relying solely on technological solutions and security measures may create a false sense of security. Although the implementation of strong technical controls is important, fostering a culture of security awareness is equally crucial to empower employees to participate actively in maintaining a secure environment (Vagale et al., 2021).

Resource Constraints: Small maritime enterprises or those with limited budgets may face challenges in implementing all of the recommended security measures. Thus, it is important to prioritize based on risk assessments and allocate resources effectively to address the most critical vulnerabilities (Yoo and Park, 2021).

Lack of Standardization: The maritime industry comprises various organizations and stakeholders with different levels of cybersecurity maturity. The absence of standardized security practices and regulations can create inconsistencies in implementing effective social engineering prevention strategies (Yoo and Jo, 2023).

4.3.6 Physical attacks

Physical cyberattacks pose unique challenges as they require physical access, technical expertise, and an understanding of physical and cyber vulnerabilities. To mitigate the risks associated with physical cyberattacks, the following are some protection measures that can be implemented:

Physical Access Controls: Strong access controls need to be implemented to restrict physical access to critical infrastructure, ships, and sensitive areas, including employing surveillance systems, secure fencing, access cards, biometric authentication, and visitor management protocols (Amro and Gkioulos, 2023b).

Employee Awareness and Training: Employees need to be educated about the risks of physical cyberattacks and the importance of following security protocols and trained to recognize suspicious behavior, report potential vulnerabilities, and adhere to access control procedures (Shapo and Levinskyi, 2021).

Secure Supply Chain: Secure supply chain practices need

to be established to verify the integrity of components and systems before deployment. The cybersecurity practices of suppliers need to be regularly assessed and thorough risk assessments need to be performed to ensure the absence of compromised or tampered components (Kavallieratos et al., 2020a).

Cybersecurity Measures: Robust cybersecurity measures need to be implemented to protect systems from both physical and cyber threats, including network segmentation, firewalls, intrusion detection systems, antivirus software, regular patch management, and encryption of sensitive data (Kavallieratos et al., 2021).

Incident Response Planning: A comprehensive incident response plan that addresses physical and cyberattacks needs to be developed, including protocols for identifying, containing, and mitigating the impact of a physical cyberattack. The plan needs to be regularly rehearsed and updated to ensure it remains effective and aligns with emerging threats (Chang et al., 2021).

Physical Security Audits: Regular physical security audits need to be conducted to identify vulnerabilities and gaps in security measures, including assessing physical access controls, surveillance systems, alarm systems, and other physical security mechanisms. Any identified weakness needs to be promptly addressed (Kavallieratos et al., 2020a).

Employee Background Checks: Thorough background checks for employees and contractors with access to critical systems and infrastructure need to be implemented to mitigate the risk of insider threats or individuals with malicious intent gaining physical access (Kavallieratos et al., 2021).

Incident Reporting and Information Sharing: A culture of reporting and information sharing needs to be established within the maritime industry. Employees and enterprises are encouraged to report suspicious activities, physical breaches, or attempted cyberattacks and collaborate with industry peers, authorities, and cybersecurity organizations to share threat intelligence and best practices (Kavallieratos et al., 2020a).

Continual Improvement: Security measures need to be regularly evaluated and updated based on emerging threats, industry best practices, and lessons learned from incidents. Employees and enterprises are encouraged to stay informed about evolving physical and cyberattack techniques and adapt security strategies accordingly (Amro et al., 2022).

Although the aforementioned protection methods are effective in mitigating physical cyberattacks in the maritime industry, it is essential to be aware of their potential shortcomings:

Human Error: A common and repetitive occurrence throughout the differing cybersecurity attack techniques is that, despite training and awareness programs, employees may still unknowingly engage in actions that compromise physical and cybersecurity measures. Mistakes, such as leaving physical access points unsecured or falling for social engineering tactics, can undermine the effectiveness of protection methods (Amro and Gkioulos, 2023b).

Insider Threats: Protection methods may not eliminate the risk of insider threats. Employees or contractors with authorized access to critical infrastructure can intentionally or unintentionally engage in malicious activities that bypass physical and cybersecurity measures (Amro et al., 2022).

Evolving Tactics: Attackers continually adapt their tactics to exploit vulnerabilities and bypass security measures. Protection methods that are not regularly updated or lack flexibility may become outdated and less effective against new or advanced physical cyberattacks (Kavallieratos et al., 2020a).

Budget Limitations: The implementation of comprehensive protection methods requires financial resources. Smaller maritime enterprises or those with limited budgets may face challenges when implementing all recommended measures, potentially leaving vulnerabilities that attackers can exploit (Kavallieratos et al., 2021).

Lack of Standardization: The absence of standardized security practices and regulations in the maritime industry can lead to inconsistencies in implementing protection methods. This lack of standardization can create gaps in security coverage and makes it challenging to address threats uniformly across the industry (Amro et al., 2023).

Complexity and Integration: Protecting against physical cyberattacks requires a combination of physical security measures and cybersecurity practices. Integrating these measures and ensuring seamless coordination can be complex and challenging, especially when dealing with legacy systems or diverse infrastructure across the maritime industry (Amro and Gkioulos, 2023a).

