Cyber-attacks on the maritime sector: a literature review

Dr Steve Symes[a] Dr Eddie Blanco-Davis[a], Professor Tony Graham[a], Professor Jin Wang[a], Dr Edward Shaw[a]

a. School of Maritime Engineering and Technology, Liverpool Logistics Offshore and Marine Research Institute (LOOM), Faculty of Engineering and Technology, Liverpool John Moores University, L3 3AF.

Email Addresses: S.W.Symes@ljmu.ac.uk **(Steve Symes),** E.E.BlancoDavis@ljmu.ac.uk **(Eddie Blanco-Davis),** A.R.Graham@ljmu.ac.uk **(Tony Graham),** J.Wang@ljmu.ac.uk **(Jin Wang),** e.j.shaw@ljmu.ac.uk **(Edward Shaw).**

Abstract

This study is an investigation into cyber attacks on automated vessels, focussing on previous 'real-world' cyber-attacks and their consequences. The future of commercial and non-commercial shipping seems to be moving towards automated vessels. Autonomous ships can provide significant financial and logistical benefits for shipping companies and their stakeholders, but these vessels suffer from shortcomings with respect to cyber security. Previous cyber-attacks are investigated for the purpose of understanding how an autonomous ship's command system is infiltrated, the consequences of an attack, and the shortfalls of the vessels security. This aim is achieved via a literature review concerning cyber-attacks on autonomous vessels with a focus on sources indicating how previous vessels' security systems were breached, the consequences of said cyber-attacks, 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 automated vessels are significantly vulnerable to cyberattacks. Automated vessels were found to have relatively easy to breach security systems. In most cases, the consequences of a cyber-attack had a negative financial impact, a loss of cargo, and a potential breach of oceanic airspace, resulting in military action. The vessels analysed 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 may indicate to the transport industry' gaps in the market' with respect to the security of autonomous vessels and viable recovery procedures.

Keywords: Automated Vessels, Cyber security, Survivability, Artificial Intelligence (A.I.), Hacking.

1. Introduction

In recent years, the maritime industry has witnessed a monumental shift with the emergence of autonomous ships [1]. These revolutionary vessels, equipped with cutting-edge technology and artificial intelligence, promise increased efficiency, reduced costs, and improved safety [2]. However, as the world embraces this transformative technology, a concerning issue looms on the horizon: the threat of cyber-attacks against accessible high-tech technologies implemented by the maritime sector [3]. This paper delves into the intricacies of this emerging challenge, exploring the potential vulnerabilities and consequences that cyber-attacks could pose.

The Rise of Autonomous Ships: autonomous ships have rapidly gained traction as a viable solution for various maritime operations. By implementing advanced sensors, machine learning algorithms, and real-time data analysis, these vessels have the potential to revolutionise the industry [4] **[5] [6]**. They potentially reduce human error, increase navigational accuracy, and enhance operational efficiencies. However, with increased reliance on technology comes the inherent risk of cyber-attacks [5].

Understanding Cyber-Attacks: cyber-attacks 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 unauthorised access to sensitive information or disrupt critical operations [6]. These attacks can take many forms, including malware infections, phishing attempts, Denial-of-Service (DoS) attacks, and ransomware campaigns [7].

Vulnerabilities in shipping: despite their advanced technological systems, new high-tech and autonomous ships are not immune to cyber threats [8]. Their vulnerability derives from their interconnectedness and reliance on complex software and hardware components [9]. These vulnerabilities can arise from inadequate cybersecurity measures,

insecure communication protocols, outdated software, or even human error during the design and implementation phases [10]. The potential consequences of cyber-attacks against the maritime sector and autonomous ships are far-reaching and alarming [11].

Consequences of Cyber Attacks on the maritime sector: the consequences of successful cyber-attacks on the maritime sector can be catastrophic [2]. They can range from financial losses due to disrupted operations and compromised cargo, to compromised safety and environmental risks [3]. For instance, a hacker gaining control of an autonomous ship's navigation system could redirect it towards hazardous areas, leading to collisions or oil spills as acts of terrorism [10]. Moreover, cyber-attacks can undermine public trust in automation, slowing [12].

Section 2 involves a review of previous cyber-attack techniques and protection models used in the maritime sector. This review aims to improve understanding of how the security of a vessel is breeched, in order to determine mitigation measures. Moreover, the consequences of cyber-attacks on the maritime sector will be evaluated to substantiate the benefit of investment to solve this problem. Additionally, the recovery processes will be evaluated to identify any shortcomings of current procedures.

2. Literature review

The scope of the literature review involves recent case studies of cyber-attacks on the maritime sector, new technology related to and including autonomous vessels, and their vulnerability to cyber-attacks. The literature will be sourced from Web of Science, *SciFinder, Scopus, Mandeley, Zotero, Google Scholar and various newspaper articles.*

The keywords or phrases used in the literature search were: Automated vessels, cyber-attack, threats to safety, Hacking, automated vessel security, maritime cyber security, cyber-attack techniques, and cyber-attack prevention.

The purpose of the literature review scope is to answer the following research questions:

1. What cyber-attacks have happened previously, and what techniques were used?
2. What was the impact and consequence of each identified cyber-attack?
3. What options are available to mitigate the risk of a cyber-attack and what are their shortcomings?

A preliminary literature search indicated that the literature detailing cyber-attacks on autonomous ships is currently scarce due to the early stages of this type of vessel's implementation. Therefore, this literature review primarily investigates cyber-attacks 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 cyber-attacks on shipping companies and non-autonomous vessels will be conducted similarly against autonomous ships [1]. The main difference is the potential consequences, as an autonomous vessel will likely be unmanned [4].

The literature search resulted in the identification of 6 different techniques used in most of the cyber-attacks to infiltrate a ship's security system.

2.1 Phishing

Phishing refers to a type of cyber threat that targets individuals or organisations [14]. It involves an attacker's attempt to manipulate human victims into revealing sensitive information, such as login credentials or financial data [15].

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 [16]. 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 hackers access to sensitive information or systems [17]. A common cycle for phishing attacks is illustrated in Figure 1.

