ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων

Επισκόπηση Θεμάτων Κυβερνοασφάλειας σε Θαλάσσια Συστήματα

(A Survey of Cybersecurity Issues in Maritime Systems)

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

των

Διακρούση Ελευθερία
Κατσαρό Παναγιώτη

Επιβλέπων: Κρητικός Κυριάκος (Αναπληρωτής Καθηγητής)

Μέλη εξεταστικής επιτροπής: Κοκολάκης Σπύρος (Καθηγητής), Στεργιόπουλος Γεώργιος (Επίκουρος Καθηγητής)

Σάμος, Ιούλιος 2024

Περίληψη

Οι λύσεις πληροφοριακών συστημάτων χρησιμοποιούνται όλο και περισσότερο στη ναυτιλιακή βιομηχανία, οδηγώντας σε έναν ολοκληρωμένο ψηφιακό μετασχηματισμό σε όλους τους τομείς των ναυτιλιακών δραστηριοτήτων. Δυστυχώς, υπό το φως ενός τέτοιου μετασχηματισμού, σημειώθηκε μια ραγδαία αύξηση των κυβερνοεπιθέσεων, οδηγώντας σε σημαντικές οικονομικές απώλειες για τις επιχειρήσεις λόγω του κόστους ανάκαμψης, των κανονιστικών κυρώσεων και των παράπλευρων ζημιών στη φήμη και την εμπιστοσύνη. Παρά το γεγονός ότι ο ναυτιλιακός τομέας θεωρούνταν προηγουμένως ασφαλής λόγω της περιορισμένης σύνδεσης στο διαδίκτυο και της απομονωμένης φύσης των πλοίων στη θάλασσα, παρατηρήθηκε μια εκπληκτική αύξηση 900% στις παραβιάσεις της κυβερνοασφάλειας που στοχεύουν την τεχνολογία λειτουργίας καθώς ο κλάδος μεταβαίνει στην ψηφιακή εποχή [1].

Λαμβάνοντας υπόψη τα παραπάνω, καθώς και την έμφαση του κλάδου στη συμμόρφωση και την ιστορική του εστίαση σε θέματα διεθνούς ασφάλειας και προστασίας, έχει καταστεί σαφές ότι τα συστήματα κυβερνοασφάλειας διαδραματίζουν κρίσιμο ρόλο στη διασφάλιση της ναυτιλιακής ασφάλειας και προστασίας. Αναγνωρίζοντας το αυτό, οι απαιτήσεις εφαρμογής της κυβερνοασφάλειας ενσωματώνονται πλέον στο κανονιστικό πλαίσιο του ναυτιλιακού τομέα.

Ενώ έχουν διεξαχθεί ορισμένες έρευνες σε αυτόν τον τομέα, η θαλάσσια κυβερνοασφάλεια παραμένει σε μεγάλο βαθμό ανεξερεύνητη. Ως εκ τούτου, η παρούσα διατριβή αναλαμβάνει μια διεξοδική διερεύνηση του τοπίου της κυβερνοασφάλειας στον ναυτιλιακό τομέα, με στόχο να προσφέρει πολύτιμες γνώσεις στις διάφορες πτυχές της θαλάσσιας κυβερνοασφάλειας, παρουσιάζοντας μια αντίστοιχη ταξινόμηση καθώς και αναλύοντας σε βάθος τις κοινές ευπάθειες, απειλές και επιθέσεις στην κυβερνοασφάλεια σε θαλάσσια/ναυτιλιακά συστήματα. Επιπλέον, προσδιορίζονται και αναλύονται διεξοδικά, συγκρίνονται και ταξινομούνται σε κατάλληλες κατηγορίες κατάλληλα αντίμετρα, με κύριο στόχο την αποκάλυψη κατάλληλων στρατηγικών μετριασμού του κινδύνου που μπορούν να καλύψουν κάθε είδους περιστατικού και περίπτωσης ασφάλειας, ικανοποιώντας παράλληλα τις απαιτήσεις και τις προτιμήσεις ασφάλειας των ναυτιλιακών οργανισμών. Προσδιορίζοντας τα κενά της έρευνας καθώς και τις κατευθύνσεις έρευνας που πρέπει να ακολουθηθούν, η παρούσα έρευνα στοχεύει να συμβάλει στην ανάπτυξη ασφαλέστερων και πιο ανθεκτικών ναυτιλιακών συστημάτων.

Λέξεις-Κλειδιά: Ασφάλεια Πληροφοριών, Κυβερνοασφάλεια, Θαλάσσια Κυβερνοασφάλεια, Ναυτιλιακά Συστήματα, Τεχνολογία Λειτουργίας, Τρωτότητες, Αντίμετρα

Abstract

Information system solutions are increasingly being utilized within the maritime industry, leading to a comprehensive digital transformation across all aspects of maritime operations. Unfortunately, in light of such a transformation, there has been a rapid increase in cyberattacks, leading to significant financial losses for businesses due to recovery costs, regulatory penalties, and collateral damage to reputation and trust. Despite the maritime sector previously being considered safe due to limited internet connectivity and the isolated nature of ships at sea, there has been a staggering 900% rise in cybersecurity breaches targeting operational technology as the industry transitions into the digital age [1].

By taking into consideration the above, as well as the industry's emphasis on compliance and its historical focus on international security and safety matters, it has become evident that cybersecurity systems play a crucial role in ensuring maritime safety and security. Recognizing this, cybersecurity implementation requirements are now being integrated into the regulatory framework of the maritime sector.

While some research has been conducted in this field, maritime cybersecurity remains largely unexplored. Therefore, this thesis undertakes a thorough investigation into the cybersecurity landscape of the maritime sector, aiming to offer valuable insights into the various aspects of maritime cybersecurity, by presenting a corresponding taxonomy as well as deeply analysing common maritime cybersecurity vulnerabilities, threats and attacks. Additionally, suitable countermeasures are identified as well as thoroughly analysed, compared and classified into proper categories with the main aim of unveiling well-suited risk mitigation strategies that can cover any kind of security incident and case while satisfying the security requirements and preferences of maritime organisations. By identifying the research gaps as well as the research directions to be followed, this research aims to contribute to the development of safer and more resilient maritime systems.

Keywords: Information Security, Cyber Security, Maritime, Maritime Cybersecurity, Maritime Systems, Operational Technology, Vulnerabilities, Countermeasures

Πίνακας περιεχομένων

Λίστα εικόνων

Λίστα πινάκων

1 *Introduction*

The economic stability of numerous regions worldwide is highly dependent on maritime transportation. Factors, such as population growth, enhanced living conditions, increased investments, and the removal of trade barriers, collectively fuel a growing dependence on this industry. In geographical areas characterised by navigable rivers or islands, maritime transportation serves as the backbone of both domestic and international trade. Furthermore, in markets prioritizing sustainable development, cost-efficiency, and environmentally friendly practices, the maritime sector plays a pivotal role by handling 90% of all goods transportation [2].

In the past decade, technological advancements have progressed at an unprecedented pace, reshaping numerous industries through the integration of innovative technologies, policies, and operational practices. Similar to various sectors, the maritime industry has embraced advanced digitization, information technology, and operational procedures. The importance of cyber technologies has escalated significantly, extending beyond the mere operation and management of various systems and processes on ships and ports. Such technologies now play a crucial role in ensuring the safety, security, and protection of ships, crews, cargo, and the marine environment. These technologies have merged Information Technology (IT) and Operational Technology (OT) on ships through networked connectivity to the Internet.

Operational technology (OT) systems, such as navigation, cargo management and propulsion control, are increasingly interconnected to provide efficiency and data collection benefits. Unfortunately, such interconnections provide a greater attack surface for hackers. Further, traditionally, ship management networks used for tasks, such as email and internet access, were separate from critical OT systems. As such, due to the lack of interconnection, no significant security problem could be exhibited. However, as such an interconnection now exists, an attack on one system can be expanded over the other. Thus, this kind of bridge provides a single point of entry for attackers who exploit vulnerabilities in the management network to gain access to critical OT systems.

Additionally, many maritime systems are based on legacy technology that lacks the security features of modern systems. In this way, these legacy systems often have unpatched vulnerabilities and are prime targets for exploitation. Further, patching and updating legacy systems can be challenging due to compatibility issues and the high cost of completely replacing or re-engineering systems.

Surely, the human factor and especially social engineering that exploits it cannot be missing from the maritime cyber security landscape. In particular, cyber-attacks often target not only technical vulnerabilities but also human weaknesses. Crew members can be tricked by social engineering tactics, such as clicking on malicious links, opening infected attachments, or infecting IT and OT systems with malware by inserting a malicious USB.

In the World Economic Forum's Global Risks Report 2020, cyberattacks targeting critical infrastructure, including shipping, are identified as the fifth top risk for 2020. According to Rizika, cyber-attacks on the

maritime industry's OT systems have surged 900% in the last three years. Reported cases have risen from 50 significant OT hacks in 2017 to 120 in 2018 and over 300 in the preceding year [3].

Furthermore, the inadequacy of proper training to address evolving threats underscores the critical nature of emerging maritime cybersecurity risks. The current curriculum in maritime and naval training institutions is insufficiently aligned with modern cybersecurity challenges. Further, domestic and international regulations are found to be lacking in effectively addressing maritime cyber threats [4].

Another significant issue is the absence of a common platform for sharing information on similar threats encountered by different countries, largely due to national security concerns. Currently, the private sector's involvement in addressing maritime cybersecurity challenges is limited, with governmental agencies bearing the primary responsibility. This reliance places immense strain on the already insufficient resources of these security agencies [5].

Last but not least, significant gaps in maritime cybersecurity have been identified in the related literature. Initially, research in this field has been hindered by data-related challenges. Information regarding cybersecurity incidents is often withheld from the public as a means of preserving the reputation of affected organizations. This reluctance stems from security and privacy concerns, which hinder organisations from disclosing vulnerability-related information that could deteriorate their security situation. Consequently, much of the analysis and response efforts have been reactive rather than proactive due to the lack of credible and actionable data for scenario modelling. Furthermore, there appears to be a limited number of studies examining the economic impacts of potential maritime cybersecurity attacks, particularly within academic literature. Although some reports on this subject are prepared for governments, they often possess limitations, since as mentioned above, the full extent of the cybersecurity incidents is often withheld from the public.

The current thesis offers, compared to the current literature, a deeper and more comprehensive insight into maritime cybersecurity by covering all related aspects and topics, starting with a categorization of cybersecurity vulnerabilities, threats and attacks and then continuing by analysing all these security subjects in detail. Further, known countermeasures are thoroughly categorised and analysed with the aim of identifying the most effective ones that can be then globally implemented. Moreover, risk management techniques that can be universally applied to successfully tackle maritime cybersecurity issues are presented. Finally, key research gaps and challenges, as identified through the current literature, are presented, as well as promising research directions for addressing these gaps.

The remaining of this thesis report is as follows. The next chapter, the background one, is going to supply a basic definition of relevant cybersecurity concepts, like vulnerabilities, threats and countermeasures, as well as a short view of onboard systems. The third chapter identifies the literature review methodology followed, clarifying the main research questions to be answered as well as the way the relevant academic literature was identified and filtered. The main part of the thesis, spanning Chapters 4-6, thoroughly examines cybersecurity issues on maritime ship systems, analyses relevant countermeasures and discusses suitable risk management techniques to apply to such systems. Chapter 7 identifies the main research gaps in maritime cybersecurity as well as unveils promising research directions to address them. Finally, the last chapter summarises the thesis's main contribution, clarifies the main experience gained, outlines the key findings achieved and supplies priorities for future research.

2 Background

2.1 Cybersecurity

During the last decade, cybersecurity has been a dominant research topic - this can be deduced by the significant number of scientific papers that have been recently published. Specifically, by searching for the keyword Cybersecurity in Google Scholar, one of the main search engines used for the retrieval of information in the context of the current survey, approximately 627k papers were obtained during the initial stages of drafting this thesis, 715K are retrieved upon its finalisation. Similarly, in Scopus 13,152 results were initially presented as relevant, while 35,644 were presented after only 3 months.

But what is cybersecurity? Based on our research, many definitions of cybersecurity are available. For the purposes of the current document, the NIST definition of cybersecurity will be used, as it applies better to the current thesis covering all aspects of maritime systems cybersecurity. This definition is as follows: "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation."

2.1.1 Cybersecurity aspects

Cybersecurity encompasses various aspects that contribute to protecting computer systems, electronic communications systems and services, data, and relevant information from potential threats. Some of the key aspects of cybersecurity include [6]:

- The network security which focuses on securing the network infrastructure (e.g. routers, switches, firewalls, network devices) so as to prevent common threats, such as unauthorized access, data breaches, and other cyber-attacks.
- The endpoint security which involves securing individual devices (e.g. computers, laptops, mobile devices, servers) from malware, viruses, ransomware, phishing attacks, internal threats and other malicious software that can compromise data and system integrity.
- The data security which concerns protecting sensitive data from unauthorized access, disclosure, alteration, and destruction. To achieve this, measures such as encryption, access control, data masking, and data loss prevention are implemented to safeguard data confidentiality, availability and integrity.
- The Identity and Access Management (IAM) which focuses on managing user identities, authentication, and authorization to ensure that only authorized users have access to the appropriate resources and data within an organization's system.

- The application security which involves securing software applications and systems from security vulnerabilities and exploits. This includes secure coding practices, application testing, and patch management to mitigate risks associated with software vulnerabilities.
- The cloud security which addresses security concerns related to cloud computing environments (comprising applications, services, data, platforms and infrastructure), including data protection, identity management, resource isolation, and compliance with security standards and regulations in cloud-based infrastructures and services.
- The Incident Response and Management which involves preparing for detecting and responding to security incidents and breaches effectively. This includes establishing incident response plans, conducting security incident investigations, and implementing measures to mitigate the impact of security breaches.
- Security Awareness and Training which focus on educating employees and users about cybersecurity best practices, security policies, and potential threats to raise awareness and promote a culture of security within an organization.
- The compliance and regulatory compliance which involve ensuring that cybersecurity measures align with relevant laws, regulations, industry standards, and compliance requirements applicable to an organization's operations and data handling practices.
- The threat intelligence and monitoring which involve gathering and analysing information about potential cyber threats, vulnerabilities, and attack techniques to proactively identify and respond to emerging security threats and trends.

2.1.2 Known vulnerabilities, threats and attacks

The following section summarizes the cybersecurity known vulnerabilities, threats and attacks. Detailed information on these topics will be presented in Chapter 4 in the context of maritime system cyber-security [7], [8].

2.1.2.1 Vulnerabilities

According to NIST vulnerability is defined as 'Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source'. The most common cybersecurity vulnerabilities according to the current literature are [9], [10]:

- *Software vulnerabilities*: Software vulnerabilities are encountered when applications contain errors or bugs, presenting opportunities for attackers to exploit these weaknesses and compromise the system. Examples of attacks resulting from software vulnerabilities include buffer overflow and race conditions.
- *Firewall vulnerabilities*: Firewalls act as protective barriers, both in software and hardware, defending networks against attacks. A firewall vulnerability refers to an error, deficiency, or mistaken assumption in the design, implementation, or configuration of the firewall that can be exploited to launch attacks against the trusted network it is meant to protect. Examples of attacks are bypass attacks, application-layer attacks and man-in-the-middle attacks.

- *Wired network vulnerabilities*: Wired network vulnerabilities exist across different layers of a network. Certain protocols may be wrongly designed or be deficient in implementing necessary security features within an unprotected network. Examples of attacks resulting from wired network vulnerabilities include ARP attacks and fragmentation attacks.
- *Wireless network vulnerabilities*: Wireless Local Area Networks (LANs) face protocol-based attacks similar to those seen in wired LANs, such as MAC flooding and DNS spoofing. Insecure wireless access points pose a potential threat by providing attackers with an entry point to gain unauthorized access to personal or corporate networks. Illustrative vulnerabilities in this context involve issues with the Service Set Identifier (SSID) like SSID Broadcasting or default SSIDs and weaknesses in Wired Equivalent Privacy (WEP), such weak encryption algorithm and key management issues.
- *Operating system vulnerabilities*: Operating systems (OS) are complex pieces of software that manage hardware and software resources on computers. Due to their complexity, they often have vulnerabilities that can be exploited by attackers. Common examples of operating system vulnerabilities are buffer overflow, privilege escalation and code injection.
- *Hardware*: Hardware vulnerabilities involve weaknesses in the physical components of a computer system. For instance, firmware attacks target the low-level software that controls hardware, such as the BIOS or UEFI, exploiting common vulnerabilities such as outdated firmware, allowing attackers to install persistent malware that can evade traditional security measures.
- *Physical security*: Physical security vulnerabilities involve weaknesses that allow unauthorized individuals to access, tamper with, or damage hardware. For example, theft and tampering are significant threats, where physical devices like laptops or servers are stolen or manipulated to extract sensitive data. Unauthorized access to restricted areas can lead to data breaches or sabotage, often due to inadequate access control measures, such as poorly implemented badge systems or unguarded entry points.
- *Authentication:* Authentication vulnerabilities in cybersecurity refer to weaknesses or flaws in the processes and mechanisms used to verify the identity of users, devices, or systems before granting access to resources. These vulnerabilities can be exploited by attackers to gain unauthorized access, leading to data breaches, theft, or other malicious activities. Examples include weak passwords, default credentials and token-based vulnerabilities.