Response and Recovery: Although incident response plans are crucial, their effectiveness depends on the speed and efficiency of detection, containment, and recovery efforts. Delayed or inadequate response can prolong the impact of a physical cyberattack and exacerbate the associated damages (Kavallieratos et al., 2020a).

4.3.7 Mitigation strategies

Below, we will look at the strategies to mitigate the various attack methods. From the literature, it seem that a holistic approach should be taken to the cyber security attack mitigation of autonomous vessels, as detailed below.

Traditional approaches to network security must be integrated throughout the design and development lifecycle, fostering a culture of "security by design" (Sahay et al., 2023). This necessitates the adoption of secure coding practices, rigorous vulnerability assessments, and penetration testing to identify and eliminate weaknesses before deployment. Network segmentation plays a critical role in mitigating the spread of potential threats (Bolbot et al., 2020). Critical control systems responsible for navigation

and propulsion should be isolated within a highly secure network segment with restricted access (Amro et al., 2020). Non-essential systems, such as entertainment or internet access, should reside in a separate segment with limited ability to interact with the core functions of the vessel (Amro and Gkioulos, 2023a). Zero-trust security principles further enhance protection by minimizing inherent trust within the network. This approach requires constant verification for all access attempts, typically through multi-factor authentication. Additionally, the principle of least privilege ensures that users only have the minimum level of access necessary for their tasks, reducing the potential damage caused by compromised credentials (Li and Yu, 2020). Continuous network monitoring and anomaly detection systems are crucial for identifying suspicious behavior and preventing unauthorized access (Zhou et al., 2018). Encryption serves as a vital defense mechanism, safeguarding the confidentiality and integrity of data. All communication channels, both internal and external, should be encrypted using robust algorithms (Ahvenjarvi et al., 2019). Data encryption at rest offers an additional layer of protection for sensitive information stored on the vessel's systems. Secure key management practices are paramount to ensure the effectiveness of encryption measures. Software updates, while essential for maintaining functionality, can introduce vulnerabilities if not handled securely (Li and Yu, 2020). Digital signatures verify the authenticity of updates before installation, while secure download protocols ensure the integrity of the downloaded code during transmission. Maintaining a record of all software versions deployed on the vessel facilitates easier identification and rollback procedures in case of security issues (Liou, 2011). While autonomous operation is the ultimate goal, a well-trained crew remains an essential line of defense. Crew members should possess a fundamental understanding of cybersecurity principles to recognize potential threats like phishing attempts, social engineering tactics, and anomalous network activity. Furthermore, established procedures for reporting suspected cyberattacks and initiating incident response protocols empower crew members to play a proactive role in safeguarding the vessel (Qiao et al., 2020). International collaboration is crucial for establishing a comprehensive framework for autonomous vessel cybersecurity (Agari, 2020). IMO presents a platform for developing standardized guidelines that address minimum security requirements (IMO, 2019). These guidelines should encompass secure coding practices, network segmentation and access control, encryption protocols, software update procedures, crew training, and standardized reporting and incident response protocols.

By adopting a holistic approach that integrates these security measures within the design, operation, and regulatory landscape, the autonomous vessel industry can navigate the evolving cybersecurity landscape and ensure the safe and reliable operation of these next-generation vessels (Kardakova et al., 2020).

4.4 MASS vulnerabilities

The works by (Kavallieratos et al., 2019) (Sahay et al., 2023) delves into the cybersecurity vulnerabilities plaguing Cyber-Enabled Ship (C-ES) systems. The findings expose a concerning landscape, highlighting critical weaknesses within the very systems upon which safe and efficient C-ES operation relies. The study identifies the Human-Machine Interface (HMI), Navigation System (NavS)–encompassing Automatic Identification System (AIS) and Electronic Chart Display and Information System (ECDIS)–and Global Maritime Distress and Safety System (GMDSS) as the most susceptible components. Notably, AIS and ECDIS further complicate the picture by being vulnerable sub-systems within the already high-risk NavS. This nested vulnerability creates a cascading effect, where the weaknesses of sub-systems propagate and elevate the risk profile of the parent system. The report underscores a crucial concept: parent systems inherit the vulnerabilities of their sub-systems. This emphasizes the criticality of securing foundational components like AIS and ECDIS. Robust security measures for these sub-systems are essential for fortifying the overall security posture of the NavS and, consequently, the entire C-ES. The analysis goes beyond mere vulnerability identification. It emphasizes the criticality of the affected systems. AIS, ECDIS, and GMDSS are not just vulnerable; they are indispensable for safe and efficient C-ES operation. Their integration with the Bridge Alert System (BAS) underscores their role in ensuring vessel safety. Compromising these systems could have disastrous consequences. The analysis employs the STRIDE threat framework to assess the threat landscape. Denial-of-Service and Spoofing emerge as the most critical threats, with a concerning frequency of occurrence (11 and 9 times respectively). These attacks have the potential to disrupt essential C-ES functions. Tampering and Elevation of Privilege are deemed medium threats due to their complexity and the attacker's presumed high motivation. Repudiation and Information Disclosure are considered low-risk threats within the C-ES context. The identified vulnerabilities demand immediate attention. Prioritizing security measures for HMI, AIS, ECDIS, and GMDSS is crucial. Additionally, mitigating Denial-of-Service and Spoofing attacks should be a top priority for securing C-ES systems. A multi-pronged approach that addresses both technical vulnerabilities and strengthens incident response protocols is essential for navigating the evolving cybersecurity landscape and ensuring the safe and reliable operation of C-ES vessels.