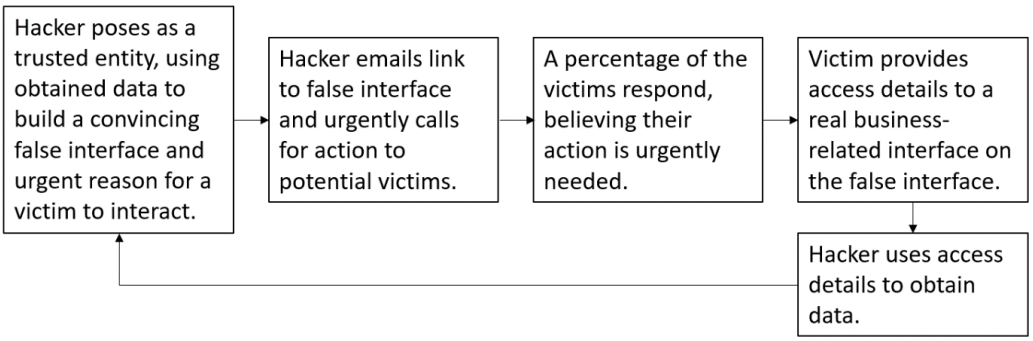

Figure 1. Phishing attack cycle

Significant examples of successful phishing cyber-attacks include: the China Ocean shipping company in July 2018 [13], the DNV (Norwegian software supplier) [18], and the CMA CGM in 2021 [19]. The attack on the DNV alone resulted in the disabling of their systems for weeks, 70 companies and over 1000 vessels were affected [18]. The 'Ragnor Locke' ransomware attack on CMA CGM resulted in their systems being down for days, costing the company 8 million US dollars [19].

Currently, the only guidelines for the maritime sector to protect against phishing attacks are calls to be vigilant and follow best practices [8]. This includes 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 [20]. Additionally, maritime enterprises should prioritise employee training and awareness programs to help recognise and report potential phishing attempts [21]. While the protection techniques mentioned above are effective in mitigating phishing attacks, they do have some potential shortcomings:

1. 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 [10].

2. Evolving Techniques: cybercriminals continuously adapt their phishing techniques to bypass security measures and exploit new vulnerabilities [4]. 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 [2].

3. Insider Threats: protection techniques primarily focus on external threats, but insider threats can also pose risks. Malicious insiders who have authorised access to systems may attempt phishing attacks or inadvertently compromise sensitive information [15].

4. Lack of Standardisation: the maritime industry is vast and diverse, making it challenging to establish standardised security practices across all organisations. This lack of uniformity can create inconsistencies in implementing and enforcing phishing protection techniques [17].

5. Advanced Phishing Methods: phishing attacks are becoming increasingly sophisticated, employing techniques like spear phishing or whaling, specifically targeting high-level executives or individuals with privileged access. Such targeted attacks can be challenging to detect and mitigate [16].

2.2 Malware

Malware, in the context of maritime cyber-attacks, refers to malicious software designed to disrupt, damage, or gain unauthorised access to computer systems and networks within the maritime industry [21]. It is a broad term encompassing various types of harmful software, such as: viruses, worms, trojans, ransomware, and spyware [22].

In maritime cyber-attacks, malware can be introduced into 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 unauthorised access to attackers [23]. Common types of malware include:

- Ransomware: software that leverages data or access to software until the hacker's demands are satisfied.
- Spyware: software that monitors other software for data (and in some instances the victim through an integrated camera) without the victim's awareness.
- Adware: software that sends its victims adverts, often leading to false product or service interfaces inviting its victim to provide payment details.
- Worms: software that spreads automatically through a computer's files, or to other computers within a network.
- Trojans: named after the Trojan Horse, it is software that appears to be a trusted file, often spread via malicious emails.
- Botnets: software that connects a victim's computer to a hackers' network, preventing the victim from using the infected computer.

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, it can compromise critical navigation, communication, or control systems, jeopardising the safety of a vessel, and its crew and cargo [24].

In 2017, the "Sea Hunter," an unmanned vessel developed by the Defence Advanced Research Projects Agency (DARPA) in the United States, was cyber-attacked using malware. In this incident, security researchers from the cybersecurity firm Fortinet employed malware to exploit weak default passwords and take advantage of unpatched software vulnerabilities [25] . In 2017, a cyber-attack on the Maersk shipping company was a significant event that drew attention to the potential vulnerabilities in the shipping industry's cybersecurity. The attack involved the NotPetya malware, which spread rapidly across computer systems worldwide, affecting various port-related industries [26]. In July 2018, the China Ocean Shipping Company (COSCO) Group, one of the world's largest shipping companies, also experienced a significant NotPetya cyber-attack that impacted its operations globally [27].

As a result of the above attacks, COSCO was forced to shut down some of its critical systems, including its website, email servers, and certain operational systems [27], Sea Hunter was left 'dead in the water' [25], and the Maersk shipping company systems were non-operating for weeks. The cumulative cost of these attacks is approximately 200 million US dollars [26]. In April 2020, a Mediterranean shipping company also experienced a Malware attack resulting in its systems having to be resettled, resulting in multiple days of delay in operations [28].

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

1. Antivirus and Anti-Malware Software: deploying robust and up-to-date antivirus and anti-malware solutions to detect, block, and remove malicious software [29].
2. Regular System Updates and Patching: ensuring that all operating systems and software applications are regularly updated with the latest security patches and updates to address vulnerabilities that malware may exploit [30].
3. Employee Education and Awareness: training employees on best practices to avoid malware, such as not opening suspicious email attachments or clicking on unknown links. Encouraging a culture of cybersecurity awareness throughout the enterprise [29].
4. Network Firewalls and Intrusion Detection Systems: implementing network firewalls and intrusion detection systems to monitor and block unauthorised access attempts and suspicious network activity [24].

5. Secure Configuration and Access Control: configuring systems securely by following industry best practices and limiting access privileges to authorised personnel only. This helps prevent unauthorised installation or execution of malware [31].

6. Regular Data Backups: maintaining regular backups of critical data and systems to mitigate the impact of any malware attack. Ensure backups are stored securely and can be readily restored if needed [32].

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

1. Antivirus and Anti-Malware Software: while antivirus and anti-malware 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 [33].

2. Regular System Updates and Patching: while 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 [34].

3. Employee Education and Awareness: human error remains a significant challenge, even with robust training programs. Employees may still fall victim to sophisticated phishing techniques or inadvertently compromise security through unintentional actions, such as clicking on malicious links or providing sensitive information [35].

4. Network Firewalls and Intrusion Detection Systems: while firewalls and intrusion detection systems provide valuable protection, they may not always detect zero-day attacks or advanced persistent threats that utilise sophisticated evasion techniques [36].