2.1.2.2 Threats

According to NIST, a cybersecurity threat is defined as ‘Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.’ The most common cybersecurity threat types are described below [11]:

- *Computer viruses*: A computer virus is a type of software that, through activation, damages the computer without the user's permission or awareness, often attempting to conceal itself within other files. Common virus extensions are ".exe," ".com," or ".pif".
- *Computer worms*: The computer worm is software that actively identifies additional machines to infect by exploiting software vulnerabilities. Every infected machine becomes the means for further propagation, i.e., worms generate multiple copies of themselves and disseminate them across vulnerable servers and computers on the web. Such a propagation takes place by exploiting the network, shared media and email messages. The vulnerabilities exploited can concern client or server software. A worm can be the medium through which other kinds of malware can be injected like viruses. Further, it can lead to system performance degradation.
- *Trojan horses*: Conversely, Trojan horses are a type of malicious software that masquerades as legitimate programs to entice users into downloading them. Hence, they are activated only when the user installs and runs the infected program file. Trojan horses typically consist of two components: the initial file sent to the user, which covertly opens a port on the computer to allow attacker access, and a second file that, when executed, grants the attacker control over the user's computer. Attackers can exploit these backdoors to obtain sensitive personal information, such as passwords, credit card details, and other critical documents from the victim's system. Additionally, Trojans facilitate the installation of additional malware by creating entry points for attackers.
- *Rootkits*: A Rootkit is a type of malicious software designed to enable hackers to gain and maintain unauthorized (root) access and control over a victim's device. Once a rootkit gains access to a computer, it enables cybercriminals to carry out various malicious activities, such as stealing financial and personal information, deploying additional malware, or utilizing compromised devices as part of a botnet to distribute spam or launch Distributed Denial of Service (DDoS) attacks.
- *Hackers and predators*: Hackers are unauthorized individuals who target systems to steal, alter, or destroy data by deploying malicious software without consent or physically destroying the targeted systems. These usually online attackers and malicious actors often employ phishing scams, spam, and other tactics to distribute harmful files and compromise security. Without firewall protection, hackers can attempt to breach computers and access private information directly. Predators, often assuming false identities, may expose sensitive personal and financial data or engage in more nefarious activities.
- *Malicious insiders*: A malicious insider threat refers to the risk posed by individuals within an organization who intentionally exploit their access to sensitive information and systems to cause harm. These insiders may be current or former employees, contractors, business partners, or anyone with authorized access to the organization's resources. The threat they pose is particularly significant due to their intimate knowledge of the organization's systems, processes, and security measures, allowing them to bypass external and internal defences with relative ease.
- *Data Threats*: Data threats involve unauthorized actions that compromise the confidentiality, integrity, or availability of data. Common examples include data breaches, where sensitive information is accessed and stolen by unauthorized parties, such as the Equifax breach that exposed millions of personal records. Ransomware attacks, like the WannaCry incident, encrypt data and demand a ransom for decryption, causing significant disruptions and potential data loss.

- *Application Threats*: Application threats target vulnerabilities within software applications to gain unauthorized access or disrupt services. SQL injection attacks, such as the one that affected Heartland Payment Systems, involve inserting malicious SQL code into an application's input fields to manipulate the database. Cross-site scripting (XSS) attacks, exemplified by the MySpace Samy worm, involve injecting malicious scripts into webpages viewed by other users, potentially leading to data theft or session hijacking.
- *Server Threats*: Server threats focus on compromising server integrity, availability, or confidentiality. Unauthorized access to servers, as seen in the Capital One breach, allows attackers to steal sensitive information. Malware infections, like the Petya ransomware, can cripple server operations by encrypting data or taking control of server functionalities. Configuration exploits, which take advantage of weak server configurations, can also lead to unauthorized access or control.
- *Network Threats*: Network threats rely on exploiting vulnerabilities in network infrastructure to intercept, disrupt, or manipulate communications. Man-in-the-Middle (MitM) attacks, such as Wi-Fi eavesdropping, intercept communications between two parties to steal data or inject malicious content. Distributed Denial of Service (DDoS) attacks, like the one on Dyn DNS, overwhelm network resources with traffic, rendering services unusable. Eavesdropping attacks capture unencrypted data traversing the network, posing significant privacy risks.
- *API Threats*: API threats exploit vulnerabilities in application programming interfaces (APIs) to gain unauthorized access, manipulate data, or disrupt services. API injection attacks, such as those targeting the Trello API vulnerability, involve injecting malicious code through API endpoints. Broken authentication mechanisms, as seen in the Uber API breach, allow unauthorized users to access sensitive data. Poorly designed APIs can inadvertently expose sensitive information, leading to data leaks and other security issues.
- *Hardware Threats*: Hardware threats involve risks and attacks that compromise the physical components of computer systems, leading to potential disruptions, data loss, or unauthorized access. Examples include physical tampering, where attackers gain direct access to hardware to steal data or install malicious devices like key loggers. Side-channel attacks, such as Spectre and Meltdown, exploit vulnerabilities in hardware design to gain access to sensitive information. Hardware failures due to aging or environmental factors, like overheating, can lead to data corruption or loss of service. Supply chain attacks, where malicious components are introduced during the manufacturing process, pose significant security risks by embedding vulnerabilities directly into hardware.

2.1.2.3 Attacks

Cyber-attacks are illegal actions that are carried out through computer channels (e.g., Wi-Fi, SSDs, IPs, and USBs) or that aim to destroy and damage computers, electronic media and internet networks, as well as management and organization systems. They are characterized as premeditated, and at times politically motivated, attacks against information, computer systems, computer programs and data that may result in violence against non-combatant targets by subnational groups or clandestine agents [12].

The most common cyber security attacks are summarized below [13]:

- *Social engineering attacks*: The act of deceiving individuals into divulging information or granting access to data networks and computer systems is referred to as "social engineering." The objective

of social engineering is to circumvent the security defences of individuals or organizations. Examples include baiting, pretexting and phishing attacks.

- *Application attacks*: An application attack occurs when cybercriminals gain unauthorized access to web applications. Attackers typically begin by examining the application layer to identify vulnerabilities in the code. Vulnerabilities within applications provide cybercriminals with opportunities to exploit them in production environments. These exploits target both the application code as well as open-source frameworks and libraries utilised by an application. Cybercriminals leverage various methods, such as exploiting code vulnerabilities (e.g., data validation vulnerabilities to conduct buffer overflow attacks), legacy certificates, and authentication deficiencies, to carry out these attacks.
- *Cryptography attacks*: Cryptographic attacks occur when an attacker attempts to compromise a cryptosystem by identifying weaknesses in the code, cipher, cryptographic protocol, or key management scheme. These attacks are categorized as either passive or active. Passive attacks involve unauthorized access to information without disrupting the communication channel, whereas active attacks involve modifying the information transmitted or initiating unauthorized transmissions of information. Passive attacks typically focus on information theft, while active attacks involve unauthorized data manipulation and tampering. Both types of attacks pose risks to the integrity and confidentiality of sensitive information.
- *Hijacking attacks*: Hijacking attacks represent a category of network security breaches where an attacker gains control over computer systems, software programs, and network communications. Many cyberattacks leverage hijacking techniques. Various types of hijack attacks exist, as outlined below:
    - *browser hijacking*: unauthorized modification of a web browser's settings to inject unwanted advertisements, redirect users to malicious websites, or alter the home page and search engine settings,
    - *session hijacking*: exploitation of a valid computer session to gain unauthorized access to information or services in a computer system, often through stealing session cookies,
    - *domain hijacking*: unauthorized acquisition of control over a domain name, typically through exploiting vulnerabilities in domain registration processes or through social engineering tactics,
    - *clipboard hijacking*: malicious act of accessing and altering the contents of a user's clipboard to replace it with malicious content, such as changing a copied URL or cryptocurrency address,
    - *domain name system (DNS) hijacking*: Unauthorized manipulation of DNS records to redirect traffic from a legitimate website to a fraudulent one, often used in phishing attacks or to distribute malware,
    - *Internet protocol (IP) hijacking*: unauthorized takeover of IP address blocks, typically by exploiting vulnerabilities in the Border Gateway Protocol (BGP) to reroute internet traffic for malicious purposes and
    - *page hijacking*: malicious activity where an attacker takes over or manipulates a web page, often by redirecting traffic to a different, usually malicious, page to steal sensitive information or injecting malicious content.

- *Computer network attacks (CNAs):* CNAs involve manipulating, corrupting, altering, or destroying information within computers and computer networks to seize control of these systems. Through CNAs, attackers can effectively shut down systems, manipulate data, and misuse resources for activities like creating botnets, ultimately compromising the integrity or availability of targeted systems. CNAs operate by leveraging data streams to execute attacks. To execute a CNA, attackers first gain unauthorized access to the network, then conduct reconnaissance to understand the network's configuration and identify optimal methods for carrying out their malicious actions. This discovery phase enables attackers to plan and execute their attacks more effectively.
- *Malware attacks:* Malware is a broad term used to describe software specifically created to cause harm to computer systems, steal data, or disrupt users. Types of this software include viruses, worms, Trojans, and rootkits. Malware code can be written in various programming or scripting languages and embedded in numerous file formats. Malware can silently collect information and conduct surveillance over extended periods without raising suspicion within the infected system. Furthermore, it can be deployed to inflict harm or sabotage on the system it infiltrates (as seen with Stuxnet), or it may be utilized for extortion purposes, demanding monetary compensation (e.g., ransomware).
- *Bots and botnets:* A "bot" is a software program designed to carry out repetitive, automated, and predefined tasks, often emulating or replacing human user behaviour. The term "botnet" is a combination of "robot" and "network." Botnets comprise multiple software agent programs, each remotely controlled. These networks of computers can act cohesively as a unit to accomplish repetitive tasks and objectives. Due to their automated nature, bots operate at a significantly faster pace than human users. They can serve practical purposes like customer service or search engine indexing, but they can also be utilized as malicious software (malware) to gain full control over a computer system. Malware bots and Internet bots can be programmed or hijacked to breach user accounts, harvest contact details, send spam, or execute other harmful activities like Distributed Denial of Service (DDoS) attacks. Under the control of an attacker, a botnet can be likened to a network of thousands or even hundreds of thousands of compromised ("zombie") computers.
- *Password attacks:* Password attacks are among the most commonly employed tactics in cyberattacks, targeting both corporate entities and individuals. The objective is to compromise institutions or individuals by obtaining or “guessing” passwords used across various platforms, including social media networks, technologies, or software employed by the target. Typically, individuals or organizations opt for simplistic passwords to minimize the risk of forgetting them. Notably, users often divulge details, such as their favourite sports team, place of origin, birthdate, spouse or partner's name, and relationship duration on their profiles. This personal information is invaluable to cyber attackers, facilitating their efforts in executing password attacks.
- *Man-in-the-middle attack:* A man-in-the-middle attack is characterized as a cyberattack where a malicious individual covertly intervenes in communication between two parties. This attack enables the perpetrator to intercept and potentially alter transmitted data. Typically, the objective of a man-in-the-middle attack is to acquire sensitive information, such as personal data, passwords, or banking details, or to impersonate one of the communicating parties. Locations offering free Wi-Fi present ideal settings for executing such attacks. In these environments, unencrypted data packets can be easily intercepted and inspected. Attackers positioned within Wi-Fi areas can reroute network traffic

through their own systems, allowing them to capture personal data and passwords from unsuspecting users.

2.1.3 Countermeasures and techniques

As per NIST, countermeasures are defined as "Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices."

To address the constantly changing landscape of cyber threats, it is crucial for both organizations and individuals to adopt a robust array of cybersecurity measures. These methods and protocols are designed to thwart, identify, react to, and rebound from cyber-attacks effectively. Below are key countermeasures that should be considered essential [14].

2.1.3.1 Prevention Strategies

- *Security Awareness Training:* Through educating employees and users about the continuously evolving threat landscape, organizations enable them to serve as vigilant protectors of digital assets. Training sessions delve into identifying phishing emails, recognizing social engineering tactics, properly using security measures, and adopting safe online behaviours.
- *Network Segmentation:* This strategy involves partitioning a network into separate segments, each with distinct access controls and permissions. By compartmentalizing sensitive data and critical systems away from less sensitive areas, network segmentation obstructs lateral movement for attackers, reducing their ability to navigate the network once they gain access. In the event of a breach, the impact remains confined within the compromised segment, preventing the threat from spreading uncontrollably. This approach is particularly essential for protecting critical infrastructure and sensitive data, bolstering the organization's ability to withstand cyber-attacks, and ensuring that a breach in one area does not cascade into systemic failure.
- *Patch Management:* Given the frequent discovery of new weaknesses, timely patch management is critical. It guarantees that potential security holes are closed off before attackers can exploit them. Automated patch management systems simplify this process, enabling organizations to promptly address emerging threats.
- *Email Filtering and Anti-phishing Solutions*: Sophisticated filtering mechanisms inspect incoming emails for malicious attachments, links, and content, intercepting them before they reach users' inboxes. Anti-phishing solutions utilize machine learning and behavioural analysis to detect and thwart phishing emails that aim to trick users into disclosing sensitive information. This proactive strategy minimizes the attack surface, reinforcing cybersecurity defences and shielding against the unintentional human errors that attackers exploit.
- *Threat Intelligence:* Threat intelligence involves the collection, analysis, and dissemination of information about potential or current threats to an organization's cybersecurity. This intelligence includes data on threat actors, their tactics, techniques, and procedures (TTPs), as well as indicators of compromise (IOCs), such as malicious IP addresses, URLs, and file hashes. By leveraging threat intelligence, organizations can proactively defend against cyber threats, enhance their security posture, and make informed decisions about their security strategies. Effective threat intelligence

helps in identifying and mitigating risks before they can be exploited by attackers, thus playing a crucial role in pre-emptive cybersecurity measures.

- *Vulnerability Assessment and Penetration Testing:* Vulnerability assessment and penetration testing are critical components of a robust cybersecurity strategy. Vulnerability assessment involves systematically scanning systems, networks, and applications to identify potential security weaknesses and misconfigurations that could be exploited by attackers. Penetration testing, on the other hand, simulates real-world attacks to test the effectiveness of existing security measures and identify vulnerabilities that may not be detected through automated scanning alone. Together, vulnerability assessment and penetration testing help organizations uncover and address security gaps, prioritize remediation efforts, and strengthen their overall defence mechanisms against potential cyber threats.

2.1.3.2 Detection and Response Measures

- *Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):* An IDS monitors network traffic and systems to detect suspicious or unauthorized activities. When an anomaly is identified, alerts are generated to notify security personnel of potential threats. IPSs take this a step further by not only detecting but also actively preventing malicious activities, automatically blocking or mitigating threats in real-time. Together, IDSs and IPSs create a proactive defence, enabling organizations to detect and thwart intrusions before they result in breaches. By analysing network patterns and behaviours, these systems improve situational awareness, offering valuable insights that assist in immediate incident response and future security improvements.
- *Security Information and Event Management (SIEM) Systems:* Through correlating and cross-referencing data, SIEM systems detect patterns, anomalies, and potential security incidents. They provide real-time monitoring and issue alerts for suspicious activities, enabling security teams to respond swiftly. SIEM's historical analysis capabilities support post-incident forensics and compliance reporting. These systems deliver a comprehensive perspective on an organization's security status, facilitating proactive threat detection, effective incident response, and ongoing enhancement of cybersecurity strategies.
- *Incident Response Plans:* Incident Response Plans (IRPs) are strategic guides that navigate organizations through the complex landscape of cyber incidents. These carefully crafted plans define detailed procedures, roles, responsibilities, and communication protocols to be followed in the event of a security breach. IRPs ensure that the response is well-coordinated, prompt, and efficient, minimizing confusion during high-pressure scenarios. From initial detection through containment, eradication, recovery, and lessons learned, IRPs establish a structured framework that facilitates a smooth transition from disorder to control.
- *Threat Hunting*: Threat hunting is a proactive approach where experienced cybersecurity professionals actively seek out signs of concealed threats within an organization's network and systems. Instead of solely depending on automated alerts, threat hunting aims to uncover anomalies and indicators of compromise that might evade conventional detection methods. This proactive strategy aids in early threat identification, enabling prompt containment and mitigation efforts. Threat hunting typically involves analysing patterns, behaviours, and outlier activities that could suggest the existence of advanced threats. By keeping ahead of adversaries, organizations enhance

their defensive capabilities and ensure that potential breaches are detected before they escalate into significant incidents.

- *Firewalls:* Firewalls are essential cybersecurity countermeasures that act as the first line of defence in network security. They function by monitoring and controlling incoming and outgoing network traffic based on established security rules, effectively creating a barrier between trusted internal networks and untrusted external networks, such as the Internet. Firewalls can be implemented as hardware, software, or a combination of both, and are crucial in preventing unauthorized access, blocking malicious traffic, and protecting sensitive data from external threats. Advanced firewalls, like next-generation firewalls (NGFWs), also provide deep packet inspection, intrusion prevention, and application-level monitoring, significantly enhancing network security.
- *Anti-virus / anti-malware software:* Anti-virus software plays a critical role in safeguarding computers and networks from malware, including viruses, worms, Trojan horses, ransomware, and other malicious programs. It operates by scanning files, applications, and system memory for known malware signatures and suspicious behaviours. Anti-virus programs can prevent, detect, and remove malware, offering real-time protection and periodic system scans to ensure the integrity and security of the system. Regular updates to the anti-virus database are essential to defend against the latest threats. By identifying and neutralizing malware, anti-virus software helps prevent data breaches, system damage, and loss of sensitive information.
- *Forensics analysis:* Forensics analysis in cybersecurity involves the meticulous examination of digital devices and networks to investigate cyber incidents and gather evidence of illegal activities. This process includes collecting, preserving, and analysing digital data to uncover the details of cyber-attacks, such as the methods used, the extent of the breach, and the identity of the attackers. Forensic analysis is crucial for understanding the nature and scope of security incidents, enabling organizations to mitigate the damage, recover compromised systems, and enhance future security measures. It also plays a pivotal role in legal proceedings, providing the necessary evidence to support the prosecution of cybercriminals and the resolution of legal disputes related to cyber incidents.

2.1.3.3 Encryption and Data Protection

- *End-to-End Encryption:* This method ensures that the transferred data remains confidential and secure throughout transmission, starting from the sender's device until it reaches the intended recipient's device. Utilizing secure communication protocols (e.g., TLS, SSH) encryption keys exclusively known to the sender and recipient, end-to-end encryption prevents and intermediaries from accessing the actual data contents.
- *Data Loss Prevention (DLP) Solutions:* These systems utilize content analysis, contextual awareness, and policies to oversee data flows, identifying and thwarting attempts to transfer, share, or leak sensitive information without proper authorization. DLP solutions can recognize patterns suggestive of data breaches, such as efforts to send confidential files via email or upload them to unauthorized cloud services. By preventing data leaks and unauthorized transfers, DLP solutions play a crucial role in safeguarding data, ensuring regulatory compliance, and upholding an organization's reputation.