5 Discussions and recommendations

This section discusses the findings presented in Section 4 and provides recommendations to combat cyberattack

risks based on the aforementioned findings. This section answers the research question: "4) What are the recommendations for future research to address their potential shortcomings?"

Given the literature reviewed in the preceding section, the maritime industry needs to prioritize investments in better protection methods to defend against a range of cyber threats. By addressing the investigated threats comprehensively, the industry can enhance its cybersecurity resilience and safeguard critical operations, data, and infrastructure.

As outlined in Section 4.3.1, to combat phishing attacks, the industry must invest in robust email security tools, implement MFA, and conduct regular employee training to raise awareness about the dangers of phishing and how to identify and report suspicious emails.

As stated in Section 4.3.2, to defend against malware, the maritime industry should deploy advanced endpoint protection solutions, regularly update and patch systems, and conduct regular vulnerability assessments. Educating employees about safe browsing habits and the risks associated with downloading or opening files from untrusted sources is crucial.

Given the literature reviewed in Section 4.3.3, DoS attacks can be mitigated through the implementation of robust network firewalls, IDS/IPS, and DDoS mitigation services. Regular testing and monitoring of network infrastructure can help detect and respond promptly to DDoS attacks.

To summarize the literature on DoS (Section 4.3.3), the maritime industry should leverage encryption technologies, such as SSL/TLS, to counter MITM attacks to secure data in transit. Strong access controls and authentication mechanisms should be implemented to verify the identities of communication endpoints and prevent unauthorized interception and tampering.

Addressing social engineering attacks requires several factors, i.e., employee education and strict access controls. Regular training programs should educate employees about the tactics used in social engineering attacks, emphasizing the importance of verifying requests for sensitive information and reporting any suspicious activity. In addition, implementing strong access controls and properly managing user privileges can help mitigate the risk of unauthorized access and information disclosure.

To protect against physical attacks, the maritime industry should invest in comprehensive physical security measures, including implementing surveillance systems, access controls, and intrusion detection systems and conducting regular physical security audits. Collaborating with security experts and sharing information about physical cyberattacks can also enhance the capability of the industry to prevent and respond to such incidents.

An important factor identified by the literature search is bandwidth. As stated previously, two types of bandwidth frequencies are used. Base-to-ship communications and frequencies enable local communication on board the vessel. The literature reviewed in the preceding section has shown that these frequencies are a target for cyberattacks because of the ease with which they are identified. The defensive measures identified to mitigate the risk of cyberattacks are firewalls, IPS, network segmentation, and various access control aspects, e.g., strong passwords and MFA. However, as stated in Section 4, all of the aforementioned defenses can be breached. For example, skilled attackers can exploit misconfigurations or zero-day vulnerabilities in firewalls to bypass them. IPS relies on predefined signatures to detect attacks; however, signatures are changing and evolving. Network segmentation limits damage, but attackers within a segment can still cause harm.

A factor identified in Section 4.3 is the standardization of the risk control methods employed to mitigate the impact of a cyberattack. It could be argued that standardization will always be a factor because of the differences in culture, vessel systems, and practical training and qualifications of staff from company to company or vessel to vessel.

Autonomous vessels are unmanned. The unmanned aspect may influence cybersecurity threats and defenses. However, because of the novelty of autonomous vessels, identifying relevant cases of specifically unmanned vessels being attacked is difficult. Given the systems in place to control such vessels, it could be said that this poses more of a risk as a completely unmanned vessel that has experienced a DoS attack could find its controls malfunctioning, as per Section 4.1.3, and the vessel could find itself dead in the water. This issue, in the short term, could be combated by having some personnel on board to manually override the controls, which could increase costs; however, those cost increases could be substantiated because of the risk of cybercriminals stalling or gaining control of the vessel.

As mentioned in Section 4.3.3, blockchain-based technologies can be utilized for data security. Blockchain-based technologies, with their decentralized and immutable ledger, have sparked interest in improving data security across various industries, have shown promising aspects pertaining to the security of maritime vessel networks, and can be potentially applied to autonomous vessels. However, Yazdinejad et al. (2023) stated that current blockchain-based technologies struggle when handling large volumes of transactions, leading to scalability issues and potential performance limitations. Rabieinejad et al. (2021) stated that the implementation of blockchain solutions can be complex and require significant technical expertise and that integration with existing systems can be challenging. Nakhodchi et al. (2021) stated that the lack of clear legal frameworks and standardized protocols can create uncertainty and hinder wider adoption. Some blockchain protocols, particularly Proof-of-Work, require significant computing power, raising concerns about energy consumption and environmental impact. Although blockchain

provides strong security, it may not be suitable for all types of data or require additional functionalities, such as data deletion or modification, in specific contexts.