5. Secure Configuration and Access Control: if access controls and configurations are not implemented correctly, attackers may exploit misconfigurations or gain unauthorised access to critical systems. Regular monitoring and auditing of access controls are necessary to ensure that secure configurations and access controls are effectively maintained [37].

6. Regular Data Backups: while regular data backups are essential, it is important to ensure that backups are 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 [38].

2.3 Denial of Service

DoS, in the context of maritime cyber-attacks, refers to a type of cyber-attack that disrupts or disables the availability of critical systems or networks within the maritime industry [39]. A DoS attack overwhelms targeted systems with a flood of illegitimate traffic or resource requests, rendering them unable to function correctly [40].

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 or shore, or even cause safety risks [39].

There are two primary forms of DoS attacks:

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 network's resources, leading to service degradation or complete unavailability [40].

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 organised groups with malicious intent, including hacktivists, competitors, or state-

sponsored actors. These attacks can be challenging to mitigate, as they often involve high volumes of traffic from multiple sources, making it difficult to distinguish legitimate requests from malicious ones [41].

In 2017, the port of Antwerp, one of Europe's largest ports, experienced a cyber-attack that disrupted its container operations. While exact details of the attack are not disclosed, it was reported that it involved a DoS component that impacted the ports IT systems, leading to operational disruptions [42].

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

1. Network Traffic Monitoring: deploying network monitoring tools to detect abnormal or suspicious traffic patterns indicating a potential DoS attack. This allows for early detection and mitigation efforts [43].

2. Load Balancers and Traffic Shaping: implementing load balancers and traffic shaping mechanisms to distribute network traffic evenly across systems, preventing overload and ensuring the availability of critical services during high-traffic periods [44].

3. Redundancy and Failover Systems: designing systems with redundant components and failover capabilities to ensure critical services and systems remain operational even if one component comes under a DoS attack [45].

4. Intrusion Detection and Prevention Systems (IDS/IPS): utilising IDS/IPS systems to detect and block malicious traffic or requests in real-time, preventing them from reaching targeted systems [46].

5. Collaborative Defence: engaging in information sharing and collaboration with industry partners, security organisations, and government agencies to exchange threat intelligence and best practices for DoS mitigation. By sharing information about emerging threats and implementing coordinated defence strategies, the maritime industry can enhance its resilience against DoS attacks [47].

6. Incident Response Planning: developing and regularly testing incident response plans to ensure a swift and coordinated response during a DoS attack. This last includes predefined procedures for isolating affected systems, implementing countermeasures, and restoring services to minimise disruption [48].

While the mentioned 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:

1. Scalability and Bandwidth: maritime systems often span large geographical areas, requiring significant bandwidth for communication and data exchange. DoS attacks targeting these systems can generate massive amounts of traffic that may overwhelm network resources, making it challenging to scale up infrastructure to handle such high volumes [49].

2. Zero-Day Attacks: DoS attacks can utilise new and previously unknown vulnerabilities or exploit weaknesses in specific maritime applications or systems. Traditional defence mechanisms may struggle to detect and mitigate these zero-day attacks, as there may not be known signatures or patterns to identify them [48].

3. 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 [45].

4. 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 [50].

5. Resource-intensive Defence Measures: implementing robust DoS protection measures can require significant resources, such as investment in advanced hardware, software, and expertise. Maritime enterprises, especially smaller ones, may face challenges implementing and maintaining these defence measures due to resource constraints [51].

6. Insider Threats: while external DoS attacks are common, insider threats within the maritime industry cannot be overlooked. Malicious insiders who have authorised access to critical systems may launch DoS attacks, making detection and prevention more challenging [50].

2.4 Man in the middle.

In maritime cyber-attacks, the term "Man in the Middle" (MITM) refers to an attack where an unauthorised entity intercepts and potentially alters communication between two legitimate parties without their knowledge. The attacker positions themselves between the sender and recipient, intercepting.

In a maritime setting, a MITM attack occurs when an attacker gains unauthorised access to the communication channels or systems used for exchanging information between vessels, ports, or 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 [53].

A 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 unauthorised locations. Similarly, intercepting communication between shipping companies and ports could result in cargo misdirection or unauthorised access to sensitive information [54]. An MITM attack is illustrated in Figure 2.

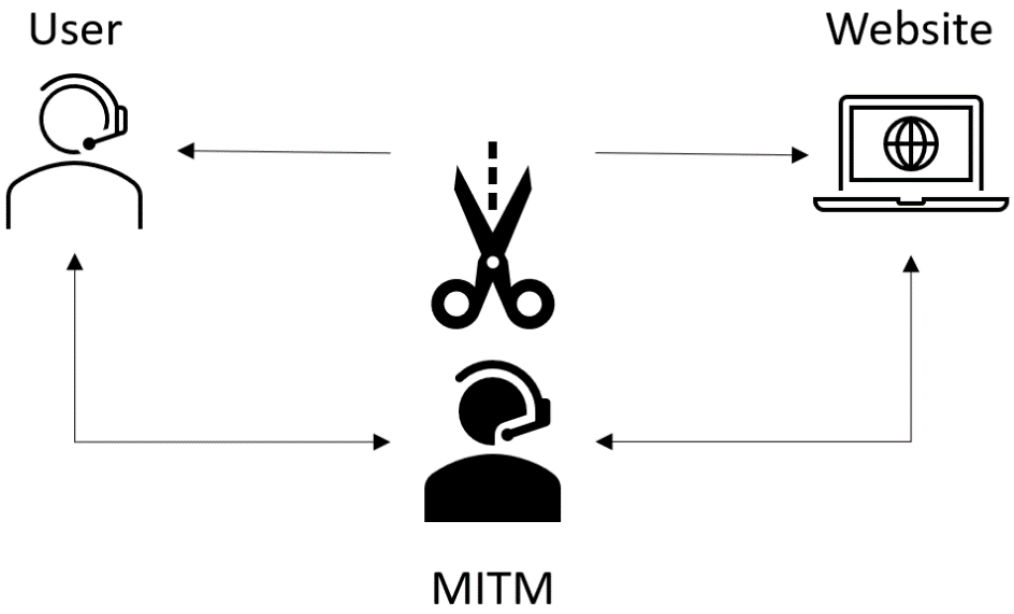

Figure 2 MITM attack

APT28 (Fancy Bear): A cyber espionage group known as APT28, or Fancy Bear, has been linked to several cyber-attacks targeting shipping and maritime companies. Their tactics include MITM attacks.