- *Zero Trust Architecture:* In a Zero Trust environment, no entity—whether internal or external to the network—is automatically considered trustworthy. Instead, access to resources and data is granted based on rigorous verification and continuous authentication. This approach relies on multifactor authentication, dynamic authorisation, robust identity verification, and micro-segmentation to uphold the principle of "never trust, always verify." By treating each access request as potentially malicious, Zero Trust Architecture (ZTA) reduces the impact of breaches by restricting lateral movement and minimizing the attack surface.
- *Encryption of data:* Encryption of data involves converting plaintext into cipher text using cryptographic algorithms to ensure that only authorized parties can access the information. It is a fundamental cybersecurity countermeasure that protects data at rest and in transit from unauthorized access, eavesdropping, and tampering.
- *Data Recovery:* Data recovery is the process of retrieving lost, corrupted, or accidentally deleted data from storage devices. Effective data recovery strategies are essential in cybersecurity to ensure business continuity and mitigate the impact of data loss due to cyberattacks, hardware failures, or human errors.
- *Backup:* Backup involves creating copies of data and storing them in separate, secure locations to protect against data loss or corruption. Regular backups are a critical cybersecurity countermeasure, enabling organizations to restore data and systems swiftly in the event of a cyber incident, such as ransomware attacks or system failures.

2.2 Maritime Systems

Maritime systems on-board ships are a comprehensive grasp of various interconnected components and technologies crucial for safe and efficient maritime operations. They are mainly divided into two categories, the IT (Information Technology) and OT (Operational Technology) systems. IT systems are components hosted in traditional computer systems, such as multi-purpose and network devices, which focus on data processing and communication. On the other hand, OT are components involved in monitoring and controlling various ship's functions while they deal specifically with the physical processes and machinery of the ship. Many OT systems are specially designed hardware and software utilizing various sensors and controlling mechanical components. Also, IT and OT systems are heavily integrated and overlap each other on the modern ship systems to improve the reliability and efficiency of the vessel's operations [15].

A typical architecture of OT systems is based on three layers. The Field device layer includes the sensors, valves, actuators and generally physical devices. The Field control layer includes Controllers and PLCs (Programmable Logic Controllers). Lastly, the Process monitoring layer includes a variety of different supervision systems, such as HMI (Human-Machine Interface), Application Servers or Workstations with specialised software.

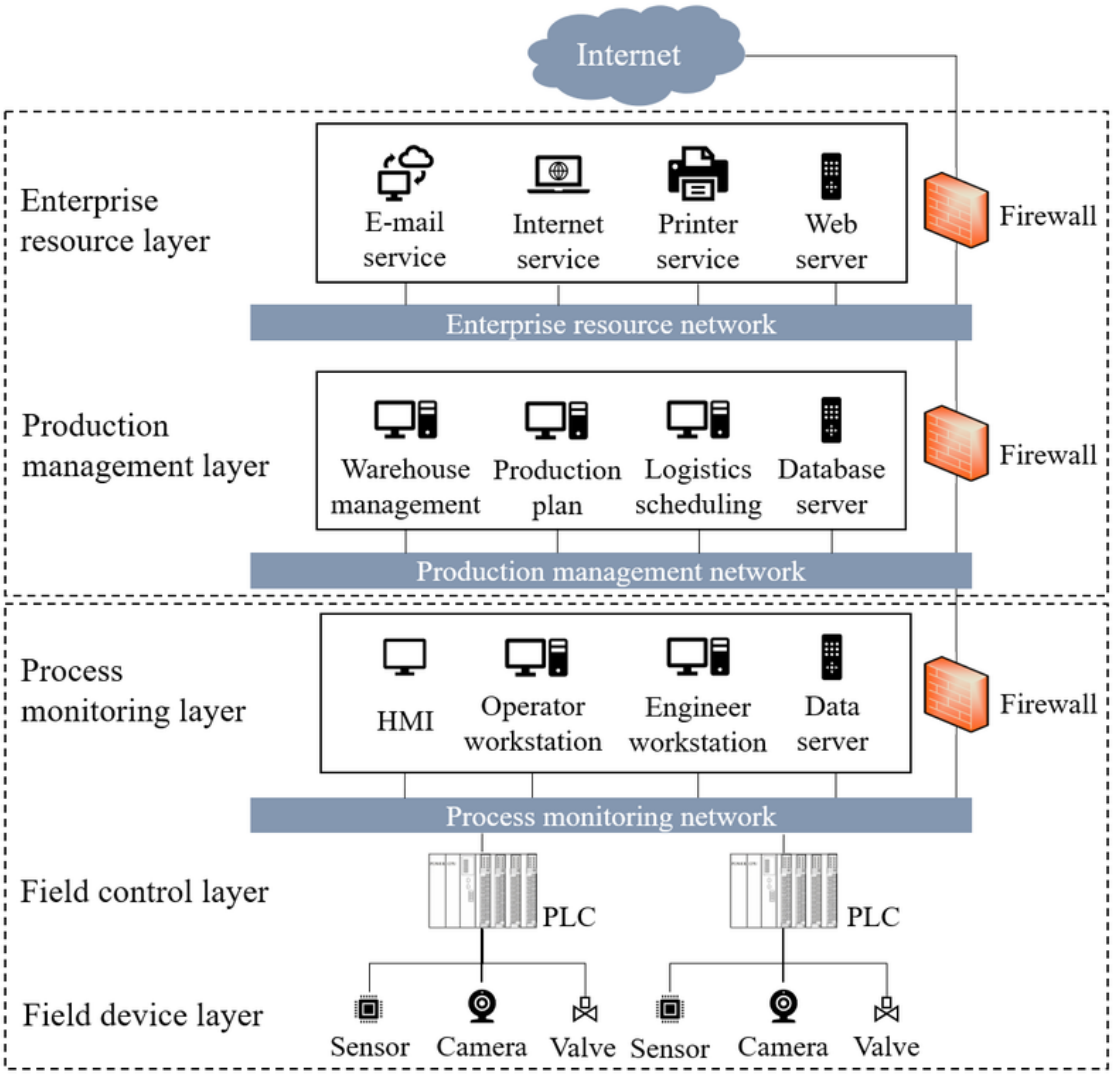

Figure 1: The typical architecture of industrial control systems.

Source: https://www.researchgate.net/figure/The-typical-architecture-of-industrial-control-systems_fig1_374565596

These systems combine electronic components, which are certainly the backbone of modern maritime systems, as well as mechanical, hydraulic, and pneumatic components that work in conjunction with electronics.

OT systems lie in how these electronic and non-electronic components are integrated and work together. Sensors collect data while electronics process it and may send commands to mechanical actuators to perform actions. Let us see a couple of examples below.

- An engine is a mechanical system, but it might be electronically controlled.
- Rudders that steer the ship are mechanical but use electronic signals for control.

In this thesis, we are going to focus on the second category, the OT systems. Not because the IT systems are better covered by the literature nor are they less important. But the IT systems are common to all industries and organizations. Research in computer science, software engineering, and cybersecurity heavily focuses

on IT systems. Instead, OT systems are proprietary for specific purposes, with closed architectures and limited access to them for research and documentation. As such, they are a perfect candidate of focus for our thesis such that we can close this main research gap.

2.2.1 OT Systems and Their Functionalities

In the complex ecosystem of maritime operations, ships OT systems play a pivotal role and consist of a variety of components. Each system is dedicated to optimizing performance, and safety as well as improving navigational accuracy. At the heart of safe maritime navigation lie advanced navigation systems designed to ensure that their navigation is carried out with the highest precision and safety. Equally important are Propulsion, Machinery and Power Management Systems, which control engines, propulsion, fuel consumption and overall efficiency. The backbone of safety on board the ship is the Safety and Emergency Management systems, including fire detection and suppression systems. Communication Systems act as an essential pipeline for operational command, security and emergency response, including satellite communications, radio and internet access. Cargo Handling and Management Systems for commercial vessels are core to operations and utilize advanced technologies to efficiently load, unload and manage cargo. Together all these components, form an integrated network and are essential for the smooth operation of modern ships, emphasizing the importance of OT in the maritime industry.

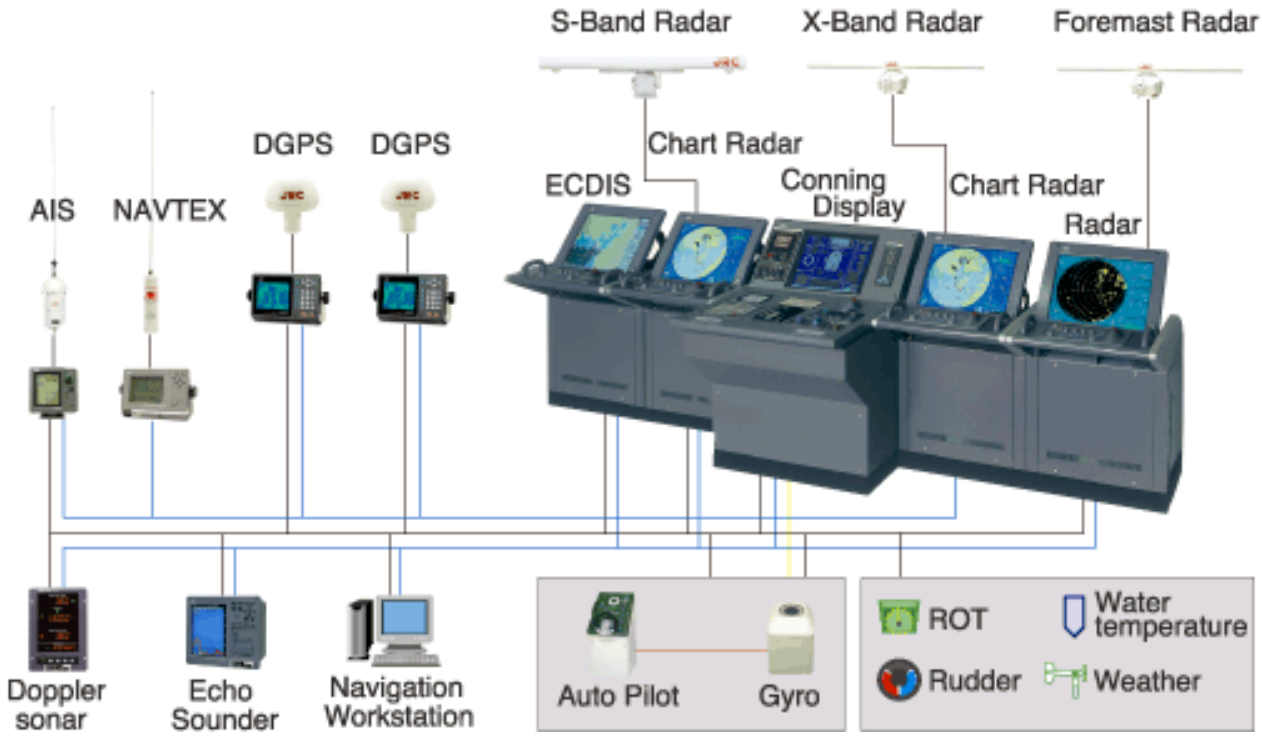

Figure 2: Bridge integrated system

Source: http://maritimeknowledge.blogspot.com/2015/12/ibsintegrated-bridge-system.html

2.2.1.1 Navigation Systems

2.2.1.1.1 Global Navigation Satellite System (GNSS)

Description: GNSS is a satellite-based navigation system providing geolocation and time information to a GNSS receiver anywhere on or near the Earth where there is an unobstructed line of sight to satellites. It can connect to international satellite navigation systems that include systems like the United States' GPS, Russia's GLONASS, Europe's Galileo, and China's BeiDou, among others.

Functionality: It is crucial for determining the ship's precise location, speed, and direction, forming the basis for navigational decisions and route planning. GPS data feeds into various other systems, such as the Electronic Chart Display and Information System (ECDIS), Automatic Identification System (AIS), and radar, ensuring accurate navigation and collision avoidance. [16], [17], [18]

2.2.1.1.2 Automatic Identification System (AIS)

Description: AIS is an automatic tracking system that uses transponders on ships and is used by vessel traffic services (VTS). Ships broadcast their position, identification, course, and speed.

Functionality: AIS operates by automatically exchanging a variety of ship data, such as identification, position, course, and speed, with nearby ships and AIS base stations, utilizing a system of VHF (Very High Frequency) radio transmissions. AIS data is displayed on ECDIS and radar screens, providing a comprehensive overview of traffic situations. It also integrates with GPS to ensure accurate position reporting. [19], [20]

2.2.1.1.3 Radar

Description: Radar systems emit radio waves to detect objects and their positions relative to the ship. They are essential for navigating through poor visibility conditions and avoiding collisions.

Functionality: Radar helps in identifying nearby ships, landmasses, and navigational hazards, especially in fog, rain, or at night. Radar information is used in conjunction with AIS and ECDIS to enhance situational awareness. It can also interface with the ship's automatic radar plotting aids (ARPA) for tracking and collision avoidance [21].

2.2.1.1.4 Electronic Chart Display and Information System (ECDIS)

Description: ECDIS is a computer-based navigation information system that complies with IMO[1] and can be used as an alternative to paper nautical charts. It integrates electronic navigational charts (ENC) with GPS and other navigational sensors to display the ship's position and navigational information.

Functionality: ECDIS enhances navigational safety by providing continuous, real-time information regarding the ship's position relative to land, navigational hazards, and maritime traffic. It integrates with GPS, radar, and AIS to provide a comprehensive navigational picture. ECDIS also connects with the ship's propulsion and steering systems for route planning and execution [22].

[1] https://www.imo.org/en/OurWork/Safety/Pages/ElectronicCharts.aspx

2.2.1.1.5 Gyrocompass

Description: A gyrocompass is a type of non-magnetic compass which is based on a fast-spinning disc and the rotation of the Earth to automatically find the geographical direction.

Functionality: Unlike magnetic compasses, gyrocompasses are not affected by external magnetic fields, providing accurate heading information crucial for navigation and autopilot systems. The gyrocompass is interconnected with autopilot systems, ECDIS, and radar, providing essential heading information that aids in navigation and steering [23].

2.2.1.1.6 Echo Sounder

Description: An echo sounder is a sonar device used to measure the depth of water beneath a ship by sending sound pulses down in the water. The time it takes for the echo to return is used to calculate the depth.

Functionality: They are crucial for preventing groundings and for navigating through shallow waters [24].

2.2.1.1.7 Long Range Identification and Tracking (LRIT)

Description: LRIT enables global identification and tracking of ships by transmitting their identity, location, date, and time every 6 hours to LRIT Data Centers, which then distribute the data to authorized parties.

Functionality: LRIT is vital for maritime security and safety, enabling competent authorities to track and monitor the movements of ships travelling through their waters or globally, aiding in search and rescue operations as well as in monitoring international compliance with maritime regulations. LRIT integrates with global satellite communication systems like Inmarsat C for transmitting its signals [25].

2.2.1.1.8 Speed Log

Description: A speed log measures the speed of a ship through water or over the ground. There are several types of speed logs, including electromagnetic, Doppler, and pressure tube systems, each using different methods to calculate speed.

Functionality: Speed information is critical for navigation, enabling accurate travel time estimates, efficient fuel consumption, and the execution of time-sensitive manoeuvres [26].

2.2.1.1.9 Autopilot

Description: Autopilot systems, also known as automatic steering, control the path of a ship without constant 'hands-on' correction by a human operator. They use the ship’s gyrocompass for heading information and are programmed to follow a set course.

Functionality: Autopilots reduce the workload on the ship's crew, especially during long voyages across open water, and improve fuel efficiency by maintaining a steadier course than manual steering. Autopilot systems are integrated with navigation systems, such as the GPS and gyrocompass to ensure accurate course following [27].

2.2.1.1.10 Integrated Bridge Systems (IBS)

Description: IBS is a combination of systems which are interconnected in order to allow centralized access to sensor information or command/control from workstation. This consolidates various navigational and operational systems on-board a ship onto a single user interface.

Functionality: The IBS interconnects many Navigation and Propulsion systems by monitoring functions on the ship's bridge. It typically integrates navigation systems, such as ECDIS, AIS, and GPS along with control systems for engines and steering gear. It can include integration with the Voyage Data Recorder (VDR) for recording navigational information, as well as radar and communication systems to ensure comprehensive situational awareness and control [28].

2.2.1.2 Propulsion, Machinery and Power Management Systems

2.2.1.2.1 Engine Control System (ECS)

Description: The main engine system of a ship includes the main propellers and associated controls. It is designed to convert fuel energy into mechanical energy to move the ship.

Functionality: It directly determines the ship's speed, manoeuvrability, and overall operational efficiency. Optimal management of the propulsion system ensures fuel economy and minimizes emissions. Interacts with the Navigation System for speed and course adjustments, the Fuel Management System for optimizing fuel usage, and the Exhaust Gas Cleaning Systems (Scrubbers) to comply with environmental regulations [22].

2.2.1.2.2 Alarm and Monitoring System (AMS)

Description: AMS comprises a central processing unit connected to multiple sensors and detectors placed throughout the ship. These sensors monitor a wide range of operational parameters, such as propulsion, fuel consumption, tank levels, temperature and pressure in critical areas, electrical systems status, and safety systems functionality.

Functionality: AMS provides real time monitoring, constantly tracks the operational parameters of machinery, structural integrity (like water ingress and hull stresses), navigational equipment, and safety systems. When parameters deviate from predefined safe limits, the AMS triggers visual and audible alarms to alert the crew. AMS is integrated with almost all other systems on-board the ship like IBS and ECS [29].

2.2.1.2.3 Power Generation and Distribution Systems

Description: This encompasses diesel generators, switchboards, transformers, and distribution panels that provide electrical power for the ship's operational and living needs.

Functionality: Ensures the availability of electrical power for critical systems like navigation, communication, cargo operations, and crew welfare, thus maintaining operational capabilities and safety [30].

2.2.1.2.4 Fuel Management Systems

Description: These systems manage the storage, treatment, and delivery of fuel to the engines and boilers, including fuel purification, viscosity control, and transfer pumps.

Functionality: Essential for ensuring that the fuel supplied to the engines is at the correct temperature and cleanliness, optimizing combustion efficiency, and meeting emissions standards. Works closely with the Exhaust Gas Treatment Systems to ensure emissions compliance and with the Engine Management System for adjusting fuel delivery based on engine load and operating conditions. It is highly integrated with virtually

all shipboard systems for data sharing and coordinated control, especially with the Bridge Integrated Control System (BICS) for information display and operational oversight [31].

2.2.1.2.5 Exhaust Gas Cleaning Systems (Scrubbers)

Description: Scrubbers are installed to remove harmful components (like sulphur oxides) from the ship's engine and boiler exhaust gasses before they are released into the atmosphere.

Functionality: Vital for complying with international regulations on sulphur emissions protecting environmental and human health. Directly connected to the Main Propulsion and Power Generation Systems [32].