This literature review identifies many different techniques and mitigation measures, some of which overlap and repeat in different sections because of the nature of cyberattacks being dynamic in approach. Thus, the techniques used to hack into the same system can cover multiple different techniques, and the attacker would no doubt find themselves faced with a plethora of different mitigation methods. However, a consistency was found in this literature review. Anatoliy et al. (2018), Kardakova et al. (2020), Shipunov et al. (2019), Vagale et al. (2021), Zhou et al. (2018), Shapo et al. (2021), and Amro et al. (2023) all referred to human error being a factor for cyberattacks. Amro et al. (2023) and Shapo et al. (2021) argued that human error will always be a problem in the maritime sector, even across multiple disciplines. Anatoliy et al. (2018) and Kardakova et al. (2020) stated that human error issues can be reduced with the use of automated systems. However, Vagale et al. (2021) stated that reliance on automation will significantly reduce the skillset of seafarers. A recommendation for this issue would be to take human factors approach to a human reliability assessment (HRA) of personnel in their specific roles, similar to the study conducted by Symes et al. (2022). Symes et al. (2022) examined the performance-shaping factors of day-to-day roles within the maritime industry and implemented a linear discriminant analysis to obtain a classification performance prediction percentage of each group of participants dealing with performance-shaping factors. The higher the prediction percentage, the higher the likelihood of a potential human error in that specific role (e.g., maritime vessel command system network programmer, system analyst, or network architect) or experiencing a specific performance-shaping factor (e.g., increased workload, fatigue, or distraction). The downside to this would be the human element of the investigation, as every human is different. Therefore, the number of candidates used would have to be relatively high (i.e., 20+).

Autonomous vessels, while offering significant advantages, introduce a new attack surface vulnerable to cyber threats (Amro et al., 2023). Below is a summary of the specific attack vectors and mitigation strategies. From the literature reviewed above, these attack vectors are based on traditional methods with a new twist that is specific to MASS. Although traditionally targeting human users, phishing attacks can be adapted for autonomous vessels with internet connectivity (Amro et al., 2020). Malicious emails or websites could be designed to trick shore-based operators into downloading malware or granting unauthorized access to critical systems (Amro et al., 2022). Malware specifically designed to target the control systems of autonomous vessels could disrupt navigation, manipulate sensor data, or even take control of the vessel (Li and Yu, 2020). These common traditional attack methods can infiltrate autonomous vessels through various channels (Kayisoglu et al., 2024). Remote access points used for monitoring and control can be exploited if not properly secured. Weak passwords, unencrypted communication, and lack of multifactor authentication can create vulnerabilities. Malicious code can be embedded in software updates downloaded from compromised servers (Kavallieratos et al., 2019). Attacks targeting manufacturers of onboard systems or software providers could introduce vulnerabilities that remain undetected until deployed on the vessel (Sahay et al., 2023). Beyond traditional methods, autonomous vessels are susceptible to attacks that exploit their unique characteristics. Attackers could manipulate sensor data (GPS, LiDAR) to create false information about the environment, potentially leading the vessel astray or causing collisions (Kavallieratos et al., 2021). Machine learning algorithms used for decision-making can be vulnerable to adversarial attacks. Malicious data fed to the system could lead to faulty route planning or incorrect responses to real-world situations (Bolbot et al., 2020).

6 Conclusions

Given the outcome of the literature review, it can be said that, as technology continues to advance and ships become more “high-tech” with complex systems, the maritime sector faces an increasing risk of cyberattacks. Integrating digital technologies, automation, and interconnected systems not only brings numerous benefits to the industry but also opens up new vulnerabilities that malicious actors can exploit.

The maritime sector must recognize that the potential for cyberattacks increases proportionally as these technological advancements continue. With more sophisticated systems and interconnected networks, the attack surface expands, providing cybercriminals greater opportunities to infiltrate, disrupt, or compromise critical maritime operations. Many high-tech systems require protection against cyberattacks. The following is a list of example systems that are vulnerable to cyberattacks in modern-day shipping:

1) Crew networks (providing Wi-Fi, entertainment, and email access);
2) Satellite communication systems;
3) Emergency position indicating radio beacon;
4) Radar and other navigation-aiding technologies;
5) Voyage data recorder;
6) Passenger information systems;
7) Power management systems;
8) Machinery management systems;
9) All monitoring systems.

In summary, the maritime industry needs to prioritize

cybersecurity and invest in robust protection measures, including implementing advanced cybersecurity solutions, conducting thorough risk assessments, and adopting best practices for secure system design, implementation, and maintenance.

In addition, fostering a cybersecurity-focused culture within the industry, which entails promoting awareness, training employees on cyber threats and best practices, and establishing effective incident response plans to mitigate the impact of potential attacks, is crucial.

By proactively addressing the growing cyber threat landscape, the maritime sector can adapt to the changing technological landscape and safeguard its operations, assets, and data from the detrimental consequences of cyberattacks. The industry needs to stay vigilant, collaborate with cybersecurity experts, and continuously enhance its cybersecurity defenses to stay ahead of evolving threats. By doing so, the maritime sector can confidently navigate the digital era, protecting its critical infrastructure and ensuring the safety, security, and reliability of maritime operations in an increasingly high-tech environment.

The future research directions for this area are somewhat difficult to define, given that the number of unmanned vessels to date is low. However, a holistic approach could be applied to simulate or predict job roles for autonomous vessels, with a specific onus on cyber threats, which would involve a new-generation HRA that incorporates a human factors approach, such as neuroimaging, to detect vulnerabilities in humans or specific job roles in the maritime autonomous vessel sector.