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 [55].

Operation Shaheen: in 2020, a threat group known as Operation Shaheen targeted shipping companies with MITM attacks. They compromised the companies' email servers, allowing them to intercept and modify email communications, potentially leading to financial fraud or cargo diversion [56].

The Sea Turtle cyber-attack, discovered in 2018, was a highly sophisticated and targeted operation that focused on infiltrating maritime and telecom organisations mainly in the Middle East and North Africa. The attackers employed a technique known as DNS hijacking. They gained access to the targeted enterprises' DNS registrars 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. This last allowed them to intercept and monitor sensitive information, such as emails, login credentials, and other communication data passing through the compromised networks [57].

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

1. Secure Communication Channels: implementing secure communication protocols, such as encrypted connections using secure sockets layer/transport layer security (SSL/TLS), helps prevent unauthorised interception and manipulation of data during transmission [53].

2. Strong authentication and access controls implementing robust authentication mechanisms, such as multi-factor authentication and secure access controls, help ensure that only authorised parties can access and exchange information, reducing the risk of MITM attacks [54].

3. Certificate-based Encryption: utilising digital certificates for encryption and authentication can enhance the security of communication channels, making it harder for attackers to impersonate legitimate entities and conduct MITM attacks [58].

4. Network Monitoring: continuous monitoring of network traffic and analysis of communication patterns can help detect any suspicious activities or anomalies that may indicate the presence of an MITM attack. Real-time monitoring enables swift response and mitigation efforts [59].

5. 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 [60].

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

1. Insider Threats: MITM attacks can be challenging to detect when perpetrated by individuals authorised 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 [58].

2. 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 [54].

3. 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. This last can enable attackers to access communication channels and carry out MITM attacks [59].

4. Interoperability Challenges: the maritime industry involves various stakeholders, each using their own 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 [60].

5. 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 [61].

6. Remote and Maritime Connectivity: maritime operations often occur in remote and challenging environments with limited connectivity options. This can make implementing real-time monitoring and response mechanisms difficult, leaving a window of opportunity for MITM attacks to go undetected or unmitigated [59].

2.5 Social engineering

Social engineering in the context of the maritime industry refers to a cyber-attack technique where attackers exploit human psychology to manipulate individuals within the sector into divulging sensitive information or performing actions that compromise security [62].

Phishing is a type of social engineering attack that typically targets its victims through emails. The attackers pose as a trusted source like a colleague, client, or even someone from a regulatory authority [61]. The message could ask the recipient to provide confidential information, such as login credentials, financial details, or ship-related data [63].

To make the attack more convincing, the attackers might research the maritime industry to personalise their messages and increase the likelihood of success. For example, they could mention specific vessels, recent regulatory changes, or industry-specific jargon to gain the target's trust [64].

If an unsuspecting employee falls for the phishing attempt and shares the requested information, the attackers can gain unauthorised access to critical systems, compromise sensitive data, or even cause disruptions to maritime operations [65].

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

1. Employee Education: conduct regular cybersecurity training programs to educate employees about social engineering techniques, phishing emails, and other common attack vectors. This will help them recognise potential threats and avoid falling victim to scams [66].

2. Strong Passwords: encourage employees to create strong, unique passwords for all their accounts and systems. Implement multi-factor authentication (MFA) wherever possible to add an extra layer of security [67].

3. Email Filtering: implement robust email filtering systems that can identify and block malicious emails, minimising the chances of phishing messages reaching employees' inboxes [66].

4. Policy and Procedures: establish clear security policies and procedures related to handling sensitive information, including guidelines on how to verify identities, report suspicious emails, and manage data securely [68].

5. Regular Updates and Patches: keep all software, applications, and operating systems updated with the latest security patches. This helps protect against known vulnerabilities that attackers may exploit [66].

6. Incident Response Plan: develop an incident response plan specific to social engineering attacks. 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 [69].

7. Security Awareness Culture: foster a security-aware culture within the maritime industry by promoting a mindset of constant vigilance. Encourage open communication among employees so they feel comfortable reporting suspicious activities or potential security breaches [66].

8. Regular Security Assessments: conduct periodic security assessments and penetration testing to identify vulnerabilities and address them proactively. This will help identify any weaknesses in systems, processes, or employee knowledge that could be exploited in social engineering attacks [67].

9. Verify Requests: encourage employees to verify requests for sensitive information, especially if they seem unusual or out of the ordinary. This can be done by contacting the supposed sender through a different channel (e.g., a phone call) to confirm the request's legitimacy [69].

10. Keep up with Industry Updates: stay informed about the latest trends and tactics in social engineering attacks within the maritime industry. This will help adapt security measures and stay one step ahead of potential threats [70].

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

1. Human Error: despite education and training, employees can still make mistakes and fall for social engineering tactics. It is challenging to eliminate human error, as attackers continuously evolve their techniques to exploit psychological vulnerabilities [71].

2. Advanced Attacks: highly sophisticated social engineering attacks may bypass traditional email filters and security measures, making them harder to detect. Attackers may employ advanced tactics like spear phishing, which targets specific individuals or groups, making it more difficult to identify and prevent [72].

3. Lack of Awareness: some employees may not pay sufficient attention or take cybersecurity seriously even with regular training. This can lead to complacency and increase the risk of falling victim to social engineering attacks [71].

4. 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 [66].

5. 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 [68].

6. False Sense of Security: relying solely on technological solutions and security measures may create a false sense of security. While implementing strong technical controls is important, it is equally crucial to foster a culture of security awareness, empowering employees to participate actively in maintaining a secure environment [67].

7. Resource Constraints: small maritime enterprises or those with limited budgets may face challenges implementing all the recommended security measures. It is important to prioritise based on risk assessments and allocate resources effectively to address the most critical vulnerabilities [70].

8. Lack of Standardisation: the maritime industry comprises various organisations and stakeholders with different levels of cybersecurity maturity. The absence of standardised security practices and regulations can create inconsistencies in implementing effective social engineering prevention strategies [69].

A few examples of social engineering cyber-attacks targeting the maritime industry a detailed below:

1. "Business Email Compromise" (BEC) Attack: in 2019, a maritime shipping company fell victim to a BEC attack. Attackers impersonated the CEO and sent emails to the company's finance department 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 [73].