2.2.1.3 Communication Systems

2.2.1.3.1 Satellite Communication (SATCOM)

Description: Utilizes satellites to provide voice, fax, internet, and data communication services globally, including FBB (Fleet Broadband) and VSAT (Very Small Aperture Terminal).

Functionality: Enables global communication for ships, critical for operational communication, weather updates, and emergency response. Integrated with navigation systems for receiving weather and navigational updates, and with the ship's computer systems for email and internet access [33].

2.2.1.3.2 HF and MF Radios

Description: HF and MF radios offer longer-range communication than VHF and are used for both routine and distress communications over hundreds or thousands of miles.

Functionality: They are important for trans-oceanic communication and as part of the GMDSS for distress alerting and safety communication. Also, HF/MF radios can interface with email and fax systems via modems [34].

2.2.1.3.3 Global Maritime Distress and Safety System (GMDSS)

Description: An internationally agreed-upon set of safety procedures, types of equipment, and communication protocols used to increase safety and make it easier to rescue distressed ships, aircraft, and people.

Functionality: The cornerstone of maritime safety, facilitating automatic distress alerting and location for ships in distress, and coordinating search and rescue efforts. Integrates with satellite communications like Inmarsat C and radio transmission to disseminate safety information [16], [35].

2.2.1.4 Cargo Management Systems

2.2.1.4.1 Cargo Control System

Description: The Cargo Management System on a ship is a specialized software and hardware solution designed to optimize the handling, storage, and monitoring of cargo. It encompasses various systems for different types of cargo, such as containers, bulk cargo, liquids, and refrigerated goods, ensuring their safe and efficient transport.

Functionality: This system functions differently from each vessel type, but has the same scope: to monitor and maintain optimal conditions for a specific cargo. The controllers, sensors, and actuators for ventilation, heating, and cooling systems fall under cargo control OT systems [36].

2.2.1.4.2 Ballast Water Management System (BWMS)

Description: The Ballast Water Management System is designed to manage and treat ballast water in ships, which is used to maintain stability and structural integrity. The system ensures that ballast water has the needed treatment to prevent the transfer of invasive aquatic species.

Functionality: The BWMS controls the pumping of ballast water in and out of tanks to maintain ship stability during loading, unloading, and transit. Also, when a vessel pumps in tanks water may have organisms. These organisms can be transferred from one territory to another and be harmful. To prevent this, BWMS filters and treats ballast water before it is discharged to remove or neutralize organisms [37].

2.2.1.5 Safety and Emergency Management systems

2.2.1.5.1 Fire Detection and Suppression System (FDSS)

Description: The Fire Detection and Suppression System acts as the ship's first line of defence against onboard fires. Depending on the system design, the FDSS can take automated actions. It might activate water sprinkler systems in designated areas to extinguish the flames directly. Fire dampers can automatically slam shut, closing ventilation ducts to prevent the spread of smoke and heat. Fire doors can also be triggered to isolate compartments and contain the fire within a specific zone.

Functionality: It employs a network of sensors, controllers, and actuators to effectively detect, contain, and extinguish fires. Smoke detectors, heat detectors, and flame detectors are strategically placed throughout the vessel to identify fire outbreaks at the earliest stages. When a sensor detects a fire, it transmits a signal to the fire control panel. This intelligent panel analyses the data, determines the location and severity of the fire, and triggers alarms to alert the crew [38].

2.2.1.5.2 Voyage Data Recorder (VDR)

Description: The Voyage Data Recorder (VDR) functions as a "black box" for ships, continuously recording critical navigational and operational data. It captures information like position, speed, heading, radar data, audio communications from the bridge, and various machinery parameters.

Functionality: In the event of an incident, the VDR preserves a detailed record of the events leading up to it. This data is invaluable for accident investigations, helping to determine the cause of the incident, assign responsibility, and ultimately improve safety measures for future voyages [39].

2.2.1.5.3 Closed-Circuit Television (CCTV)

Description: Closed-Circuit Television (CCTV) systems on-board ships consist of strategically placed cameras and monitors, providing real-time surveillance of various areas, both internal and external. This includes engine rooms, cargo holds, passenger areas, and the ship's perimeter.

Functionality: They can help monitor for hazards, such as fire, flooding or piracy incidents allowing for early detection and response. Additionally, they can observe machinery operation and identify potential issues before they escalate into emergencies [40].

2.2.2 Advantages and Disadvantages

The advantages of the maritime systems are numerous while sophisticated electronic systems contribute to the efficiency, safety, and environmental soundness of maritime operations. However, it is important to acknowledge that these systems also come with limitations. Overreliance can lead to complacency, and dependence on external signals makes them susceptible to disruption. Understanding both the strengths and weaknesses of maritime systems is critical to ensure safe and successful operations.

Below we will see the main advantages and disadvantages of each system.

Navigation Systems:

- Advantages:
    - Increased accuracy and precision in positioning and navigation.
    - Improved situational awareness for collision avoidance.
    - Access to real-time weather and hazard information.
- Disadvantages:
    - Overreliance on technology can lead to complacency and reduced navigational skills.
    - System failure can be critical in situations requiring manual navigation.
    - Complex systems can be challenging to troubleshoot for non-technical crew.
    - Dependence on accurate electronic charts and updates.

Propulsion, Machinery, and Power Management Systems:

- Advantages:
    - Increased efficiency in fuel consumption and reduced operating costs.
    - Improved engine performance and reliability for smoother operation.
    - Automated monitoring and control systems for reduced human error.
    - Real-time data on engine health and diagnostics for preventive maintenance.
- Disadvantages:
    - They require highly skilled personnel for operation and maintenance.
    - System failures can lead to loss of propulsion and power, creating critical situations.
    - Reliance on spare parts and technical expertise, potentially causing delays at sea.

Communication Systems:

- Advantages:
    - Reliable communication with shore and other vessels for emergencies and coordination.
    - Improved crew communication within the ship for efficient operation.
    - Access to global communication networks for weather updates, news, and support.
    - Facilitation of remote diagnostics and troubleshooting by shore side experts.
- Disadvantages:

- System failure can disrupt critical communication during emergencies.
- Reliance on satellite networks can be affected by weather conditions or technical issues.
- Dependence on trained personnel to operate and maintain communication equipment.

Cargo Management Systems:

- Advantages:
  - Improved cargo stowage planning for optimal stability and weight distribution.
  - Real-time cargo tracking and inventory management.
  - Enhanced safety through monitoring cargo weight and distribution.
  - Increased efficiency in loading and unloading operations.
- Disadvantages:
  - System errors can lead to improper cargo stowage, impacting stability.
  - Reliance on accurate data entry for effective system operation.
  - Limited functionality for non-standard or specialized cargo.

Safety and Emergency Management systems:

- Advantages:
  - It can identify fires in their incipient stages, well before they become visible.
  - Early fire detection provides ample warning for the crew to evacuate and take necessary safety measures, minimizing the risk of injuries or fatalities.
  - Prompt fire suppression helps contain the flames and limits damage to the ship's structure, equipment, and cargo.
- Disadvantages:
  - It can sometimes generate false alarms due to malfunctioning sensors.
  - Accidental activation of water sprinkler systems or CO2 can lead to damage or life loss.

The above marine systems exchange data between them, either information or commands. This data is processed for the immediate execution of processes or decision-making without delays, errors and immediately. By extension, we can say that maritime systems are increasingly adopting fog computing architectures due to their distributed nature and the need for real-time processing. Fog computing offers several advantages that are particularly relevant to maritime environments. First, it offers reduced latency by processing data closer to its source, so it can provide faster response times for critical maritime operations. Second, it enables bandwidth conservation which helps minimize the amount of data that needs to be transmitted to centralized cloud servers. This is quite beneficial in maritime settings where connectivity can be limited or expensive. Third, it can improve reliability because fog computing allows for continued operation even when internet connectivity is intermittent, which is common at sea. Fourth, it can enhance security when processing sensitive data locally while it reduces the risk associated with transmitting information over long distances. Last but not least, real-time analytics as supported by fog computing can enable quicker decision-making based on immediate data processing, which is crucial for navigation and safety systems.

3

Literature Review Methodology

3.1 Main Research Goals

The main goal of the current thesis is to supply a thorough analysis of maritime cybersecurity and its scope. For this purpose, a systematic review was conducted so as to address in depth the following topics (mapping actually to respective research questions) related to maritime cybersecurity:

- *What are the currently identified cybersecurity issues in maritime systems and how can they be categorized?* An analysis and classification of the currently identified cybersecurity issues presented in maritime systems will be covered in Chapter 4.
- *How have the above-mentioned issues been exploited in real-life attacks?* Examples of real-life attacks on maritime systems through the exploitation of the aforementioned issues will also be covered in Chapter 4.
- *Which countermeasures have been identified to address the aforementioned issues? Furthermore, which countermeasures can be considered the best?* A detailed classification and analysis of the countermeasures for cybersecurity in maritime systems as suggested in the current literature is presented in Chapter 5. In addition, based on such classification/analysis, as well as specific objective criteria, a comparison of the reported countermeasures is also disclosed at the same chapter to identify the most suitable countermeasures to be integrated into the cybersecurity plan of the maritime systems.
- *Which risk management techniques can be applied to address maritime cybersecurity issues?* The risk management techniques, which can be globally integrated to address the maritime cybersecurity issues are covered in Chapter 6.
- *Which research gaps have been identified and how they can be addressed based on the current literature?* Identification of the research gaps, as understood through the available literature and as unveiled by the aforementioned analysis, as well as promising research directions for addressing these gaps are covered in Chapter 7.

3.2 Literature Search

The literature considered relevant during the drafting of the thesis was mainly sourced through the Google Scholar, Scopus and Web of Science search engines since such sources are well-established in many research

areas and jointly cover well the available literature. For the purpose of identifying the articles/publications relevant to the thesis scope, the search methods that were implemented in this thesis focused on advanced search by applying a suitable search pattern over the aforementioned engines which was relevant to the aforementioned questions and thus to this thesis goal. The hereunder keywords were utilized, as standalone keywords or in combination, during the research process of the thesis: cybersecurity, maritime systems, AIS, automation systems, boilers, cargo monitoring systems, DGPS, ECDIS, GMDSS, GPS, gyrocompass, IBS, main engines, radar, steering gear, VHF, threats, vulnerabilities, attacks, countermeasures, attack scenarios, risk management, gaps. The aforementioned search pattern utilised is defined as follows: *C1 && C2 && C3*, where *C1* indicates the security type concerned and maps to (cybersecurity), *C2* defines the object being protected and maps to (AIS || automation systems || boilers || cargo monitoring systems || DGPS || ECDIS || GMDSS || GPS || gyrocompass || IBS || main engines || radar || steering gear || VHF|| maritime systems) while *C3* concerns the security concepts relevant to the thesis and maps to (threats || vulnerabilities || attacks || countermeasures || attack scenarios || risk management || gaps).

3.3 Publication Filtering

Due to the generic nature of the aforementioned keywords, the search engine results were carefully examined and filtered so as to utilise only those publications that are utmost relevant to the current thesis. Firstly, inclusion criteria were applied concerning the type of publication (i.e., published thesis, scientific article, research paper, and technical reports), publication source, as well as year of publication, mainly considering scientific articles and research papers published during the last five years on IT and/or maritime related journals and conferences. Naturally, the language of the publication was also taken into consideration; in the context of this thesis, only publications drafted in English were considered relevant due to the ability of the authors to fully understand text/content in only this language, which is the most established one for academic publications. Additionally, in the context of published articles/papers, only peer-reviewed ones were selected for obvious quality, objectivity, and best academic practice reasons.

Furthermore, the relevance of the publication was examined through its available, high-level information, such as the article metadata, keywords as well as the table of its contents (if exists) plus its introduction and abstract sections. In case relevance was difficult to judge based on the aforementioned knowledge, the full content of the publication was examined. It is estimated that approximately 280 articles were assessed during this procedure, out of which only 106 were flagged as ‘relevant’.

Next, the quality of the publication was examined. In particular, the content of the retrieved publication was carefully examined so as to only rely on relevant information of high quality, taking into consideration the following factors:

- *the writing quality*: well-written and effortlessly comprehensible articles were preferred compared to poorly-written articles
- *the research methodology followed*: extensively researched publications with proper contributions suitably assessed were preferred against publications lacking such research methodology
- *the publication’s objectivity*, evaluated based on how objective is the comparison of the publication's contribution with the state-of-the-art, the objectivity and suitability of the evaluation measures, the consideration of state-of-the-art approaches in the evaluation and the existence of a "threats to validity" section.

Out of the 106 publications flagged as 'relevant' through the initial validation procedure, only 80 publications were finally selected for the purposes of this thesis based on this last filtering step.

3.4 Quantitative Analysis

Out of the 80 finally selected publications, 21% are related to already published MSc/PhD thesis, 62% are published in scientific journals, 11% are technical reports and TRANSAV articles published by universities, while 6% are published in conference/workshops.

Furthermore, the main publications relate to the following publishers: universities with 39% of the publications, MDPI with 15% of the publications, IEEE with 5% of the publications, Springer with 4% of the publications, Cambridge University Press represents 2% of the publications, while other publishers constitute 35% of the publications.

4 *Cybersecurity Issues in Maritime Systems*

While the shipping industry advances, the surge in cyber-attacks targeting this sector has become a critical concern. These attacks are not limited to mere data theft or financial loss but extend to the very heart of maritime operations, the OT systems. Unlike IT systems, where the primary concerns are confidentiality, integrity, and availability of information, OT systems are integral to the physical operations of ships. The compromise of OT systems poses unique and severe risks, including financial damage, environmental disasters, ship damage, and even loss of life. Thus, we move from pure security concerns to protection and safety concerns as well [1], [41], [42].

Given the substantial literature on the cybersecurity of IT systems, we will specifically focus on the vulnerabilities and threats targeting OT systems within the maritime domain. OT, the backbone of ship operations, controls the navigation, propulsion, and communication systems. The compromise of these systems can lead to dire consequences. For example, a breach in the Navigational OT systems could disrupt the vessel's navigation system, leading to potential collisions or grounding. Maritime cybersecurity: are on-board systems ready?

Similarly, attacks on the communication systems could sever the crucial link between the ship and the shore, leaving the vessel isolated in case of emergencies.

Therefore, it is imperative to focus on enhancing the cybersecurity posture of OT systems within maritime operations. This involves not only implementing robust security measures but also fostering a culture of cybersecurity awareness among the maritime workforce. The subsequent sections will delve into the vulnerabilities of OT systems, the nature of cyber threats targeting these systems, and the strategies required to mitigate such risks effectively. Our goal is to highlight the critical need for a solid cybersecurity framework that safeguards OT systems against emerging cyber threats, thereby ensuring the safety, security, and continuity of maritime operations in an increasingly digitized world [43], [44].

4.1 Classification and analysis of vulnerabilities

The vulnerabilities in maritime technologies can be classified by their type into several categories, including software vulnerabilities, network vulnerabilities, physical vulnerabilities and human factor vulnerabilities.

Software vulnerabilities encompass issues like software bugs, flaws in the software code, use of unreliable/insecure libraries. These vulnerabilities can lead to malfunctions, inaccurate data processing, insecure protocols, and unauthorized access. The non-consideration or improper application of secure programming practices of OT systems is also an issue that can leave such systems vulnerable to exploitation.

This issue might involve hardcoded credentials, weak default passwords for critical systems, disabled security features on equipment.

Network vulnerabilities are weaknesses in the communication networks connecting OT systems that create opportunities for attackers to intercept data, disrupt operations, or inject malicious code. These could involve insecure communication protocols between bridge systems and other equipment, open ports on network devices that attackers can exploit, or (implementation/design) vulnerabilities in satellite communication protocols used for data transmission [45].

Hardware vulnerabilities are weaknesses within physical components of a system that attackers can exploit to gain unauthorized access, disrupt operations, or steal data. The attackers can exploit vulnerabilities such as exposed physical ports (USB, LAN), the system can use a legacy hardware with known vulnerabilities or use physical equipment for tampering.

The human factor plays a critical role in maritime cybersecurity. Crew members can be susceptible to social engineering attacks targeting shipboard systems, misinterpret information displayed on critical equipment, or operate systems incorrectly. These risks are amplified by weak physical access controls, poor password policies, and a lack of security awareness training [1], [46].

Furthermore, we are going to give a short description of each vulnerability, to provide a comprehensive understanding of how it can affect a system [47], [48], [49], [50], [51], [52].