Competing interest Jin Wang is an editorial board member for the Journal of Marine Science and Application and was not involved in the editorial review, or the decision to publish this article. All authors declare that there are no other competing interests.

References

Agari (2020) Damages from business email compromise (BEC) top the 2019 FBI IC3 list. Retrieved from https://www. agari. com/blog/business-email-compromise-2019-ic3#:~:text=Business%20Email%20Compromise%20(BEC)%20was,on%20cybercrime%20impact%20in%202019 [Accessed on Sep. 19, 2023]

Ahmed A, Gkioulos V (2022) Utilizing AIS for command and control in maritime cyber attacks. Computer security-ESORICS, 535-553. https://doi.org/10.1007/978-3-031-17143-7_26

Ahvenjarvi S, Czarnowski I, Szyman P (2019) Safe information exchange on board of the ship. Trans-nav International Journal on Maritime Navigation and Safety of Sea Transportation 13(1): 165-171. DOI: 10.12716/1001.13.01.17

Alop A (2019) The main challeges and barriers to the successful 'smart shipping'. Transnav-International Journal on Marine Navigation and Safety of Sea Transportation 13(3): 521-528. DOI: 10.12716/1001.13.03.05

Amro A, Gkioulos V (2023a) Evaluation of a cyber risk assessment approach for cyber physical systems: maritime and energy use cases. Journal of Marine Science and Engineering 11(4). https://doi.org/10.3390/jmse11040744

Amro A, Gkioulos V (2023b) Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. Int Journal of Information Security 22(1): 249-288. https://doi.org/10.1007/s10207-022-00638-y

Amro A, Gkioulos V, Katsikas S (2020) Connect and protect: Requirements for maritime autonomous surface ship in urban passenger transportation. Computer Security, ESORICS 11980: 69-85. https://doi.org/10.1007/978-3-030-42048-2_5

Amro A, Gkioulos V, Katsikas S (2023) Assessing cyber risk in cyber physical systems using the ATT&CK framework. ACM Transactions on Privacy and Security 2: 26. https://doi.org/10.1145/3571733

Amro A, Oruc A, Katsikas S (2022) Navigation data anomaly analysis and detection. Information 13(3): 104. https://doi.org/3390/info13030104

Anatoliy P, Kristina V, Aleksandr V (2018) Technologies of safety in the Bank Sphere from cyber attacks. ELConRUS. Moscow, 14-19. DOI: 10.1109/EIConRus.2018.8317040

Bakdi A, Glad IV (2021) Testbed scenario design exploiting traffic big data for autonomous ship trails under multiple conflicts with collision/grounding risks and spatio-temporal dependencies. IEEE Transactions on Intelligent Transportation Systems 22(12): 7914-7930. DOI: 10.1109/TITS.2021.3095547

Bakdi A, Vanem E (2022) Fullest COLREGs evaluation using fuzzy logic for collabarative decision making analysis of autnomous ships in complex situatuions. IEEE Transactions on Intelligent 23 (10): 18433-18445. DOI: 10.1109/TITS.2022.3151826

Baker J (2020) MSC confirms website shutdown caused by cyber attack. Retrieved from LLoyds List: https://lloydslist.com/LL1131957/MSC-confirms-website-shutdown-caused-by-cyberattack#:~:text=The%20website%20and%20headquarters%20network,due%20to%20a%20malware%20attack [Accessed on Apr. 16, 2020]

Bolbot V, Theotokatos G, Van Collie A (2023) A novel risk assessment process: Application to an autonomous inland waterways ship. IMEJRR Glasgow. DOI: 10.1177/1748006X211051829

Bolbot V, Theotokatos G, Vassalos D (2020) A novel cyber-risk assessment method for ship systems. Safety Science, 224871472. https://doi.org/10.1016/j.ssci.2020.104908

Boudehenn C, Cexus J, Boudraa A (2023) Holistic approach of integrated navigation equipment for cybersecurity at sea. ICCSASMCS, 75-86. https://doi.org/10.1007/978-981-19-6414-5_5

Chang C, Kontovas C, Yang Z (2021) Risk assessment of the operations of maritime autonomous surface ships. RESS 207: 107324. https://doi.org/10.1016/j.ress.2020.107324

Chiu S, Provan G, Vasco D (2001) Shipboard system diagnostics & reconfiguration using model-based autonomous cooperative agents. Control Applications in Maritime Systems 34(7): 323-329. https://doi.org/10.1016/S1474-6670(17)35103-0

Corfield G (2023) The Telegraph-Royal Navy contractor forced to pay off cyber criminals. Retrieved from https://www. telegraph. co.uk/business/2023/07/07/royal-navy-contractor-forced-to-pay-offcyber-criminals/ [Accessed on Nov. 7, 2023]

Dittman K, Hansen P, Blanke M (2021) Autonomy for ships: A sovereign agents architecture for reliability and safety by design. SYSTOL, Saint-Raphael, France, 50-57