2. "Spear Phishing" Attack on Port Operations: in 2023, a spear phishing attack targeted a major port. Hackers sent customised 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 allowed attackers access to internal networks, disrupting port operations and causing delays in cargo handling [74].

3. "Watering Hole" Attack on Vessel Operations: in 2023, attackers compromised a maritime shipping company's website that crew members frequently visited. The attackers injected malicious code into the website, which exploited vulnerabilities in crew members' browsers when they accessed the compromised site. This allowed the attackers to gain unauthorised access to vessel systems, compromising critical shipboard systems and potentially enabling them to manipulate navigation controls or access sensitive information [75].

4. "Phishing" Attack on Port Authority: in 2020, a port authority experienced a phishing attack targeting its employees. 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 unauthorised access to the port's systems and sensitive data [76].

Each of the attacks mentioned above had severe consequences to the companies themselves and the maritime sector. Details of these consequences are outlined below:

1. Business Email Compromise" (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 company's financial stability and damaged its reputation and customer trust [73].

2. "Spear Phishing" Attack on Port Operations: the spear phishing attack on the major port caused disruptions in its operations. The malware installed through the malicious emails allowed attackers to gain unauthorised access to the port's internal networks. This led to delays in cargo handling, potentially impacting supply chains, customer satisfaction, and financial losses for both the port and associated businesses [74].

3. "Watering Hole" Attack on Vessel Operations: the compromise of the maritime shipping company's website led to unauthorised access to vessel systems. This puts vessel operations at risk, as 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 [75].

4. "Phishing" Attack on Port Authority: the phishing attack on the port authority resulted in unauthorised access to the port's systems and sensitive data. The attackers could exploit 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 [76].

2.6 Physical attacks

Physical cyber-attacks in the maritime industry involve exploiting physical assets, systems, or infrastructure to launch or facilitate cyber-attacks [36]. These attacks' blur the lines' between physical security and cybersecurity, leveraging vulnerabilities in both realms. Here are a few examples of physical cyber-attacks in the maritime industry:

1. Unauthorised 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, they can disrupt operations, steal data, or plant malicious code [37].

2. 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 unauthorised access or control over the compromised systems [38].

3. Supply Chain Attacks: attackers exploit weaknesses in the maritime industry's supply chain by tampering with physical components or systems before they are deployed. This includes 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 cyber-attacks [37].

4. Physical Infrastructure Tampering: attackers physically manipulate or sabotage physical infrastructure elements within the maritime industry to cause disruption or enable cyber-attacks. This can involve 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 [38].

Physical cyber-attacks 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 cyber-attacks, there are some protection measures detailed below:

1. Physical Access Controls: implement strong access controls to restrict physical access to critical infrastructure, ships, and sensitive areas. This includes employing surveillance systems, secure fencing, access cards, biometric authentication, and visitor management protocols [6].

2. Employee Awareness and Training: educate employees about the risks of physical cyber-attacks and the importance of following security protocols. Train them to recognise suspicious behaviours, report potential vulnerabilities, and adhere to access control procedures [58].

3. Secure Supply Chain: establish secure supply chain practices by verifying the integrity of components and systems before deployment. Regularly assess suppliers' cybersecurity practices and perform thorough risk assessments to ensure the absence of compromised or tampered components [36].

4. Cybersecurity Measures: implement robust cybersecurity measures to protect systems from both physical and cyber threats. This includes network segmentation, firewalls, intrusion detection systems, antivirus software, regular patch management, and encryption of sensitive data [38].

5. Incident Response Planning: develop a comprehensive incident response plan that addresses physical and cyber-attacks. Include protocols for identifying, containing, and mitigating the impact of a physical cyber-attack. Regularly rehearse and update the plan to ensure it remains effective and aligns with emerging threats [20].

6. Physical Security Audits: conduct regular physical security audits to identify vulnerabilities and gaps in security measures. This includes assessing physical access controls, surveillance systems, alarm systems, and other physical security mechanisms. Address any identified weaknesses promptly [36].

7. Employee Background Checks: implement thorough background checks for employees and contractors with access to critical systems and infrastructure. This helps mitigate the risk of insider threats or individuals with malicious intent gaining physical access [38].

8. Incident Reporting and Information Sharing: establish a culture of reporting and information sharing within the maritime industry. Encourage employees and enterprises to report suspicious activities, physical breaches, or attempted cyber-attacks. Collaborate with industry peers, authorities, and cybersecurity organisations to share threat intelligence and best practices [36].

9. Continual Improvement: regularly evaluate and update security measures based on emerging threats, industry best practices, and lessons learned from incidents. Stay informed about evolving physical and cyber-attack techniques and adapt security strategies accordingly [9].

While the aforementioned protection methods are effective in mitigating physical cyber-attacks in the maritime industry, it is essential to be aware of their potential shortcomings:

1. Human Error: a common and repetitive occurrence throughout the differing cyber security 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 [5].

2. Insider Threats: protection methods may not eliminate the risk of insider threats. Employees or contractors with authorised access to critical infrastructure can intentionally or unintentionally engage in malicious activities that bypass physical and cybersecurity measures [9].

3. 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 cyber-attacks [36].

4. Budget Limitations: implementing 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 [38].

5. Lack of Standardisation: the absence of standardised security practices and regulations in the maritime industry can lead to inconsistencies in implementing protection methods. This lack of standardisation can create gaps in security coverage and make it challenging to address threats uniformly across the industry [7].

6. Complexity and Integration: protecting against physical cyber-attacks 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 [6].

7. Response and Recovery: while 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 cyber-attack and exacerbate the associated damages [37].

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

1. Physical Infrastructure Tampering: in one instance in 2019, attackers gained unauthorised physical access to MV COSCO's port facility and tampered with the communication systems and navigation equipment. This resulted 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 port's reputation [77].

2. Unauthorised Vessel Access: in May 2022 attackers managed to gain unauthorised access to the commercial vessel Nippon Maru and physically connected a device to its onboard systems. This allowed them to manipulate the vessel's navigation controls, potentially endangering the crew and jeopardising the vessel’s safety. The consequences included compromised vessel operations, potential accidents, and the need for extensive remediation efforts to mitigate the impact [77].