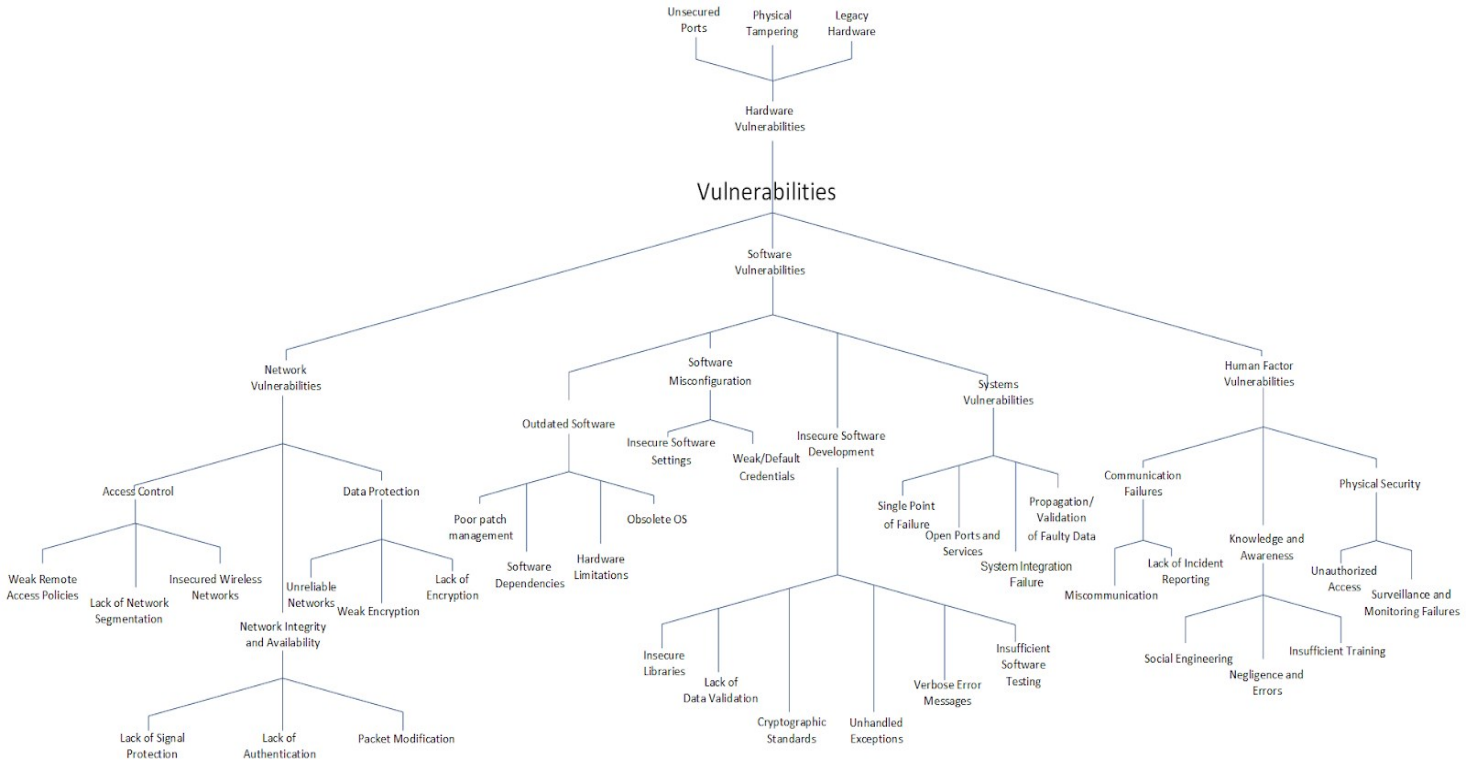

Figure 3: Vulnerabilities hierarchy tree

4.1.1 Software Vulnerabilities

- *Outdated Software*: Outdated software refers to software applications or operating systems that are no longer receiving official updates and support from their developers or manufacturers. These updates are crucial for maintaining security, fixing bugs, and adding new features. Here's a breakdown of the key aspects
    - *Poor patch management*: Failure to identify, acquire, and install security patches in a timely manner leaves systems (encompassing the vulnerable outdated software) susceptible to known exploits.
    - *Obsolete OS*: Outdated operating systems are no longer supported by vendors and may have unpatched vulnerabilities.
    - *Software Dependencies*: Software (new or old) may depend on other outdated components, creating a chain of dependency that prevents updates and patch application.
    - *Hardware Limitations*: Legacy hardware may not support newer software updates, requiring a complete system overhaul to maintain security.
- *Software Misconfiguration*: Software misconfiguration means the incorrect or suboptimal settings, parameters, or configurations within a software application or system that can lead to security vulnerabilities and potential exploitation.
    - *Insecure Software Settings*: This refers to configuration options in a software application or system that are set to values that weaken security or introduce vulnerabilities. These settings may be default values provided by the software vendor, or they may be custom settings that are configured incorrectly or insufficiently.
    - *Weak/Default Credentials*: This vulnerability refers to user accounts (typically administrative or privileged accounts) that have weak or default passwords. Weak passwords are easy to guess or crack using brute force or dictionary attacks.
- *Insecure Software Development*: This vulnerability refers to practices that lead to software with vulnerabilities. These vulnerabilities can be exploited by attackers to gain unauthorized access to systems, steal data, or disrupt operations.
    - *Verbose Error Messages*: Detailed errors (e.g., showing the whole stack trace) can provide attackers with insights into the database layout, software stack, or internal operations.
    - *Unhandled Exceptions*: These can cause software crashes or unintended behaviour, which might be exploited by attackers to conduct a denial of service attack.
    - *Cryptographic Standards*: Default settings that use weak or deprecated cryptographic standards can make encryption easy to break or not at all applied (e.g., by downgrading to protocol versions that exploit such weak standards).
    - *Lack of Data Validation and Cleansing*: This is the failure of software to adequately check, filter, and sanitize data received from external sources or user input before processing or storing it. It's a critical security flaw that can lead to other vulnerabilities.
    - *Insecure libraries*: This vulnerability refers mostly to third-party software components that contain vulnerabilities or are outdated. These libraries are often integrated into larger software applications to provide specific functionality or speed up development.
    - *Insufficient Software Testing*: This vulnerability refers to the inadequate or incomplete testing of software before deployment, leaving it vulnerable to errors, bugs, and security flaws.

- *System Vulnerabilities:* These are weaknesses inherent in the design, architecture, or overall operational practices of the system. These vulnerabilities are not isolated flaws in individual components but rather reflect broader issues that can increase the risk of multiple vulnerabilities.
    - *Single Point of Failure*: Systems that share critical resources, such as databases or network bandwidth, can be compromised at one point, which affects multiple systems reliant on these shared resources.
    - *Propagation/Validation of Faulty Data*: Errors in data from sensors or input systems can propagate through connected systems, leading to widespread operational issues.
    - *System Integration Failure*: When there are improper connections and interaction of different system components between systems. These can manifest as synchronization errors leading to data inconsistencies or interface misuse causing unexpected behaviour and flaws.
    - *Open Ports and Services*: Systems shipped with unnecessary open ports or services running by default can expose critical systems to network attacks.

4.1.2 Network Vulnerabilities

- *Access Control*
    - *Lack of Network Segmentation*: Inadequate separation between IT and OT environments.
    - *Weak Remote Access Policies*: Unrestricted or poorly secured remote access procedures create vulnerabilities.
    - *Insecure Wireless Networks*: Vulnerable to eavesdropping and unauthorized access.
- *Data Protection*
    - *Lack of Encryption*: Data is transmitted in plain text, allowing easy interception.
    - *Weak Encryption*: Encryption algorithms are weak or improperly implemented.
    - *Unreliable Networks/Protocols*: Transmission of data over insecure networks or using unreliable protocols, increasing the risk of data loss, interception, or corruption during transit.
- *Network Integrity and Availability*
    - *Lack of Signal Protection*: Lack of measures to protect communication signals from interference can lead to disruptions in network operations and potential data loss.
    - *Lack of Authentication*: Missing mechanisms to verify the origin and integrity of messages.
    - *Packet Modification*: Data packets are intercepted and altered in transit.

4.1.3 Hardware vulnerabilities

- *Unsecured Ports*: Most maritime systems have physical ports, such as USB and serial ports, for maintenance, communication with other devices and diagnostics. These ports can be exploited if not properly secured. Malicious actors could introduce malware through these ports or access sensitive data.
- *Legacy Equipment*: Older systems might still be using outdated hardware that has known vulnerabilities. These vulnerabilities may not have corresponding patches available, making the systems difficult to secure.
- *Physical Tampering*: Physical access to a system could allow attackers to tamper with hardware components. This could involve modifying firmware, installing eavesdropping devices, or even disabling critical safety features.

4.1.4 Human Factor Vulnerabilities

- *Knowledge and Awareness Issues*
  - *Insufficient Training*: Crew members may not be adequately trained in recognizing and mitigating security threats.
  - *Social Engineering*: Crew members may be tricked into revealing sensitive information or executing malicious actions through manipulation techniques.
  - *Negligence and Errors*: Human errors, such as incorrect settings adjustments or failure to follow protocols, can lead to serious security lapses.
- Physical Security
  - *Unauthorized Access*: Insufficient measures to prevent access to sensitive or critical areas by unauthorized personnel.
  - *Surveillance and Monitoring Failures*: Lack of proper surveillance or monitoring can allow security breaches to go unnoticed.
- Communication Failures
  - *Miscommunication*: Poor communication can lead to misunderstandings or misinterpretations of critical information, affecting decision-making processes.
  - *Lack of Incident Reporting*: Failure to report security incidents promptly can hinder effective response and exacerbate issues.

A significant concern for maritime OT systems lies in common vulnerabilities present in many systems. These weaknesses include outdated operating systems lacking vendor support, exposing them to unpatched vulnerabilities. Additionally, inadequate anti-virus protection and a lack of malware safeguards leave systems susceptible to malicious attacks. Furthermore, weak security configurations are widespread, with practices like ineffective network management, reliance on default administrator credentials, and a lack of network segmentation creating a breeding ground for attackers.

4.2 Classification and analysis of threats

Following the literature we can classify the threats generally on the cybersecurity landscape by type. In particular, threats in maritime cybersecurity can generally be divided into two types: intentional threats and unintentional threats [11].

Intentional threats, also known as malicious threats, are deliberate attempts to cause harm or disrupt the operation of maritime OT systems. These threats are perpetrated by actors with a specific goal in mind, ranging from financial gain to causing physical damage. On the other hand, unintentional threats encompass actions or events that disrupt or damage OT systems on ships without any malicious intent. They can arise from human error, environmental factors, or equipment malfunction.

Also, in the maritime cybersecurity, various threat actors (also known as threat agents) with different motivations pose significant threats and have a significant impact on the security environment [14]. The motivations driving these malicious activities in the maritime domain include financial motives, interference with essential operations and threats to the safety of human life. These actors range from the incidental to the highly deliberate, including activists, criminals, states, state-sponsored groups and terrorists. Accidental actors can inadvertently compromise systems by, e.g., using infected USB devices, without malicious intent. Potential criminals, including unhappy employees, may aim to disrupt operations, attract media attention or

damage reputations, sometimes driven by a desire for revenge. Criminals may be tempted by financial rewards and engage in activities, such as commercial or industrial espionage to obtain valuable data or gain a competitive advantage. Criminals relish the challenge of penetrating cybersecurity measures and reaping financial or reputational rewards for successful penetration. At a more serious level, government agencies, state-sponsored organizations and terrorists carry out attacks based on political or ideological motivations [5], [53], [54], [55], [56].

Table 1: Threat actors and potential threats

Actor Type	Threats
Accidental actors	· Unintended threats arising from human error or knowledge gaps
Criminals	· financial gain · commercial espionage · industrial espionage
Activists	· revenge · disruption of operations · media attention · reputational damage
States - State-sponsored Organizations - Terrorists	· damage national infrastructure · espionage · financial gain · commercial espionage · industrial espionage · reputational damage

All mentioned threat actors try to identify and exploit the ship's systems vulnerabilities to achieve their purpose. In particular, the threats can penetrate, disrupt or damage a system source from its vulnerabilities. As a consequence, we classify the threats based on the root vulnerability categories (see Figure 4). Certainly, some threats, e.g., spoofing, can partially fall under both software and network vulnerabilities depending on the specific technique used.

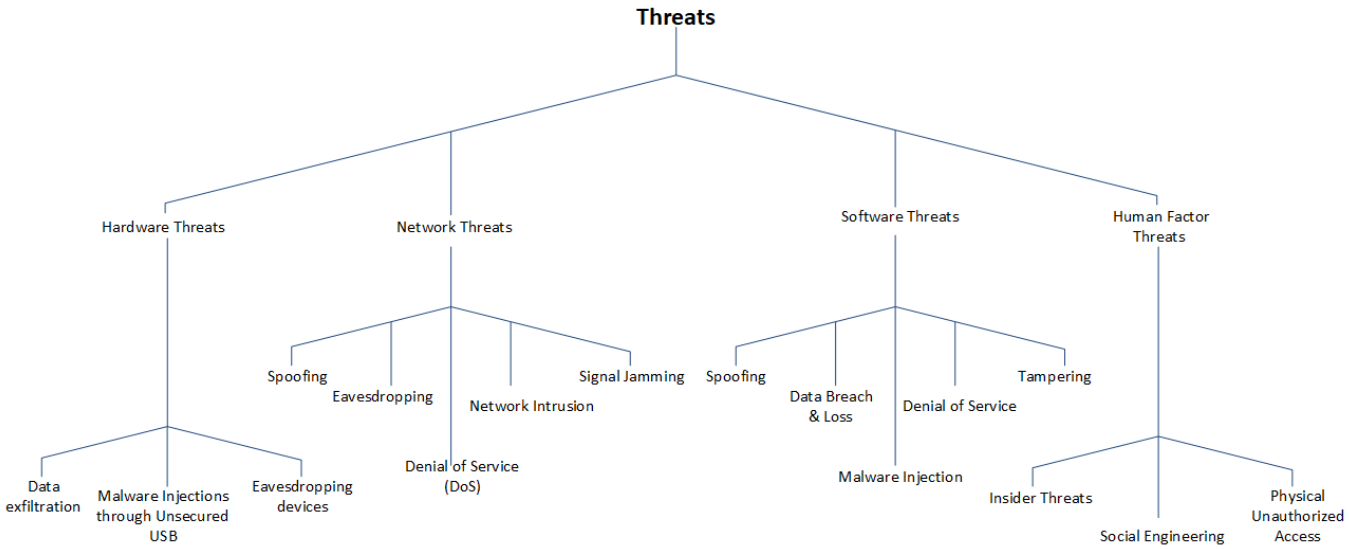

Figure 4: Threats hierarchy tree

4.2.1 Software Threats

Software vulnerabilities create openings for various threats to exploit shipboard OT systems. Additionally, they highlight the importance of maintaining up-to-date software, patching systems diligently, and implementing strong authentication measures.

Malware Injection

Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network. This can include viruses, worms, Trojan horses, ransomware, and spyware. Malware can be introduced into a ship's systems through malicious email attachments, infected USB drives, compromised software updates, or by exploiting security vulnerabilities in software. Once installed, malware can disrupt operations, steal sensitive data, or allow attackers to gain remote control over ship systems.

Legacy software and unsupported operating systems with unpatched vulnerabilities can be targeted for malware installation. The consequences of malware depend on its type, potentially causing data breaches, system disruptions, or even safety hazards.

Data Breach & Loss

Data breaches occur when unauthorized access to sensitive information stored on a system is gained. This information could include navigation data, sensor readings, crew information, or cargo details. Data breaches can occur due to unpatched vulnerabilities that allow attackers to steal data stored on systems. Also, insufficient authentication measures can make it easier for attackers to gain unauthorized access and steal data.

Spoofing

Spoofing often exploits vulnerabilities in authentication mechanisms. It is a fraudulent act where a person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Tampering

Tampering refers to the deliberate alteration or manipulation of system operations, software, or data, often to disrupt operations or steal sensitive information. It encompasses changes made to software configurations, code injections, or physical interference with hardware devices.

Denial of Service

Denial of Service (DoS) is a security threat aimed at disrupting the normal functioning of a targeted system. This threat is realised by attacks which attempt to overwhelm a server with a significant volume of requests so as to reduce its availability as well as its ability to serve legitimate requests. Such attacks exploit specific vulnerabilities in the system, such as bugs in the software that cause it to consume excessive resources or crash when processing certain requests.

4.2.2 Network Threats

Network vulnerabilities create another critical attack vector for malicious actors targeting shipboard OT systems. The interconnected nature of maritime systems, including onboard and off-shore platforms, increases the attack surface and potential impact of cyber threats [11].

Denial of Service (DoS)

Similar to software threats, Denial of Service (DoS) attacks aim to disrupt service. From a network perspective, these attacks flood a network or its resources with illegitimate requests, rendering them unavailable to legitimate users.

Eavesdropping

Eavesdropping involves intercepting communication traffic on a network without authorization. Attackers can steal sensitive information like navigation data, crew communication, or cargo details. Weak encryption standards or insecure network configurations and protocols can facilitate eavesdropping on communication.

Network Intrusion

The threat here is that the attackers can gain unauthorized access to a network to steal data, disrupt operations, or sabotage systems. Attackers can exploit vulnerabilities in unpatched network devices like firewalls or routers to gain access to the network. Inadequate authentication protocols for network access can be exploited to gain such unauthorized entry.

Spoofing

Spoofing as a network threat could involve spoofing IP or MAC addresses or other identifiers to gain unauthorized access or manipulate network traffic.

Signal Jamming

Signal jamming involves deliberately interfering with communication signals. Threat actors might use specialized equipment to jam radio frequencies or GPS signals, disrupting critical communication channels.

4.2.3 Hardware Threats

Malware Injections through Unsecured USB

Malware can be injected by exploiting unsecured USB ports to introduce malware or malicious code into the systems. USB drives can be used as vectors for delivering various types of malware, such as viruses, worms, Trojans, or rootkits.

Eavesdropping devices

Someone may attempt to physically install eavesdropping devices, such as RF transmitters, microphones or network taps to intercept and capture sensitive information or communications.

Data exfiltration

Attackers with physical access to maritime systems or networks may exploit hardware vulnerabilities to exfiltrate sensitive data, such as operational data, navigation information, or confidential documents.

4.2.4 Human Factor Threats

Even the most robust software and network security can be compromised by human error or manipulation. Literature highlights the importance of understanding the human factor in maritime cybersecurity and the need for effective training programs to mitigate these threats [46].

Social Engineering

Social engineering attacks go beyond the scope of phishing emails and delve deeper into exploiting human psychology and social interactions to gain unauthorized access to systems or information. Attackers employ various tactics to manipulate trust, bypass security measures, and achieve their goals.

Insider Threats

Insider threats pose a significant risk to shipboard OT systems. Unlike traditional cyberattacks that originate from external sources, insider threats involve malicious activities by authorized personnel who already have legitimate access to critical systems and data. These threats can be particularly dangerous because they can bypass many security measures and operate with a level of trust that external attackers cannot achieve.

Physical Unauthorized Access

Physical unauthorized access occurs when an individual gains physical entry to areas containing shipboard OT systems or network components without proper authorization. This can lead to severe consequences, compromising the confidentiality, integrity, and availability of critical systems and data.

The following table presents an overview of the potential cyber threats to ship's maritime systems, categorized by the primary threat category. For each threat, the table details the exploited vulnerabilities, potential damages or consequences, and the specific OT systems that could be affected in order to understand the diverse range of the cyber threats, their underlying vulnerabilities and the potential effects.