EclecticIQ Thr`eat Research Team (2023) Multi-year spearphishing campaign targets he maritime industry likely for financial gain. Retrieved from https://securityboulevard.com/2023/03/multi-year spearphishing-campaign-targets-the-maritime-industry-likely-for financial-gain/ [Accessed on Oct. 1, 2023]

Ehlers T, Portier M, Thoma D (2022) Automation of maritime shipping for more safety and environmental protection. AT Automatisierungstechnik 70(5): 406-410. https://doi.org/10.1515/auto-2022-0003

Epikhin A, Modina M (2021) Problems of introducing unmanned vessels on the basis of statistical studies of emergencies and ship losses. Marine Interllectual technologies 3: 77-82. DOI: 10.37220/MIT.2021.53.3.010

Fang Y, Pu J, Liu S (2022) A control strategy of normal motion and self-rescue for autonomous underwater vehicle based on deep reinforcement learning. AIP Advances 1: 12. https://doi.org/10.1063/ 5.0076857

Gkioulos V, Ahmed A (2021) AIS for ship survivability in maritime cyber attacks. Computer Security-ESORICS, 91-119. https://doi.org/10.3390/info13010022

Goud N (2018) Cyber attack on COSCO. Retrieved from https://www.cybersecurity-insiders.com/cyber-attack-on-cosco/ [Accessed on Nov. 3, 2023]

Greenberg A (2017) The untold story of NotPetya, the most devastating cyberattack in history. Retrieved from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed the-world/ [Accessed on Oct. 22, 2023]

Greiman V (2019) Navigating the cyber sea: dangerous atolls ahead. 14th ICCWS, Reading, UK, 87-93

Hopcraft R, Harish A, Jones K (2023) Raising the standard of maritime voyage data recorder security. Journal of Marine Science and Engineering 11(2): 267. https://doi.org/10.3390/jmse11020267

Issa M, Ilinca A, Rizk P (2022) Maritime autonomous surface ships: Problems and challenges facing the regulatory process. Sustainability 14(23): 15630. https://doi.org/10.3390/su142315630

Jung B, Moon S, Shin Y (2022a) Development of autonomous recovery system for pipeline of naval ships by using a multistage control algorithm. Transactions on Mechatronics 27(2): 1150-1161. DOI: 10.1109/TMECH.2021.3082631

Jung J, Lee Y, Yeu T (2022b) Multi-Modal sonar mapping of offshore cable lines with an autonomous surface vehicle. Journal of Marine Science and Engineering 10(3). https://doi.org/10.3390/jmse10030361

Kardakova M, Shipunov I, Knysh T (2020) Cyber security on sea transport. RESS 982: 481-490. DOI: 10.1007/978-3-030-19756-8_46

Kavallieratos G, Diamantopoulou V, Katsikas S (2020a) Shipping 0; Security requirements for the cyber-enabled ship. IEEE Transactions on Industrial Informatics 16(10): 6617-6625. DOI: 10.1109/TII.2020.2976840

Kavallieratos G, Katsikas S, Gkioulos V (2019) Cyber-attacks against the autonomous ship. Computer Security 11387: 276-230. https://doi.org/10.1007/978-3-030-12786-2_2

Kavallieratos G, Katsikas S, Gkioulos V (2020b) Modelling shipping 0; A reference architecture for the cyber-enabled ship. ACIIDS Phuket, 202-217. DOI: 10.1109/TII.2020.2976840

Kavallieratos G, Spathoulas G, Katsikas S (2021) Cyber risk propagation and optimal selection of cybersecurity for complex cyberphysical systems. SENSORS 21(5): 1691. https://doi.org/3390/s21051691

Kayisoglu G, Bolat P, Tam K (2024) A novel application of the CORAS framework for ensuring cyber hygiene on shipboard RADAR. The Journal of Marine Engineering and Technology 23(2): 67-81. DOI: 10.1080/20464177.2023.2292782

Li J, Yu X (2020) Robust saturated tracking control of an autonomous surface vehicle. CCDC, Hefei, China, 3472-3477

Liberati A, Altman DG, Tetzlaff J, Mulrow C, Gøtzsche PC, Ioannidis JPA, Clarke M, Devereaux PJ, Kleijnen J, Moher D (2009) The PRISMA statement for reporting systematic reviews and meta analyses of studies that evaluate health care interventions: explain and elaboration. The Journal of Clinical Epidemiology 62(10): 1-34. https://doi.org/10.1136/bmj.b2700

Liou J (2011) AUV hydrodynamics for survivability and controllability. MTS/IEEE OCEANS Conference, Paris, France, 1-9. DOI: 23919/OCEANS.2011.6107155

Livelli K, Smith R, Gross J (2020) Operation Shaheen. Cylance, Irvine, California, USA, 1-32

Loukas GK (2019) A taxonomy and survey of cyber physical intrusion detection approaches for vehicles. AD HOC Networks 84: 124-147. https://doi.org/10.1016/j.adhoc.2018.10.00

Manuel R (2023) The Defense Post. Retrieved from https://www.thedefensepost.com/2023/07/18/uk-drone-swarm-operation-seebyte/ [Accessed on Jul. 18, 2023]

Martelli M, Cassara P, Tonellotto N (2020) The internet of ships. ERCIM NEWS, 17-18. Available from https://hdl.handle.net/11568/1114393 [Accessed on Oct. 20, 2020]