3. Supply Chain Compromise: in a supply chain attack to Mediterranean shipping company (MSC) 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 attackers to manipulate navigation data remotely. The consequences included compromised navigation accuracy, potential collisions or groundings, and potential disruption to maritime traffic [77].

4. Unauthorised Physical Access to Port Facilities: in July 2022, attackers gained unauthorised access to a port facility in South America by exploiting physical vulnerabilities such as weak access controls or inadequate surveillance systems. This unauthorised access allowed the attackers to tamper with critical infrastructure, compromise systems, or plant physical devices that facilitated further cyber-attacks. The consequences included disruptions in port operations, potential breaches in sensitive data, and compromised safety and security of the port and associated assets [77].

3. Discussions and recommendations

Given the literature reviewed above, the maritime industry needs to prioritise 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 2.1, to combat phishing attacks, the industry must invest in robust email security tools, implement multi-factor authentication, and conduct regular employee training to raise awareness about the dangers of phishing and how to identify and report suspicious emails.

It is stated in Section 2.2 that 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 2.3, Denial of Service attacks can be mitigated through the implementation of robust network firewalls, intrusion detection and prevention systems, and DDoS mitigation services. Regular testing and monitoring of network infrastructure can help detect and respond promptly to DDoS attacks.

To summarise the literature in Denial 2.4, the maritime industry should leverage encryption technologies, such as SSL/TLS, to counter man-in-the-middle attacks to secure data in transit. Strong access controls and authentication mechanisms should be implemented to verify the identities of communication endpoints and prevent unauthorised interception and tampering.

Addressing social engineering attacks requires different factors. These factors are employee education and strict access controls. Regular training programs should educate employees about the tactics used in social engineering attacks, emphasising the importance of verifying requests for sensitive information and reporting any suspicious activity. Additionally, implementing strong access controls and properly managing user privileges can help mitigate the risk of unauthorised access and information disclosure.

To protect against physical attacks, the maritime industry should invest in comprehensive physical security measures. This includes implementing surveillance systems, access controls, intrusion detection systems, and conducting regular physical security audits. Collaborating with security experts and sharing information about physical cyber-attacks can also enhance the industry's ability to prevent and respond to such incidents.

4. 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 cyber-attacks. Integrating digital technologies, automation, and interconnected systems brings numerous benefits to the industry, but it also opens up new vulnerabilities that malicious actors can exploit.

The maritime sector must recognise that the potential for cyber-attacks rises 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 cyber-attack. The following is a list of example systems that are vulnerable to cyber-attacks in modern-day shipping:

- Crew networks (providing Wi-Fi, entertainment, email access, etc.).
- Satellite communication systems.
- Emergency Position Indicating Radio Beacon (EPIRB).
- Radar and other navigation aiding technology.
- Voyage data recorder.
- Passenger information systems.
- Power management systems.
- Machinery management systems.
- All systems monitoring systems.

In summary, the maritime industry needs to prioritise cybersecurity and invest in robust protection measures. This includes implementing advanced cybersecurity solutions, conducting thorough risk assessments, and adopting best practices for secure system design, implementation, and maintenance.

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

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 cyber-attacks. It is essential for the industry to stay vigilant, collaborate with cybersecurity experts, and continuously enhance its cybersecurity defences 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.

Author Contributions:

Dr Steve Symes – Wrote most of this manuscript, including the abstract, introduction, literature review and parts of the discussion. This author undertook the literature search on the following aspects: cyber security in the maritime sector, cyber threats, the consequences, and the potential risk control options available. This author also integrated the co-authors' text contributions into a cohesive manuscript.

Professor Tony Graham – This co-author was the source of the idea doing this literature analysis. This author also obtained data from his vast wealth of knowledge on ship survivability concerning cyber-attacks. This co-author also proofread this literature review.

Professor Jin Wang – This co-author proofread the literature review and gave a great deal of assistance when discussing the findings from the literature analysis.

Dr Eddie Blanco*-Davis* – This co-author, having worked in the shipping industry for many years, was an advisor on how cyberattacks are dealt with in real-time, in an emergency situation. This heavily benefitted this research as it allowed for the inclusion of data and techniques that could not be found in literature searches alone.

Dr Edward Shaw was also an advisor on some of the techniques used by hackers, being a qualified ethical hacker (CEH) and cyber security architect (Network+, Security+, AZ-900, SC-900).

All authors have read and agreed to the published version of the manuscript*.*

Conflicts of Interest: The authors declare no conflict of interest.

Disclaimer

This paper is the authors' opinion and does not necessarily represent the beliefs and policies of their employers.

References

[1] A. Ahmed and V. Gkioulos, "From click to sink: Utilizing AIS for command and control in maritime cyber attacks," in *Computer security- ESORICS*, pp. 535-553, 2022.

[2] A. Ahmed and V. Gkioulos, "From click to sink: Utilizing AIS for command and control in maritime cyber attacks," in *Computer security-ESORICS*, pp. 535-553, 2022.

[3] S. Ahvenjarvi, I. Czarnowski and P. Szyman, "Safe information exchange on board of the ship," *Trans-nav international journal on maritime navigation and safety of sea transportation,* vol. 13, no. 1, pp. 165-171, Mar 2019.

[4] A. Alop, "The main challeges and barriers to the successful 'smart shipping'," *Transnav-International journal on marine navigation and safety of sea transportation,* vol. 13, no. 3, pp. 521-528, Sep 2019.

[5] A. Amro and V. Gkioulos, "Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth," *Int Journal of Information security,* vol. 22, no. 1, pp. pp.249-288, Feb 2023.

[6] A. Amro and V. Gkioulos, "Evaluation of a cyber risk assessment approach for cyber physical systems: maritime and energy use cases," *Journal of marine science and engineering,* vol. 11, no. (4), Apr 2023.

[7] A. Amro, V. Gkioulos and S. Katsikas, "Assessing cyber risk in cyber physical systems using the ATT&CK framework," *ACM transactions on privacy and security,* vol. 2, p. 26, May 2023.

[8] A. Amro, V. Gkioulos and S. Katsikas, "Connect and protect: Requirements for maritime autonomous surface ship in urban passenger transportation," *Computer security, esorics,* vol. 11980, pp. pp.69-85, 2020.

[9] A. Amro, A. Oruc and S. Katsikas, "Navigation data anomaly analysis and detection," *Information,* vol. 13, no. 3, Mar 2022.