Table 2: Known vulnerabilities and their effects

Threat	Category	Vulnerability	Effect
Malware Injection	Software	Outdated software / Poor patch management / Insecure software settings / Weak authentication mechanisms / Insecure software development / Insecure libraries	System disruption / Data theft / Remote system control / Safety hazards

Data Breach & Loss	Software	Unpatched vulnerabilities / Weak authentication / Lack of data validation / Insecure data handling	Unauthorized data access / Data integrity issues / Legal/regulatory implications / Financial losses / Reputational damage
Tampering	Software	Insecure configurations / Code injection vulnerabilities / Lack of input validation	Altered system behaviour / Unauthorized access / Data corruption / Safety hazards
Denial of Service (DoS)	Software/Network	Software bugs / Resource exhaustion / Protocol vulnerabilities / Lack of redundancy	Service disruption / System unavailability / Operational disruption
Eavesdropping	Network	Weak encryption / Insecure protocols / Unprotected communication channels	Data interception / Privacy violations / Intellectual property theft
Network Intrusion	Network	Unpatched network devices / Weak access controls / Inadequate network segmentation	Unauthorized access / Data theft / System manipulation / Sabotage
Spoofing	Software/Network	Weak authentication mechanisms / Lack of validation / Social engineering tactics	Unauthorized access / Data manipulation / System impersonation
Signal Jamming	Network	Vulnerable wireless protocols / Lack of signal protection	Communication disruption / Navigation disruption / Safety hazards
Malware Injection (Hardware)	Hardware	Unsecured USB ports / Physical access vulnerabilities	Malware propagation / Data exfiltration / Unauthorized system control
Eavesdropping Devices	Hardware	Physical access vulnerabilities / Lack of surveillance	Data interception / Privacy violations / Intellectual property theft
Data Exfiltration (Hardware)	Hardware	Unsecured removable media / Physical access vulnerabilities	Data theft / Potential extortion/blackmail / Loss of competitive advantage
Social Engineering	Human Factor	Lack of security awareness / Trust exploitation / Human psychology vulnerabilities	Unauthorized access / Data breaches / System disruption
Insider Threats	Human Factor	Excessive access privileges / Lack of monitoring / Disgruntled employees	Data theft / Sabotage / System disruption / Unauthorized access

Physical Unauthorized Access	Human Factor	Inadequate access controls / Lack of surveillance / Social engineering tactics	Hardware tampering / Data theft / System disruption / Malicious device installation

4.3 Classification and analysis of attack types

We classify and analyse the cyber-attacks in OT systems based on their target type (targeted or untargeted), the vulnerabilities that they concern and the OT system that they affect. The classification is given in the table below while the analysis of each attack follows after it [10], [57], [57], [58], [59], [60], [61].

Table 3: Mapping of attacks, vulnerabilities and affected systems

Attack	**Vulnerabilities**	**System**
Malware	Software & Human Factor Vulnerabilities	Shipboard IT and OT systems, including navigation systems (ECDIS), engine control systems, and communication networks.
Jamming/ Digital Radio Frequency Memory (DRFM)/ Blip enhancement.	Network Vulnerabilities	Radar, AIS, and other radio frequency-based communication and navigation systems.
Social engineering Phishing Attacks/ Spear Phishing/ Watering Hole Attack	Human Factor Vulnerabilities	All
Brute force	Software & Human Factor Vulnerabilities	Systems with login credentials
DoS	Software, Network and Human Factor Vulnerabilities	All systems
Man-in-the-middle	Software Vulnerabilities & Network Vulnerabilities	Ship-to-shore communication systems, on-board network communications, and satellite communications e.g. AIS, ECDIS, IBS, GNSS, VSAT, Radio
supply chain	Software, Network and Human Factor Vulnerabilities	All systems
Spoofing	Software Vulnerabilities & Network Vulnerabilities	AIS, GPS, GNSS, Radar
Port scanning	Network Vulnerabilities	Shipboard network infrastructure and port authority systems

Injection attacks	Software Vulnerabilities	Maritime navigation and communication systems, such as Electronic Chart Display and Information System (ECDIS) and Automatic Identification System (AIS)
Replay attacks	Network Vulnerabilities	AIS and maritime communication systems
Session hijacking attacks	Software Vulnerabilities & Network Vulnerabilities	Shipboard systems with remote access capabilities, such as Integrated Bridge Systems (IBS
Buffer overflow attacks	Software Vulnerabilities	Maritime software systems, including ECDIS, Voyage Data Recorders (VDR)
Side-channel attacks	Hardware Vulnerabilities	Encrypted maritime communication systems and on-board cryptographic devices
Authentication & authorisation attacks	Software Vulnerabilities & Human Vulnerabilities	Access control systems of shipboard networks
Service abuse	Software Vulnerabilities & Network Vulnerabilities	Maritime cloud services and satellite communication systems
Privilege escalation	Software Vulnerabilities & Network Vulnerabilities	On-board IT and OT (Operational Technology) systems, including engine control systems and navigation systems
infrastructure attacks	Software Vulnerabilities & Network Vulnerabilities	Virtualized maritime IT environments and data centres supporting maritime operations
Drive-by download attacks	Software Vulnerabilities & Human Vulnerabilities	Crew and officer computers connected to the internet or intranet
Node capture attacks	Hardware Vulnerabilities	Wireless sensor networks on ships or offshore platforms
Node replication attacks	Network Vulnerabilities	Sensor networks and communication nodes in maritime environments
Node outage attacks	Network Vulnerabilities	Critical nodes in shipboard networks, such as communication hubs and sensor nodes

Phishing Attacks: Phishing attacks represent the most prevalent form of cyberattack, incorporating elements of social engineering and malware tactics. In phishing, attackers leverage email services and counterfeit websites to cause harm or steal information. Phishing is specifically designed to deceive users into visiting

fake websites which obtain sensitive personal information like usernames and passwords. Spear phishing, the next attack kind, is a sub-category within phishing tactics.

Spear-phishing attacks: Spear-phishing, which involves sending targeted emails containing suspicious links to gain unauthorized access, is among the most prevalent types of cyberattacks. Once access to the information system is obtained, either through malicious software or directly from the targeted audience through deceiving techniques, hackers install key-loggers to capture logins and passwords, enabling them to access user accounts. Despite the frequency of spear-phishing attacks, port managers in the maritime sector often opt to minimize incident reporting due to the sensitive nature of the industry.

Watering hole attack: Watering hole attacks focus on exploiting security vulnerabilities within specific websites frequented by a targeted group. These attacks are aimed at employees of organizations or crew members, aiming to compromise their personal computers through infections on legitimate websites. Watering hole attacks are challenging to detect because they originate from trusted and popular websites while they might be also activated only in some cases, e.g., when employees from the targeted groups visit the infected web-sites. Implementing systems that analyse compromised websites has been proposed as a measure to mitigate the cyber risks associated with watering hole attacks.

Malware: Malware, a term referring to malicious software, is created to gain unauthorized access or inflict damage on computers, servers, or networks, typically, without the user's knowledge. This includes viruses, spyware, and ransomware. Malware typically infiltrates systems through pirated software and is often distributed via files downloaded from torrents, USB drives, or malicious websites. Even connecting an infected mobile phone to a ship's computer for charging can introduce viruses into the ship's network (i.e., the malware can exploit the data transfer capabilities of the USB interface to move from the phone to the computer, potentially compromising the computer's security and allowing unauthorized access to sensitive data), potentially disrupting critical systems like the Electronic Chart Display and Information System (ECDIS). Various types of malware pose ongoing threats to users, aiming to monitor user activities, steal confidential information for extortion or online exposure, perpetrate identity fraud, and facilitate criminal or terrorist activities within the maritime sector.

Jamming: Jamming can be divided into two categories: barrage jamming and spot jamming. Barrage jamming works by flooding the radar display with high levels of noise. The technique makes it difficult for radar operators to distinguish between genuine blips and interference. Spot jamming is a variant of barrage jamming that aims to disrupt radar detection in a specific spot or area. It focuses on masking real targets within a specific region by introducing noise.

Digital Radio Frequency Memory (DRFM): Digital Radio Frequency Memory (DRFM) is an electronic technique used to capture and retransmit RF (Radio Frequency) signals. DRFM systems work by converting incoming RF signals into digital format, storing coherent copies in digital memory, and then replaying them as required. Jammers can employ DRFM to generate deceptive signals that mimic legitimate targets, making it difficult for radar systems to distinguish between real and false targets. This deception can occur reactively or predictively, where stored signals are used to create false targets positioned both ahead of and behind the intended target.

Blip enhancement: Blip enhancement is used to amplify the size of small target returns, which can potentially mislead radar operators who use blip size for target identification.

Social engineering: This is a deceiving technique employed by potential cyber attackers to manipulate individuals into revealing sensitive information, often through interactions on social media platforms.

Understanding human behaviour is crucial for a successful attack, and hackers may use patterns of social media or instant messaging usage to gather information about in-port network activities. Such attacks may involve fake internal notices from the company or use scare tactics to prompt immediate responses from users due to fabricated emergencies. Reaction to these tactics can lead to the downloading of malicious software.

Brute force: A brute force attack is a method used by cybercriminals to gain unauthorized access to systems, networks, or accounts by systematically trying all possible combinations of passwords or encryption keys until the correct one is found. This type of attack relies on the sheer computing power and time available to the attacker, rather than exploiting vulnerabilities in the system. Brute force attacks can be highly effective but are often time-consuming and detectable due to the large number of attempts made.

(Distributed) Denial of Service (DDoS): A distributed denial of service (DDoS) attack is intended to obstruct legitimate and authorized users from accessing information, typically achieved by overwhelming the target network with a continuous barrage of traffic from multiple sources. This tactic can render systems like the AIS ineffective, as they are unable to receive positional data from neighbouring vessels. The objective of a DDoS attack is to disrupt normal operations on a particular server or network.

Man-in-the-middle: A man-in-the-middle (MITM) attack is a type of cyberattack where a malicious actor intercepts and potentially alters the communication between two parties without their knowledge. The attacker positions themselves between the communicating parties, gaining access to sensitive information such as login credentials, credit card numbers, or other private data. This type of attack can occur in various forms, including eavesdropping, session hijacking, and SSL stripping.

Supply chain: Supply chain attacks focus on causing harm by exploiting the weakest link in the entire network. International shipping, spanning from origin to destination, depends on crucial processes and stakeholders for container tracking, validation, and international approvals. Given the real-time connectivity among supply chain members, targeting ports, terminals, or other entities can effectively manipulate the system. A clear example of the damaging impact of such an attack is altering the destination of a container, which necessitates understanding the supply chain and its vulnerabilities to modify critical information.

Spoofing: A GPS spoofing attack manipulates the targeted GPS receiver to show an incorrect location by receiving a deceptive GPS signal (Lund et al., 2018). GPS spoofing is a type of cyberattack in which an attacker sends false GPS signals to deceive a GPS receiver into thinking it is in a different location or following a different path than it actually is. This attack exploits the fact that GPS receivers rely on signals from satellites to determine their location. By mimicking these signals, the attacker can manipulate the receiver's perceived position, time, and velocity.

Port scanning: Cyber attackers identify the most susceptible network ports through a classic technique known as scanning. Ports are virtual endpoints used by applications to communicate through the host operating system and connect to the Internet. During a port scanning attack, the attacker sends packets to a computer, changing the destination port each time. The primary objective of this attack is to determine which ports the user has enabled for incoming connections.

Injection Attacks: Injection attacks involve inserting malicious code into a program via user input fields, which is then executed by the server. This can lead to unauthorized access, data breaches, or complete control over the system. Common types include SQL injection, where malicious SQL statements are executed, and command injection, where attackers execute arbitrary commands on the host operating system.

Replay Attacks: Replay attacks occur when an attacker intercepts and retransmits a valid data transmission to deceive the receiver into believing it is an authentic request. This can lead to unauthorized transactions or access, as the system is tricked into repeating previously valid actions without detecting the manipulation.

Session Hijacking Attacks: Session hijacking attacks involve an attacker taking over a user's session by stealing or predicting session tokens or cookies. Once the attacker has control, they can impersonate the user, accessing sensitive data and performing unauthorized actions under the user's identity.

Buffer Overflow Attacks: Buffer overflow attacks exploit vulnerabilities in software where excessive data is written to a buffer, causing it to overflow and overwrite adjacent memory. This can lead to unpredictable behaviour, including crashes, data corruption, or the execution of malicious code, allowing attackers to gain control of the system.

Side-Channel Attacks: Side-channel attacks exploit indirect information leakage from a system, such as power consumption, electromagnetic emissions, or timing information, to infer sensitive data like cryptographic keys. These attacks do not target the direct weaknesses in algorithms but rather the physical implementation of the system.

Authentication & Authorization Attacks: Authentication and authorization attacks focus on bypassing or exploiting weaknesses in the mechanisms that verify user identities and permissions. Techniques include brute force attacks, exploiting weak passwords, session fixation, and exploiting flaws in access control policies to gain unauthorized access or escalate privileges.

Service Abuse: Service abuse attacks exploit legitimate services or features in unintended ways to gain unauthorized benefits, disrupt service, or consume resources. Examples include exploiting free-tier service limits, abusing APIs for unintended purposes, and generating excessive traffic to degrade performance.

Privilege Escalation: Privilege escalation attacks involve exploiting vulnerabilities or misconfigurations to gain higher-level permissions than initially granted. Attackers start with limited access and elevate their privileges to perform unauthorized actions, access restricted data, or take full control of the system.

Infrastructure Attacks (VM and Hypervisor): Infrastructure attacks on virtual machines (VMs) and hypervisors target the underlying virtualization layers. These attacks can exploit vulnerabilities to escape the confines of a VM, access other VMs, or gain control over the hypervisor, potentially compromising entire virtual environments.

Drive-By Download Attacks: Drive-by download attacks occur when a user unknowingly downloads and installs malicious software just by visiting a compromised or malicious website. The attack leverages browser vulnerabilities or social engineering to deliver malware without the user's explicit consent or knowledge.

Node Capture Attacks: Node capture attacks target individual nodes in a network, especially in wireless sensor networks. The attacker physically captures and compromises the node, extracting sensitive data and potentially reprogramming it to act maliciously within the network.

Node Replication Attacks: Node replication attacks involve an attacker adding replicas of legitimate nodes into a network to disrupt operations or gather information. These replicated nodes can be used to confuse, mislead, or eavesdrop on network communications, undermining the network's integrity.

Node Outage Attacks: Node outage attacks aim to disable or destroy network nodes, causing disruptions in communication and data collection. This can be achieved through physical destruction, battery exhaustion, or software vulnerabilities, leading to reduced network functionality and resilience.

4.3.1 Stages of Cyberattack in the Maritime Industry

The cyberattacks in the maritime industry may be performed according to the following stages:

- *Reconnaissance stage*: the attacker could gather all the available host and network information, including information about Navigational and Surveillance Systems.
- *Resource development*: all the necessary infrastructure is prepared to facilitate the execution of attacks using RF links/wired connections, malware or exploits.
- *Initial access*: techniques can be implemented to compromise the network devices and peripherals (including the satellite communications equipment), RF ship–to-ship or ship-to-shore connections and vulnerable RF surveillance sensors.
- *Execution*: several techniques (e.g. GPS spoofing, AIS spoofing, network manipulation) can be deployed to manipulate Maritime data (NMEA Radar/GNSS/AIS) and change the operational status of the Maritime OT devices/systems.
- *Persistence stage*: the attacker could modify configuration files or the settings of the receivers of the Navigation and Surveillance systems in order to maintain access.
- *Privilege escalation*: techniques similar to the other MITRE ATT&CK [62] matrices can be implemented, which are applicable to Maritime OT systems, in order to obtain administrator access, DBA access, file system access etc.
- *Defence escalation*: the attacker can take advantage of Maritime/navigational messages that are transmitted in plain text and implement spoofing techniques such as IP spoofing.
- *Discovery*: the target is to identify the navigation and surveillance devices and the data flow among them.
- *Lateral movement*: remote access techniques and direct connectivity (e.g., via USB stick) are feasible, taking advantage of the enhanced connectivity between sensors and management systems.
- *Collection*: the target is to capture the Maritime traffic which is exchanged between the bridge components.
- *Command and control*: the attacker is capable of mimicking the ship's bridge network using techniques to connect the ship's surveillance sensors with the attacker's C2 system, e.g., attacker's ECDIS.
- *Exfiltration*: the attacker can apply techniques to exfiltrate NMEA (Radar/AIS/GNSS) data.
- *Impact*: the results of an attack against Maritime OT systems are described, which could cause manipulation of the Maritime Picture, Denial of Service and/or loss of availability and control.

Prior to concluding the analysis of the maritime cyberattacks, it is worth mentioning the most popular attack tool, which is BRAT [63], as well as the MITRE ATT&CK [64] framework which serves as an inclusive knowledge base and model that outlines the various tactics, techniques, and procedures (TTPs) used by attackers during different stages of a cyberattack.

BRAT [63] is a holistic and user-friendly tool for conducting Bridge Attack simulations. It is designed as a modular framework that provides interactive implementations of cyber-attacks targeting the communication of nautical data within Integrated Bridge Systems (IBSs). These attacks can be individually configured, combined, scheduled, and orchestrated automatically. To the best of our knowledge, BRAT represents the first domain-specific tool for simulating the execution of internal network attacks against maritime systems. It has the potential to enhance security assessments and enables system engineers to systematically identify and validate vulnerabilities across numerous components. Additionally, BRAT facilitates the development

and validation of appropriate countermeasures against cyber-attacks, including effective detection and preventive authentication. Moreover, BRAT can be integrated into Maritime Education and Training (MET) for bridge crews, enhancing awareness and improving their ability to respond to cyber threats effectively.

The MITRE ATT&CK framework [64] is a repository of security threat intelligence that examines how attackers infiltrate and propagate within computer systems, focusing on insights gathered from actual breaches. This data is characterized by three key elements, known as Tactics, Techniques, and Procedures (TTPs), which form the basis for implementing Defense in Depth (DiD) strategies. The framework comprehensively documents and organizes cyber adversary behaviours without strict chronological constraints.

- *Tactics*: Outline the methods and goals utilized during an attack;
- *Techniques*: Encompassing 185 primary techniques and 367 sub-techniques, these represent technical approaches for achieving tactical objectives in cyberattacks;
- *Procedures*: These define the sequential steps of an attack process.

4.4 Reporting of real-life attacks

We are now going to delve into the most popular maritime cyberattacks. These attacks carry significant repercussions for both the targeted systems and organizations, influencing greatly how such entities respond to such incidents [1], [12], [65].

4.4.1 Cyberattack on Saudi Oil and Gas Company Aramco - 2012

In 2012, ARAMCO, the largest oil and gas operator in Saudi Arabia, experienced a catastrophic cyberattack. An employee mistakenly opened a phishing email containing a malicious link, resulting in the installation of a virus, leading to file corruption and disrupted phone communications. Approximately 35,000 computers were infected, resulting in the loss of three-quarters of the company's data. As ARAMCO provides 10% of the world's oil, it was compelled to halt sales temporarily. After 17 days, the company resorted to giving away oil for free to maintain supply within Saudi Arabia. It took ARAMCO five months to recover from the incident and return to normal operations.