Martelli M, Russo E, Merlo A, Zaccone R (2024) Adversarial waypoint injection attacks on Maritime Autonomous Surface Ships (MASS) collision avoidance systems. The Journal of Marine Engineering and Technology, 1-12. DOI: 10.1080/20464177.2023.2298521

Martelli M, Virdis A, Di Summa, M. (2021) An outlook on the future marine traffic management system for autonomous ships. IEEE Access 9: 157316-157328. DOI: 10.1109/ACCESS.2021. 3130741

Mascellino A (2023) Fata morgana watering hole attack targets shipping, logistics firms. Retrieved from https://www.infosecuritymagazine.com/news/fata-morgana-watering-hole-attacks/ [Accessed on May 23, 2023]

McGillivary P (2018) Why maritime cybersecurity is an ocean policy priority and how it can be addressed. Marine Technology Society Journal 52(5): 44-57. DOI: 10.4031/MTSJ.52.5.11

Meland P, Bernsmed K, Nesheim D (2021) A retrospective analysis of maritime cyber security incidents. Trans-nav-international Journal on Maritime Navigation and Safety of Sea Transportation 15(3): 519-530. DOI: 10.12716/1001.15.03.04

Mission Secure (2023) Mission secure-maritime security. Retrieved from https://www.missionsecure.com/maritime-security-perspectivesfor-a-comprehensive-approach [Accessed on Nov. 25, 2023]

Nakhodchi S, Zolfaghari B, Yazdinejad A, Dehghantanha A (2021) SteelEye: An application-layer attack detection and attribution model in industrial control systems using Semi-deep learning. 2021 18th International Conference on Privacy, Security and Trust, 1-8. DOI: 10.1109/PST52912.2021.9647777

National Cyber Security Centre (2023) APT28 exploits known vulnerability to carry out reconnaissance and deploy malware on cisco routers. Retrieved from https://www.ncsc.gov.uk/files/Advisory_APT28-exploits-known-vulnerability.pdf [Accessed on Apr. 13, 2023]

Nicaise V (2021) Cybermaretique: a short history of cyberattacks against ports. Stormshield. Retrieved from https://www.stormshield.com/news/overview-of-cyberattacks-on-connected-cities/ [Accessed on Jul. 2023]

Onishchenko O, Shumilova K, Volianskyi Y (2022) Ensuring cyber resilience of ship information systems. Transnav-international Journal on Marine Navigation and Safety of Sea Transportation 16(1): 43-50. DOI: 10.12716/1001.16.01.04

Park C, Kontovas C (2023) A BN driven FMEA approach to assess maritime cybersecurity risks. Ocean & Coastal Management 235:

106480. https://doi.org/10.1016/j.ocecoaman.2023.106480
Pitropakis N, Logothetis M, Lambrinoudakis C (2020) Towards the creation of a threat intelligence framework for maritime infrastructures. Computer Security Esorics, 53-68. https://doi.org/1007/978-3-030-42048-2_4
Polemi N, Van-Maele C (2023) Cybersecurity in maritime infrastructure. Retrieved from https://rusieurope.eu/wp-content/uploads/2023/06/cybersecurity-in-maritime-critical-infrastructurecrimson-report.pdf [Accessed on Apr. 20, 2023]
Port Technology Team (2022) Major European ports hit by cyber attack. Available from http://www.Porttechnology.com [Accessed on Jul. 3, 2023]
Qiao S, Zheng K, Wang G (2020) A path planning method for autonomous ships based on SVM. Ocean Engineering, 3068-3072. DOI: 10.1109/CCDC49329.2020.9164806
Qiu Y, Li Y, Lang J (2021) An optimal tracking control method for unmanned ship approach. CCDC (33rd): 546-551. DOI: 10.1109/CCDC52312.2021.9602845
Rabieinejad E, Yazdinejad A, Dehghantanha A, Srivastava G (2024) Two-level privacy-preserving framework: federated learning for attack detection in the consumer internet of things. IEEE Transactions on Consumer Electronics, 1. DOI: 10.1109/TCE.2024.3349490
Rabieinejad E, Yazdinejad A, Dehghantanha A, Parizi RM, Srivastava G (2021) Secure AI and blockchain-enabled framework in smart vehicular networks. IEEE Globecom Workshops GC wkshps. Madrid, Spain, 1-6. DOI: 10.1109/GCWkshps52748.2021.9682140
Sahay R, Estay DAS, Meng WZ, Jensen CD, Barfod MB (2023) A comparative risk analysis on CyberShip system with STPA-Sec, STRIDE and CORAS. Computers and Security 128: 117-129: https://doi.org/10.1016/j.cose.2023.103179
Sakhnini J, Karimipour H, Dehghantanha A, Yazdinejad A, Gadekallu T, Victor N (2023) A generalizable deep neural network method for detecting attacks in industrial Cyber-Physical systems. IEEE Systems Journal 17(4): 5152-5160. DOI: 10.1109/JSYST. 2023.3286375
Sepehri A, Vandchali H, Montewka J (2022) The impact of shipping 0 on controlling shipping accidents: A systematic literature review. Ocean Engineering, 243. https://doi.org/10.1016/j.oceaneng.2021.110162
Serru T, Nguyen N, Rauzy A (2023) Modeling cyberattack propagation and impacts on cyber physical system safety: An experiment. Electronics (1): 12. https://doi.org/10.3390/electronics12010077
Shapo V, Levinskyi M (2021) Means of cyber security aspects studying in maritime specialists education. Infrastructures and Mobile Applications 1192: 389-400. DOI: 10.1007/978-3-030-49932-7_38
Shipunov I, Voevodskiy K, Gatchin Y (2019) About the problems of ensuring information security on unmanned ships. EICONRUS, 1-9. DOI:10.1109/EIConRus.2019.8657219
Silva R, Hickert C, Sookoor T (2022) AlphaSOC: reinforcement learning-based cybersecurity automation for cyber-physical systems. ICCPS, 290-291. DOI: 10.1109/ICCPS54341.2022.00036
Silverajan B, Ocak M, Nagel B (2018) Cybersecurity attacks and defences for unmanned smart ships. IEEE ICC, 15-20. DOI: 1109/Cybermatics_2018.2018.00037
Solnor P, Volden O, Fossen T (2022) Hijacking of unmanned surface vehicles: A demonstration of attacks and countermeasures in the field. Journal of Field Robotics 39(5): 631-649. https://doi.org/1002/rob.22068
Symes SW, Fairclough S, Wang J, Yang Z, Blanco-Davis E (2022) Simulator based human performnace assessment in a ship engine room using functional near-infrared spectroscopy. Liverpool John Moores University, Liverpool, 29303124
Talos C (2018) DNS hijacking abuses trust in core internet service. Available from http://www. CiscoTalosIntelligence.com [Accessed on Jul. 5, 2023]
Tam K, Jones K (2018) Cyber-risk assessment for autonomous ships. International Conference on Cyber Security and Protection of Digital Services, Scotland, 1-8. https://doi.org/10.1109/CyberSecurity43720.2018
The International Maritime Organisation (IMO) (2019) Imo. org. Retrieved from https://www.imo.org/en/OurWork/Security/Pages/Cyber-security. aspx#: ~: text=Maritime%20cyber% 20risk20refers%20to, being%20corrupted%2C%20lost%20or%20compromised [Accessed on Oct. 10, 2023]
Tidy J (2023) BBC news-technology. Retrieved from https://www.bbc.co.uk/news/technology-66998064 [Accessed on Oct. 4, 2023]
Titov A, Barakat L, Kovalev O (2019) Risk assessment of operating unmanned ships. Marine Intellectual Technologies 4(4): 11-23. DOI: 10.17586/2226-1494-2021-21-1-73-84
Turner J (2018) Sea hunter: inside the US navy's autonomous submarine tracking vessel. Retrieved from https://www.navaltechnology.com/features/sea-hunter-inside-us-navys-autonomoussubmarine-tracking-vessel/ [Accessed on Nov. 3, 2023]
Tusher H, Munim Z, Nazir S (2022) Cyber security risk assessment in autonomous shipping. Maritime Economics and Logistics 24(2): 208-227. https://doi.org/10.1057/s41278-022-00214-0
Vagale A (2022) Evaluation simulator platform for extended collision risk of autonomous surface vehicles. Journal of Marine Science and Engineering 10(5): 14-17. DOI: 10.3390/jmse10050705
Vagale A, Bye R, Fossen T (2021) Path planning for autonomous surface vehicles II: a comparative study of algorithms. Journal of Marine Science and Technology 26(4): 1307-1323. https://doi.org/10.1007/s00773-020-00790-x
Yazdinejad A, Dehghantanha A, Parizi R, Hammoudeh M, Karimipour H, Srivastava G (2022) Block hunter: federated learning for cyber threat hunting in blockchain-based IIoT networks. IEEE Transactions on Industrial Informatics 18(11): 8356-8366. DOI: 10.1109/TII.2022.3168011
Yazdinejad A, Dehghantanha A, Parizi R, Srivastava G, Karimipour H (2023) Secure intelligent fuzzy blockchain framework: Effective threat detection in IoT networks. Computers in Industry, 144. DOI: 1016/j.compind.2022.103801
Yazdinejad A, Parizi RM, Srivastava G, Dehghantanha A, Choo K KR (2019) Energy efficient decentralized authentication in internet of underwater things using blockchain. IEEE Globecom Workshops GC Wkshps, Waikoloa, USA, 1-6. DOI: 10.1109/GCWkshps45667.2019.9024475
Yoo J, Jo Y (2023) Formulating cybersecurity requirements for autonomous ships using SQUARE methodology. SENSORS 11(1): 23. DOI: 10.3390/s23115033
Yoo Y, Park H (2021) Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ships. Journal of Marine Science and Engineering, 9. https://doi.org/10.3390/jmse9060565
Zhou X, Liu Z, Ni S (2018) Collision risk identification of autonomous ships based on the synergy ship domain. CCDC, Beijing, China, 6746-7652
Zhou X, Liu Z, Wu Z (2021) A system-theoretic approach to safety and security co-analysis of autonomous ships. Ocean Engineering 222: 108569. https://doi.org/10.1016/j.oceaneng.2021.108569