[10] P. Anatoliy, V. Kristina and V. Aleksandr, "Technologies of safety in the Bank Sphere from cyber attacks," in *ELConRUS*, Moscow, 2018.

[11] A. Bakdi and I. V. Glad, "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,* vol. 22, no. 12, pp. 7914-7930, Dec 2021.

[12] A. Bakdi and E. Vanem, "Fullest COLREGs evaluation using fuzzy logic for collabarative decision making analysis of autnomous ships in complex situatuions," *IEEE transactions on intelligent* , vol. 23, no. 10, pp. 18433-18445, Oct 2022 .

[13] N. Landau, "Cyber Talk," 26 july 2018. [Online]. Available: http://www.cybertalk.org/2018/07/26/maritime-shipping-giant-cosco-hit-ransomware-attack/amp/. [Accessed july 2023].

[14] M. Ben Farah, E. Ukwandu and X. Bellekens, "Cyber security in the maritime industry: A systematic survey of recent advances and future trends," *Inofrmation,* vol. 1, p. 13, 2023.

[15] V. Bolbot, G. Theotokatos and A. Van Collie, "A novel risk assessment process: Application to an autonomous inland waterways ship," in *IMEJRR 2023*, Apr 2023.

[16] V. Bolbot, G. Theotokatos and D. Vassalos, "A novel cyber-risk assessment method for ship systems," *Safety Science,* p. 131, Nov 2020.

[17] C. Boudehenn, J. Cexus and A. Boudraa, "Holistic approach of integrated navigation equipment for cybersecurity at sea," in *ICCSASMCS*, 2023.

[18] A. Adegunwa, *1000 ships affected by ransomware attack on DNV software,* Accessed - July 2023: Information security buzz, January 7th 2023.

[19] J. Baker, *CMA CGM raises cyber threat risk level,* Accessed - July 2023: Lloyds list maritime intelligence, 2021.

[20] C. Chang, C. Kontovas and Z. Yang, "Risk assessment of the operations of maritime autonomous surface ships," *RESS,* p. 207, Mar 2021.

[21] S. Chiu, G. Provan and D. Vasco, "Shipboard system diagnostics & reconfiguration using model-based autonomous cooperative agents," *Control applications in maritime systems,* vol. 1, no. 1, pp. pp.323-329, 2011.

[22] K. Dittman, P. Hansen and M. Blanke, "Autonomy for ships: A sovereign agents architecture for reliability and safety by design," in *SYSTOL pp.50-57*, 2021.

[23] T. Ehlers, M. Portier and D. Thoma, "Automation of maritime shipping for more safety and environmental protection," *AT-Automatisierungstechnik,* vol. 70, no. 5, pp. 406-410, May 25th 2022.

[24] A. Epikhin and M. Modina, "Problems of introducing unmanned vessels on the basis of statistical studies of emergencies and ship losses," *Marine interllectual technologies,* vol. 3, pp. 77-82, 2021.

[25] Naval Technology, *Sea Hunter: inside the US navy's autonomous submarine tracking vessel,* Accessed - July 2023: Naval-Technology.com, 2017.

[26] A. Greenberg, *The untold story of NotPetya, the most devastating cyberattack in history,* Accessed - July 2023: Wired.com, 2017.

[27] N. Goud, *Cyber attack on COSCO,* Accessed - July 2023: Cybersecurity-Insiders.com, 2018.

[28] J. Baker, *MSC confirms website shutdown caused by cyber attack,* Accessed - July 2023: Lloyds List , 2020.

[29] V. Greiman, "Navigating the cyber sea: dangerous atolls ahead," in *14th ICCWS* , pp.87-93, 2019.

[30] Y. Fang, J. PU and S. Liu, "A control strategy of normal motion and self-rescue for autonomous underwater vehicle based on deep reinforcement learning," *AIP Advances,* vol. 1, p. 12, Jan 1st 2022.

[31] R. Hopcraft, A. Harish and K. Jones, "Raising the standard of maritime voyage data recorder security," *Journal of marine science and engineering,* vol. 11, no. 2, Feb 2023.

[32] M. Issa, A. Ilinca and P. Rizk, "Maritime autonomous surface ships: Problems and challenges facing the regulatory process," *Sustainability,* vol. 14, no. (23), Dec 2022.

[33] B. Jung, S. Moon and Y. Shin, "Development of autonomous recovery system for pipeline of naval ships by using a multistage control algorithm," *Transactions on Mechatronics,* vol. 27, no. 2, pp. pp.1150-1161, Apr 2022.

[34] J. Jung, Y. Lee and T. Yeu, "Multi-Modal sonar mapping of offshore cable lines with an autonomous surface vehicle," *Journal of marine science and engineering,* vol. 10, no. 3, Mar 2022.

[35] M. Kardakova, I. Shipunov and T. Knysh, "Cyber security on sea transport," *RESS,* pp. pp.982,481-490, 2020.

[36] G. Kavallieratos, V. Diamantopoulou and S. Katsikas, "Shipping 4.0; Security requirements for the cyber-enabled ship," *IEEE transactions on industrial informatics,* vol. 16, no. 10, pp. pp.6617-6625, Oct 2020.

[37] G. Kavallieratos, S. Katsikas and V. Gkioulos, "Modelling shipping 4.0; A reference archetecture for the cyber-enabled ship," in *ACIIDS*, 2020.

[38] G. Kavallieratos, G. Spathoulas and S. Katsikas, "Cyber risk propagation and optimal selection of cybersecurity for complex cyberphysical systems," *SENSORS,* vol. 5, p. 21, May 2021.

[39] J. Li and X. Yu, "Robust saturated tracking control of an autonomous surface vehicle," in *CCDC*, pp.3472-3477, 2020.

[40] J. Liou, "AUV hydrodynamics for survivability and controllability," in *MTS/IEEE OCEANS Conference*, Paris, 2011.

[41] G. K. V. Loukas, "A taxonomy and survey of cyber physical intrusion detection approaches for vehicles," *AD HOC Networks,* pp. 124-147,84, Mar 1st 2019.

[42] Port Technology Team, "Major European ports hit by cyber attack," Porttechnology.com, Accessed - July 2023, Feb, 3rd 2022.

[43] M. Martelli, P. Cassara and N. Tonellotto, "The internet of ships," *ERCIM NEWS,* pp. 17-18, Oct 2020.