4.4.2 Ghost Shipping / Port of Antwerp – 2013

Between 2011 and 2013, the Belgian port of Antwerp fell victim to cybercriminals orchestrating drug trafficking schemes. These hackers were contracted by traffickers to infiltrate the IT systems overseeing container movement and tracking. Over a span of two years, the systems of at least two port-operating companies were consistently compromised by the hackers. The cyberattack exploited a vulnerability in the Electronic Container Release System (ERS), which was introduced in the port of Antwerp in 2005. The ERS functioned by having carriers, instead of freight forwarders, transmitting unique electronic numbers (pin codes) via email to recipients, agents, and terminal ports. These pin codes corresponded to specific containers and were essential for retrieving containers from the terminal warehouses. In 2011, a group of intruders successfully breached the container management system, gaining access to data that revealed the precise location and security status of containers within the port. Armed with this information, the attackers dispatched unauthorized drivers to steal the compromised cargo before the legitimate owners could claim it. The breach was detected when entire containers went missing. To facilitate their illicit activities, the criminal group employed phishing attacks, sending malicious software via email to port staff. Despite initial efforts

to fortify the systems with firewalls, the hackers circumvented these defences and deployed keylogging software on legitimate computers within the port facilities. This enabled them to remotely capture keystrokes and screenshots from staff monitors, granting them unfettered access to sensitive port data.

4.4.3 Vessels GPS in Korea – 2015

In April 2015, South Korea encountered a significant GPS jamming cyberattack, impacting over 1000 aircraft and 250 ships. Such attacks pose grave threats, as affected vessels are rendered unable to accurately determine their positions, jeopardizing their ability to navigate safely or return to port. The incident was attributed to state-sponsored actors from North Korea. GPS jamming entails deliberate interference aimed at obstructing or halting signals rather than altering them (spoofing). Consequently, the lack of data and connectivity with Automatic Identification System (AIS), Electronic Chart Display and Information System (ECDIS) as well as Voyage Data Recorder (VDR) on-board devices result in their dysfunction when GPS signals are disrupted.

4.4.4 Port Operations of A.P. Moller-Maersk - 2017

On June 27th, 2017, the IT infrastructure of A.P. Moller – Maersk fell victim to the NotPetya ransomware attack, marking a significant cyber vulnerability for the maritime industry. This attack had widespread repercussions, affecting all of Maersk's global operations, including 17 terminals. Among these terminals, two were compromised in the port of Rotterdam, with the remaining 15 located in various ports worldwide. Due to issues with the company's information systems, some cargo shipments were not delivered to their intended destinations. Despite potential damage to its reputation, Maersk promptly disclosed details of the attack via its Twitter account, outlining the steps taken to address the incident and sharing insights for the benefit of other companies. Notably, maritime law does not mandate disclosure of cyber incidents. The financial toll on Maersk was estimated at approximately $300 million, necessitating continued operations without IT infrastructure for several days until activities could resume.

Maersk was compelled to suspend operations at multiple ports globally, resulting in a 20 percent reduction in volume. To restore services, the organization replaced 45,000 computers, 4,000 servers, and installed 2,500 new applications.

4.4.5 Long Beach Terminal of Cosco - 2018

In July 2018, the aforementioned ransomware cyberattack 'NotPetya' targeted the Cosco Long Beach Terminal, affiliated with Cosco Shipping. This attack rendered the telephone systems inactive and disrupted email exchange within the affected area. To prevent further compromise, the company isolated its network from other regions, prioritizing security over potential widespread system failure. Despite these challenges, the cyberattack did not disrupt the company's daily operations, and all ships continued to function normally. However, as a precautionary measure, the company temporarily severed connections with external regions. Remarkably, within one week of the incident, the company successfully restored its operations to normal, underscoring its robust infrastructure for managing such emergencies.

5 Countermeasures for Cybersecurity in Maritime Systems

5.1 Classification of countermeasures

In this chapter, we examine the countermeasures against the threats that secure or eliminate if feasible the existing vulnerabilities on the maritime ship's systems. We tried to establish a taxonomy based on the type of countermeasures and categorize them into three main groups: Technical Countermeasures, Operational Countermeasures and Administrative Countermeasures [66], [67], [68].

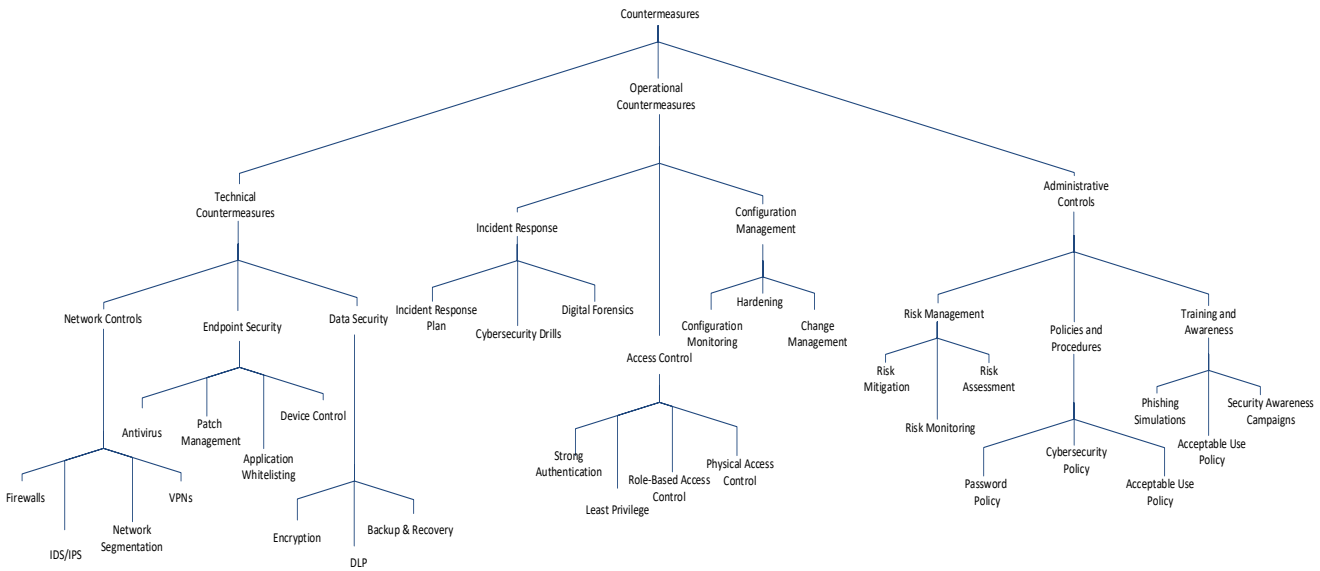

Figure 5: Countermeasures hierarchy tree

5.1.1 Technical Countermeasures

This category covers a wide range of technological solutions and tools for securing maritime systems, networks, and data. It includes subcategories like Network Controls, Endpoint Security and Data Security.

Network Controls aim to secure the network infrastructure, prevent unauthorized access, and mitigate network-based threats. On the other hand, Endpoint Security refers to the set of security measures and tools applied to individual computing systems or endpoints, such as laptops, desktops, servers, and mobile devices, to protect them from cyber threats. Finally, Data Security encompasses the methods and technologies used to protect data from unauthorized access, modification, disclosure, or destruction. It involves measures to ensure the confidentiality, integrity, and availability of data throughout its lifecycle, both when data is stored on systems or in transit during network transmission.

Network Controls

The main security controls that have been suggested in the literature for maritime systems are as follows.

Firewalls: Firewalls control incoming and outgoing network traffic based on predefined security rules, acting as a barrier between trusted and untrusted networks. They are essential for preventing unauthorized access and filtering out malicious traffic. They can separate effectively the OT from the IT systems, by allowing only the necessary traffic. Such a measure should be properly configured; otherwise, it could allow unauthorized traffic to critical systems.

Intrusion Detection/Prevention Systems (IDS/IPS): IDS monitors network traffic for suspicious activity and alerts accordingly the administrators, while IPS takes a step further by actively blocking detected threats. These systems are crucial for identifying and mitigating network-based attacks in real time. Such systems have some potential weaknesses, especially the generation of many false positives that might overwhelm the administrators. Further, an IPS can disrupt legitimate traffic if not properly tuned.

Network Segmentation: By dividing the network into smaller zones or segments, network segmentation limits the spread of attacks and prevents unauthorized access to sensitive areas of the network. As such, this measure represents an effective way to contain potential breaches and minimize the impact of a compromise. Nevertheless, it requires careful planning and implementation because it can increase complexity and management overhead.

Virtual Private Networks (VPNs): A VPN creates secure encrypted tunnels over public networks, enabling remote access to maritime systems while protecting the confidentiality and integrity of the transmitted data. On the other hand, VPN vulnerabilities can be exploited to gain unauthorized access thus requiring the use of strong authentication and encryption protocols.

On the other hand, VPN vulnerabilities can be exploited to gain unauthorized access thus requiring the use of strong authentication and encryption protocols.

Endpoint Security

The practice is to protect individual devices or endpoints (including computers, servers, ICS, HMI) connected to a ship's systems network from cyber threats.

Antivirus Software: These solutions are designed to detect and remove malicious software, such as viruses, worms, and Trojans, from on-board systems and endpoints. Regular updates are necessary to ensure

protection against the latest threats. Despite its advantages, this countermeasure may face challenges as it might not be as effective against new (and maybe more advanced) or unknown malware (zero-day attacks).

Patch Management: Applying security patches and updates to software and operating systems is crucial to address known vulnerabilities that could be exploited by attackers. Effective patch management reduces the attack surface and minimizes the risk of successful cyber-attacks. While valuable, patching can be time-consuming and may require system downtime. However, it has to be carefully applied, as some patches might introduce new problems. While patches are designed to fix existing vulnerabilities, they can sometimes inadvertently introduce new ones due to coding errors, unintended side effects or compatibility issues.

Application Whitelisting: Instead of attempting to identify and block malicious software, application whitelisting takes a more proactive approach by allowing only authorized programs to run on the system. This can prevent the execution of unauthorised or malicious code. However, this countermeasure requires thorough testing to ensure compatibility with legitimate applications. Further, it can be possible that a legitimate application might be infected without having then the ability to block it so as to prevent its infection from overwhelming the whole endpoint device.

Device Control: Device control measures restrict the use of unauthorized devices, such as USB drives or external storage, from connecting to the network or systems. This helps prevent data leakage and the introduction of malware through removable media. On the other hand, strict device control policies can hinder legitimate work activities that require the use of external devices for data transfer or maintenance purposes and this can lead to frustration among the users.

Data Security

The practice to protect digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. This includes data which are stored on devices or systems, data in transit which are transmitted over networks and data that are being processed by applications.

Encryption: Encryption scrambles data, making it unreadable without the correct decryption key. It is essential for protecting sensitive data, both when stored on systems and in transit during the network transmission. However, it is important to note that encryption can be computationally expensive (on devices with limited computing capabilities like AIS) and requires secure key management and storage practices. Further, secure encryption protocols and schemes have to be adopted to avoid the breaking of data encryption.

Data Loss Prevention (DLP): DLP solutions monitor and control the movement of sensitive data, preventing unauthorized access, transmission, or exfiltration. They can enforce data policies (i.e Data at rest policy) and alert administrators to potential data breaches or leaks. It is important to mention that DLP solutions can be complex to configure and require a deep understanding of the organization's data flows and sensitivity levels. Improper configuration can lead to false positives or negatives, impacting productivity and potentially missing actual data breaches.

Backup and Recovery: Regular backups of critical data and systems are essential for ensuring business continuity and minimizing the impact of data loss or corruption due to cyber-attacks or other incidents (like physical ones, such as fire). Robust backup and recovery processes enable organizations to restore data and

resume operations quickly. However, the data backup itself can be targeted by attackers especially when it is reachable through the network and the recovery processes need to be tested regularly to ensure that any backup is recoverable. Also, there is a need for infrastructure that can support the backup data, backup data are not only information but can be backup images from OT systems in order to be restored when needed. The backup frequency and necessity might depend on the criticality and sensitivity of the data.

5.1.2 Operational Countermeasures

This category focuses on the processes, procedures, and activities related to the day-to-day operation and management of cybersecurity measures. This control incorporates subcategories, such as Access Control, Incident Response, and Configuration Management.

Access Control is a set of policies, procedures, and mechanisms that regulate and manage access to systems, applications, networks, and data. It ensures that only authorized individuals or entities can access specific resources based on their roles, responsibilities, and privileges. Incident Response is an approach to address and manage cyber security incidents, like data breaches, system compromises, or cyber-attacks. Lastly, Configuration Management is the process of systematically managing and controlling the configuration of systems, applications, and infrastructure components throughout their lifecycle. It establishes and maintains the integrity of systems, ensuring that changes are properly controlled, documented, and tracked.

While these countermeasures are effective, their success relies heavily on proper implementation, comprehensive employee training, and ongoing maintenance. Processes must also be updated regularly to address new threats and vulnerabilities. However, even with these precautions, human error and a lack of information security awareness can sometimes undermine these security controls.

Access Control

A set of mechanisms, policies and procedures that regulate who or what can view, use, or modify resources within a computing environment.

Strong Authentication: Implementing strong authentication mechanisms, such as multi-factor authentication (MFA), is crucial for verifying user identities and preventing unauthorized access to maritime systems and data. MFA combines multiple factors (e.g., something you know, something you have, and something you are) for enhanced security. Of course, strong authentication has negatives as it may cause inconvenience to the users due to the additional authentication steps involved and can be technically complex and cost effective to implement because of the additional equipment needed (software, hardware etc).

Least Privilege: The principle of least privilege ensures that users are granted only the minimum permissions and access rights necessary to perform their job functions. This practice limits the potential damage that can be caused by compromised accounts or insider threats. To restrict access can create inconvenience and hinder productivity if users frequently need to request elevated privileges for legitimate tasks. Also, Implementing and maintaining least privilege policies can be time-consuming for IT administrators, especially in dynamic environments where roles and tasks change frequently.

Role-Based Access Control (RBAC): RBAC assigns suitable permissions and access rights on specific resources based on an individual's role within the organization, rather than granting broad access to all resources. It simplifies access management and ensures that users have access only to the resources they need (in order to fulfil their tasks). However, it may not scale well in large or dynamic environments where granular permissions are needed, unlike Attribute-Based Access Control (ABAC), which offers flexibility by considering individual attributes for fine-grained access control.

Physical Access Control: Implementing physical security measures, such as access control systems (e.g., biometric scanners, smart cards), is essential for restricting access to sensitive areas of maritime facilities and vessels. It prevents unauthorized personnel from gaining physical access to critical systems or infrastructure. Nevertheless there are drawbacks to this as well, depending on the technology and scale of implementation, physical access control systems can be costly to install and maintain. This includes the cost of hardware (e.g., readers, scanners, and cameras), software, installation, and ongoing maintenance and support.

Incident Response

Incident Response Plan: A well-defined and regularly updated incident response plan outlines the procedures and steps to be followed in the event of a cyber incident. It helps organizations respond effectively, minimize the impact (including potential disruptions to business continuity), and facilitate recovery. Also, to develop an effective incident response plan can be complex and time-consuming, it requires expertise in cybersecurity, legal compliance, and operational processes.

Digital Forensics: Digital forensics involves the investigation and analysis of digital evidence to determine the cause, scope, and impact of a cyber incident. It aids to identify the attack vectors, attributing the attack, and gathering evidence for legal or regulatory purposes. It can be applied to all conventional systems and find the root cause and create the appropriate case studies in order to avoid the same situation in the future

Configuration Management

Hardening: System hardening involves securing systems by disabling unnecessary services, removing default accounts, and applying security patches and secure configurations. This reduces the attack surface and minimizes the potential for exploitation. However, there are drawbacks on this by having compatibility issues when existing software or applications that rely on the vulnerable services or features or the overhead for the IT team to secure and maintain the hardening as it requires ongoing effort to keep configurations up-to-date, apply new patches, and monitor for changes that might introduce vulnerabilities.

Change Management: Implementing a structured change management process ensures that changes to systems, applications, and configurations are properly reviewed, tested, and documented. This helps prevent unintended consequences and maintains system integrity.

Configuration Monitoring: Continuously monitoring system configurations and settings allows organizations to detect unauthorized changes or deviations from baseline configurations. This aids in identifying potential security breaches or misconfigurations that could introduce vulnerabilities in the system (or its parts). However, configuration monitoring can consume significant resources, potentially leading to alert fatigue from excessive notifications and false positives due to its sensitivity to changes.

5.1.3 Administrative Controls

This category addresses the policies, procedures, and management practices that govern cybersecurity within an organization. It includes subcategories like Policies and Procedures, Training and Awareness and Risk Management.

The Policies and Procedures category refers to the set of documented guidelines, rules, and instructions that outline an organization's approach to cybersecurity. On the other hand, the Training and Awareness programs are designed to educate and inform the crew about cybersecurity risks, best practices, as well as their roles and responsibilities in maintaining a cyber secure environment. Finally, Risk Management is a systematic process of identifying, assessing, and responding to potential risks that could impact an organization's assets, operations, or objectives.

Policies and Procedures

Cybersecurity Policy: A comprehensive cybersecurity policy is essential for defining an organization's cybersecurity goals, responsibilities, and acceptable use of technology. It serves as a guiding framework for implementing and maintaining effective security measures across the organization.

Password Management: Password management is the set of practices, policies, and procedures designed to create, store, protect, reset and regularly update strong passwords to ensure secure access to systems.

Acceptable Use Policy: An acceptable use policy establishes rules and guidelines for appropriate and inappropriate use of organizational (IT) resources, including systems, networks, and data. It helps ensure that people understand their responsibilities, the usage restrictions on resources and the potential consequences of (resource) misuse.

Training and Awareness

Cybersecurity Drills: Conducting regular cybersecurity drills and exercises helps organizations test and improve their incident response capabilities. These drills simulate real-world attack scenarios and allow personnel to practice their roles and responsibilities, identifying areas for improvement. While the real life scenarios are high complexity and need conductors with high expertise on cyber security they are a valuable tool for enhancing preparedness. Also, the frequency of drills should be determined based on the organization's risk profile and resources, but an annual schedule of the drill can maintain readiness and identify areas for improvement

Phishing Simulations: Conducting phishing simulations involves sending mock phishing emails to the crew to test their ability to recognize and respond appropriately to such attacks. These simulations typically involve creating realistic phishing emails, tracking user interactions (such as clicking links or opening attachments), providing feedback and training to victims, and analysing metrics to evaluate the effectiveness of the training program.