[44] M. Martelli, A. Virdis and M. Di Summa, "An outlook on the future marine traffic management system for autonomous ships," *IEEE access,* pp. pp. 9, 157316-157328, 2021.

[45] P. McGillivary, "Why maritime cybersecurity is an ocean policy priority and how it can be addressed," *Marine technology society journal,* vol. 52, no. 5, pp. 44-57, Oct 2018.

[46] P. Meland, K. Bernsmed and D. Nesheim, "A retrospective analysis of maritime cyber security incidents," *Trans-nav-international journal on maritime navigation and safety of sea transportation,* vol. 15, no. (3), pp. 519-530, Sep 2021.

[47] O. Onishchenko, K. Shumilova and Y. Volianskyi, "Ensuring cyber resilience of ship information systems," *Transnav-international journal on marine navigation and safety of sea transportation,* vol. 16, no. (1), pp. pp.43-50, Mar 2022.

[48] C. Park and C. Kontovas, "A BN driven FMEA approach to assess maritime cybersecurity risks," *Ocean & coastal management,* p. 235, Mar 15th 2023.

[49] N. Pitropakis, M. Logothetis and C. Lambrinoudakis, "Towards the creation of a threat intelligence framework for maritime infrastructures," *Computer security esorics,* pp. 53-68, 2020.

[50] S. Qiao, K. Zheng and G. Wang, "A path planning method for autonomous ships based on SVM," *Ocean Engineering,* pp. pp.3068-3072, 2020.

[51] Y. Qiu, Y. LI and J. Lang, "An optimal tracking control method for unmanned ship approach," *CCDC (33rd),* pp. 546-551, 2021.

[52] O. Schinas and D. Metzger, "Cyber-seaworthiness: A critical review of the literature," *Marine Policy,* p. 151, May 2023.

[53] A. Sepehri, H. Vandchali and J. Montewka, "The impact of shipping 4.0 on controlling shipping accidents: A systematic literature review," *Ocean Engineering,* p. 243, Jan 1st 2022.

[54] T. Serru, N. Nguyen and A. Rauzy, "Modeling cyberattack propagation and impacts on cyber physical system safety: An experiment," *Electronics,* vol. (1), p. 12, January 2023.

[55] National Cyber Security Centre, *APT28 exploits known vulnerability to carry out reconnaissance and deploy malware on cisco routers,* Accessed - July 2023: NCSC.go.uk, 2021.

[56] K. Livelli, R. Smith and J. Gross, "Operation Shaheen," Cylance, Accessed - July 2023, 2020.

[57] C. Talos, *DNS hijacking abuses trust in core internet service,* Accessed - July 2023: Cisco Talos Intelligence.com, April 17, 2018.

[58] V. Shapo and M. Levinskyi, "Means of cyber security aspects studying in maritime specialists education," *Internet of things, infrastructures and mobile applications,* pp. pp. 1192, 389-400, 2021.

[59] I. Shipunov, K. Voevodskiy and Y. Gatchin, "About the problems of ensuring information security on unmanned ships," in *EICONRUS*, Moscow, 2019.

[60] R. Silva, C. Hickert and T. Sookoor, "AlphaSOC: Reinforcement learning-based cybersecurity automation for cyber-physical systems," in *ICCPS*, pp.290-291, 2022.

[61] B. Silverajan, M. Ocak and B. Nagel, "Cybersecurity attacks and defences for unmanned smart ships," in *IEEE ICC*, pp.15-20, 2018.

[62] P. Solnor, O. Volden and T. Fossen, "Hijacking of unmanned surface vehicles: A demonstration of attacks and countermeasures in the field.," *Journal of field robotics,* vol. 39, no. 5, pp. 631-649, Aug 2022.

[63] K. Tam and K. Jones, "Cyber-risk assessment for autonomous ships," in *international conference on cyber security and protection of digital services*, 2018.

[64] A. Titov, L. Barakat and O. Kovalev, "Risk assessment of operating unmanned ships," *Marine Intellectual Technologies,* vol. 4, no. 4, pp. 11-23, 2019.

[65] H. Tusher, Z. Munim and S. Nazir, "Cyber security risk assessment in autonomous shipping," *Maritime economics and logistics,* vol. 24, no. (2), pp. pp.208-227, Jun 2022.

[66] A. Vagale, "Evaluation simulator platform for extended collision risk of autonomous surface vehicles," *Journal of marine science and engineering,* vol. 10, no. 5, May 2022.

[67] A. Vagale, R. Bye and T. Fossen, "Path planning and collision avoidance for autonomous surface vehicles II; a comparative study of algorithms," *Journal of marine science and technology,* vol. 26, no. 4, pp. 1307-1323, Dec 2021.

[68] A. Vagale, R. Bye and T. Fossen, "Path planning for autonomous surface vehicles II: a comparative study of algorithms," *Journal of marine science and technology,* vol. 26, no. 4, pp. 1307-1323, Dec 2021.

[69] J. Yoo and Y. Jo, "Formulating cybersecurity requirements for autonomous ships using SQUARE methodology," *SENSORS,* vol. 11, no. 1, p. Chapter 23, May 24th 2023.

[70] Y. Yoo and H. Park, "Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalised ships," *Journal of marine science and engineering,* vol. (6), p. 9, Jun 2021.

[71] X. Zhou, Z. Liu and S. NI, "Collision risk identification of autonomous ships based on the synergy ship domain," in *2018 CCDC*, Beijing, 2018.

[72] X. Zhou, Z. Liu and Z. Wu, "A system-theoretic approach to safety and security co-analysis of autonomous ships," *Ocean Engineering,* p. pp.222, Feb 15th 2021.

[73] Agari, *Damages from business email compromise (BEC) top the 2019 FBI IC3 list,* Accessed - July 2023: Agari.com, 2019.

[74] Security Boulevard, *Multi-year spearphishing campaign targets he maritime industry likely for financial gain.,* Accessed - July 2023: Securityboulevard.com, 2023.

[75] A. Mascellino, *Fata Morgana watering hole attack targets shipping, logistics firms,* Accessed - July 2023: Infosecurity magazine, 2023.

[76] V. Nicaise, *Cybermaretique: a short history of cyberattacks against ports,* Accessed - July 2023: Stormshield, 2021.

[77] N. Polemi and C. Van-Maele, "Cybersecurity inmaritime infrastructure," European Commission, Brussels, 20/04/2023.

590

591

592

593

594

595

596