Security Awareness Campaigns: Regular security awareness campaigns, through various channels like newsletters, posters, or video content, help keep cybersecurity top-of-mind for the crew. These campaigns

involve training sessions, workshops & seminars as well in order to promote a security-conscious culture and emphasize the importance of vigilance and adherence to security policies.

Risk Management

Risk Assessment: Performing comprehensive risk assessments involves identifying, analyzing, and evaluating potential cybersecurity risks to maritime systems, infrastructure, and operations. This process helps organizations prioritize risks based on their likelihood and potential impact.

Risk Mitigation: Based on the risk assessment findings, organizations can implement appropriate countermeasures and risk mitigation strategies to reduce the likelihood or impact of identified risks. This may involve a combination of technical, operational, and managerial controls.

Risk Monitoring: Risk management is an ongoing process that requires continuous monitoring for emerging risks, changes in the threat landscape, and the constant evaluation of the effectiveness of implemented mitigation strategies. Regular monitoring allows organizations to adapt and adjust their risk management approach as needed.

5.2 Vulnerabilities and Countermeasures correlation

The table below offers a general mapping between vulnerabilities and the countermeasures that cover them. It is important to note that the specific countermeasures required per vulnerability may vary depending on the systems unique circumstances, risk profile, and existing security controls. Furthermore, some vulnerabilities may necessitate a combination of countermeasures for effective mitigation, while others may have dedicated countermeasures that directly address the vulnerability.

Table 4: Vulnerabilities and the related countermeasures

Vulnerabilities	***Countermeasures***
Software Vulnerabilities	
Poor patch management	Patch Management
Obsolete OS	Hardening, Change Management
Software Dependencies	Patch Management, Antivirus, Application Whitelisting
Hardware Limitations	Hardening, Change Management
Verbose Error Messages	Hardening, Change Management, Configuration Monitoring
Unhandled Exceptions	Hardening, Change Management, Configuration Monitoring
Open Ports and Services	Firewalls, Hardening, Configuration Monitoring, Application Whitelisting
Weak Cryptographic Standards	Hardening
Systemic Vulnerabilities	
Resource Starvation	Network Segmentation, Firewalls, IDS/IPS, Application Whitelisting

Propagation of Faulty Data	Backup and Recovery
System Integration Failure	Change Management, Configuration Monitoring, Backup and Recovery
Network Vulnerabilities	
Lack of Network Segmentation	Network Segmentation
Weak Remote Access Policies	VPNs, Strong Authentication, Least Privilege, RBAC
Unsecured Wireless Networks	Firewalls, Encryption, Network segmentation, Strong Authentication
Lack of Encryption	Encryption, Cybersecurity Policy
Weak Encryption	Encryption, Cybersecurity Policy
Signal Jamming	Physical Access Control, Acceptable Use Policy
Lack of Authentication	Strong Authentication, Role-Based Access Control (RBAC)
Packet Modification	Encryption, IDS/IPS, Network segmentation
DoS Attacks	Firewall, IDS/IPS, Network segmentation, Hardening
Human Factor Vulnerabilities	
Insufficient Training	Cybersecurity Drills, Security Awareness Campaigns, Phishing Simulation
Social Engineering	Cybersecurity Policy, Cybersecurity Drills, Security Awareness Campaigns, Phishing Simulation, Device Control, DLP, Strong Authentication
Negligence and Errors	Security Awareness Campaigns, Least Privilege, Configuration monitoring, change management
Unauthorized Access	Physical access control, RBAC, least privilege, policies, risk monitoring, hardening, network segmentation. Strong Authentication
Surveillance and Monitoring Failures	Configuration monitoring, Risk monitoring, IDS/IPS
Miscommunication	Incident Response Plan, Security Awareness Campaigns, Cybersecurity Drills
Lack of Incident Reporting	Incident Response Plan, Cybersecurity Drills, Cybersecurity Training

5.3 Countermeasures Comparison

Most of the literature aligns with the NIST Cybersecurity Framework, which emphasizes the principles of identify, protect, detect, respond, and recover. These principles were adopted by the International Maritime Organization (IMO) in 2021 as part of its Guidelines on Maritime Cyber Risk Management, which recommend that all vessels integrate cybersecurity risk management into their existing safety management systems. Most of the literature aligns with the NIST Cybersecurity Framework, which emphasizes the principles of identify, protect, detect, respond, and recover. These principles were adopted by the

International Maritime Organization (IMO) in 2021 as part of its Guidelines on Maritime Cyber Risk Management, which recommend that all vessels integrate cybersecurity risk management into their existing safety management systems.

On the other hand, we maintain a more simple classification of countermeasure protection mechanisms. In particular, we have classified the mentioned countermeasures based on their primary functions, i.e., Prevention, Detection, Response, and Recovery.

The first step to protect your systems is the Prevention category, which aims to proactively safeguard maritime systems by implementing measures that deter cyberattacks and reduce or eliminate vulnerabilities. Detection focuses on identifying cyber threats promptly. Response relates to taking swift actions to contain and mitigate the impact of an attack. Finally, you must Recover from the attack and restore all systems to normal operations.

Apart from the response type, the following table, Table 5, includes additional criteria that allow us to compare the identified countermeasures: (a) the type of the measure (based on our classification as presented in Section 5.1, (b) its cost, (c) the implementation complexity of the measure, (d) the efficiency, (e) adaptability, (f) user impact and (g) the training requirements. Each criterion assigned a value of "Low, Moderate, High" and combinations of them when a criterion can cover a wider range of values.

The cost of implementing a countermeasure encompasses the initial purchase or licensing fees, ongoing maintenance expenses, and potential costs associated with personnel training, infrastructure upgrades, and operational disruptions.

Also, the complexity of a countermeasure refers to the technical expertise, integration effort, operational impact required for successful implementation and management.

Further, the efficiency of a countermeasure is determined by its ability to achieve the desired security outcomes while minimizing the use of resources; countermeasures with high efficiency can effectively mitigate risks without excessive costs or operational overhead.

The adaptability of a countermeasure refers to its flexibility and capacity to adjust to evolving threats, technologies, and operational environments. Highly adaptable countermeasures can maintain their effectiveness over time and across different scenarios.

The user impact of a countermeasure assesses the extent to which it affects the daily operations, workflows, and productivity of users. Countermeasures with low user impact seamlessly integrate into existing processes and minimize disruptions.

As a last criterion, we use the training requirements which evaluate the level of knowledge and skills necessary for the personnel to effectively implement, manage, and utilize a countermeasure. Countermeasures with low training requirements are easier to adopt and maintain, reducing the burden on staff.

Table 5: Countermeasures compared according to important criteria

Mechanism	***Type***	***Countermeasures***	***Cost***	***Complexity***	***Efficiency***	***Adaptability***	***User Impact***	***Training Requirements***
Prevention	Technical	Firewalls	Low to Moderate	Moderate	High	Moderate	Low	Low
		Network Segmentation	Moderate to High	High	High	High	Moderate	Moderate to High
		VPNs	Moderate	Moderate	Moderate	High	Low	Moderate
		Intrusion Prevention Systems (IPS)	Moderate to High	Moderate to High	High	Moderate	Moderate	Moderate to High
		Antivirus	Low	Low	Moderate	Moderate	Low	Low
		Patch Management	Low to Moderate	Moderate	High	Low	Low to Moderate	Moderate
		Application Whitelisting	Moderate	High	High	Low	Moderate	High

	Device Control	Moderate	Moderate	High	Low	Moderate	Moderate
	Encryption	Moderate to High	Low to Moderate	Moderate	High	Low	Low to Moderate
	Data Loss Prevention (DLP)	High	High	Moderate	Moderate	Moderate	High
Operational	Strong Authentication	Moderate to High	Moderate	High	Moderate	Moderate	Moderate
	Least Privilege	Low to Moderate	Moderate	High	Moderate	Moderate	Moderate
	Role-Based Access Control (RBAC)	Moderate	Low to Moderate	High	Moderate	Low	Low to Moderate
	Physical Access Control	Moderate to High	Moderate	High	Low	Low	Moderate
	Hardening	Low to Moderate	Moderate to High	High	Low	Low to Moderate	Moderate to High
Administrative	Cybersecurity Policy	Moderate to High	Moderate to High	High	Low to Moderate	High	High

		Password Policy	Low	Low	Moderate	Moderate to High	Moderate to High	Low
		Acceptable Use Policy	Low	Low to Moderate	High	Low to Moderate	Moderate to High	Moderate
Detection	Technical	Intrusion Detection Systems (IDS)	Moderate to High	Moderate to High	Moderate	Moderate	Low	Moderate to High
	Operational	Configuration Monitoring	Moderate	Moderate	Moderate	Moderate	Low	Moderate
Response	Operational	Incident Response Plan	Low to Moderate	Moderate	High	High	Moderate	Moderate
		Cybersecurity Drills	Moderate	Moderate	Moderate to High	High	Moderate	Moderate
		Digital Forensics	Moderate to High	High	Moderate to High	Moderate	Low	High
Recovery	Technical	Backup and Recovery	Moderate to High	Moderate	High	Moderate	Low	Moderate
	Administrative (Partial)	Risk Mitigation (it can also involve prevention and detection measures)	Moderate to High	Moderate to High	High	Low to High	Low to High	Moderate

The following table compares the strengths and the weaknesses of each countermeasure. We took into account their effectiveness, costs, operational impact, and ease of implementation, then we created the table with the advantages and disadvantages of the listed countermeasures. In accordance with the previous table we can find the most effective, low to moderate cost as well as the least complexity countermeasures for our vulnerabilities.

Table 6: Countermeasure strengths and weaknesses

Countermeasure	***Strengths***	***Weaknesses***
Firewall	Cost-effective, easy to deploy, blocks unauthorized traffic, customizable	Can be misconfigured, ineffective against zero-day attacks, requires regular updates
Intrusion Prevention System (IPS)	Real-time threat blocking, can be integrated with other security tools	Can disrupt legitimate traffic, requires regular updates and fine-tuning, potential for false positives
Network Segmentation	Limits the impact of a breach, customizable to specific security needs	Requires careful planning and implementation, can increase network complexity
VPN	Protects data in transit, essential for secure remote access, can be used to connect disparate networks securely	Requires strong authentication and encryption, can introduce latency, vulnerable to misconfigurations
Antivirus Software	Easy to deploy and use, essential for basic protection, can scan files and systems in real-time	Not effective against zero-day attacks, can impact system performance, requires regular updates
Patch Management	Essential for maintaining security, can be automated	Requires downtime for installation, some patches may introduce new problems, not all vulnerabilities have patches available
Application Whitelisting	Highly effective against unknown malware, prevents execution of unapproved software	Can be complex to manage, requires thorough testing to avoid blocking legitimate applications.
Device Control	Prevents unauthorized devices from connecting	Can inconvenience users, can be bypassed with social engineering or technical means
Encryption	Protects data confidentiality, essential for compliance	Can be computationally expensive, requires secure key management and storage
Data Loss Prevention (DLP)	Enforces data handling policies, helps with regulatory compliance, can monitor and block sensitive data transfers	Can generate false positives, can impact network performance, requires careful configuration and tuning to avoid blocking legitimate traffic
Strong Authentication	Enhances security by requiring multiple factors for verification	Can impact user experience, requires additional infrastructure and user training
Least Privilege	Limits potential damage, helps prevent privilege escalation attacks	Requires careful role definition and assignment, can be complex to implement in large organizations
Role-Based Access Control (RBAC)	Easy to understand and implement, scales well to large organizations, improves efficiency and security	Roles may not always align perfectly with individual responsibilities, requires ongoing maintenance as roles change
Physical Access Control	Essential for protecting physical assets, deters unauthorized entry	Can be expensive to implement and maintain, requires ongoing monitoring and maintenance, vulnerable to social engineering attacks
Hardening	Reduces the attack surface, strengthens overall system security	Requires specialized knowledge, potential for misconfigurations, can impact functionality if not done carefully

Intrusion Detection System (IDS)	Can detect a wide range of attacks, provides alerts for further investigation, can be used for log analysis	Can generate false positives, requires skilled analysts to interpret alerts, may not detect all types of attacks
Configuration Monitoring	Helps maintain system integrity and security, can be automated	Requires baseline configurations and continuous monitoring, can generate a large number of alerts
Incident Response Plan	Essential for minimizing damage and downtime	Effectiveness depends on plan quality and team preparedness, requires regular review and testing
Cybersecurity Drills	Helps identify weaknesses in incident response process	Effectiveness depends on realism and relevance of scenarios, requires time and resources to plan and execute
Digital Forensics	Essential for evidence collection and legal procedures	Can be time-consuming and expensive
Backup and Recovery	Essential for systems continuity	Backups can be targeted by the attacker, recovery may not be complete
Risk Mitigation	Can reduce the likelihood and impact of risks	Effectiveness depends on accuracy of risk assessment and implementation of appropriate controls

5.4 Conclusions

The selection and implementation of effective countermeasures are critical components of strong cyber security. However, it is difficult to identify the golden ratio between the cost and the effectiveness. There is a point where the cost of countermeasures can become increasingly expensive without a proportional increase in effectiveness. This is a fundamental principle in cybersecurity and risk management, often referred to as the "law of diminishing returns".

The initial investment in basic security controls like firewalls, antivirus software, and patch management typically yields a significant increase in security for a relatively low cost. These foundational measures address common vulnerabilities and significantly reduce the risk of attacks. Some countermeasures, like extensive data loss prevention solutions, can be very expensive to buy and maintain. They might require specialized expertise, extensive training, and ongoing monitoring. These costs may not be justified if the additional protection they offer is minimal compared to existing controls.

Based on the provided tables, the most efficient, cost-effective, and relatively easy-to-implement countermeasures for maritime cybersecurity can be summarized in the below table.

Table 7: Selection of most efficient, cost-effective, and easy-to-implement countermeasures

Prevention	Firewalls	Essential for basic network protection, they offer a high level of effectiveness against unauthorized access and known threats at a relatively low cost and easy implementation.
	Antivirus Software	Provides crucial protection against known malware with minimal cost and easy deployment.
	Patch Management	Crucial for addressing software vulnerabilities, patch management is highly effective and can be automated, making it relatively easy to implement.

	Strong Authentication	Strong authentication significantly enhances security against unauthorized access with moderate cost and implementation effort.
	Least Privilege	Offers high protection against insider threats and compromised accounts with minimal cost and moderate implementation complexity.
	Hardening	Reduces the attack surface and overall system vulnerability, with low to moderate cost and complexity.
Detection	IDS	Detects a wide range of attacks, with moderate to high cost and complexity.
Response	Incident Response Plan	Essential for minimizing the impact of security incidents, with low to moderate cost and moderate complexity.
	Cybersecurity Drills	Regular drills are essential for improving response capabilities and identifying weaknesses, and they are a low-cost way to enhance incident response.
Recovery	Backup and Recovery	Essential for system continuity, with moderate to high cost and moderate complexity.

Many existing countermeasures effectively address several critical for maritime cybersecurity. They offer a good balance of cost-effectiveness, providing substantial protection without financial overweight. Additionally, some countermeasures are relatively easy to implement, requiring minimal specialized knowledge or resources. This ease of implementation allows for swift deployment, ensuring timely protection against known threats and vulnerabilities. Furthermore, most existing countermeasures effectively mitigate known threats, providing a strong defense against common attacks and vulnerabilities.

Despite their strengths, current countermeasures have areas that need improvement. A significant challenge lies in their limited effectiveness against zero-day attacks, which are new and unknown threats that exploit vulnerabilities before patches or countermeasures are available. Additionally, some countermeasures can negatively impact user experience, causing inconvenience or disrupting workflows, which may hinder adoption or lead to workarounds that compromise security. Furthermore, several countermeasures require specialized knowledge or expertise to implement and manage effectively, limiting their accessibility to organizations with limited resources or technical expertise. Addressing these challenges requires ongoing research, development, and collaboration to enhance the effectiveness and usability of maritime cybersecurity countermeasures.

However, all mentioned countermeasures vary in their implementation timelines. Some, like firewalls and antivirus software, can be deployed relatively quickly to provide immediate protection. Others, such as developing comprehensive incident response plans or implementing regular cybersecurity drills, may require more time to fully establish. However, for long-term maritime cybersecurity, it is crucial to invest in 'security by design' principles. This involves developing secure protocols specifically for maritime systems, moving beyond the current reliance on potentially vulnerable technologies and communication protocols. Implementing encryption for all data transmissions, designing resilient and segmented network architectures, and creating maritime-specific security standards are essential steps. While these systemic changes may

require significant time and resources, they are fundamental to creating a robust and sustainable maritime cybersecurity environment.

6 Risk Management in Maritime Cybersecurity

6.1 Definition and importance of risk management

The shipping industry is undergoing a significant shift towards digitalization, wherein advancements like Big Data analytics, the Internet of Things (IoT), Cloud computing, Machine Learning, and Artificial Intelligence (AI) are set to revolutionize traditional vessel operations. The emergence of unmanned autonomous ships reflects a significant interest in the industry, while remote monitoring and control systems aboard vessels have already been set in place for numerous companies globally. Cybersecurity extends beyond mere prevention of unauthorized access by hackers, which could compromise confidentiality and control. It also encompasses the preservation of information and system integrity and availability, ensuring business continuity and the sustained functionality of digital assets and systems. To achieve this, attention must be paid not only to protecting ship systems from physical attacks but also to drafting resilient system designs and supporting processes, incorporating contingency measures to address potential disasters.

As ships increasingly adopt digitalization, integration, and automation, the imperative for cyber risk management on-board intensifies. With the ongoing evolution of technology, the convergence of information technology (IT) and operational technology (OT) on-board vessels has become more prevalent, often leading to continuous connectivity to the Internet. The proliferation of big data, smart ships, and the IoT amplifies the volume of information accessible to cyber attackers and expands the potential attack surface for cybercriminals. Consequently, the imperative for robust cyber risk management approaches becomes increasingly critical both presently and in the foreseeable future [69].

According to the International Maritime Organization (IMO), cyber risk management is defined as "the process of identifying, analysing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders" [70]. In this context, IMO advocates for integrating cyber risk considerations into the objectives and functional requirements outlined in the International Safety Management (ISM) code[2]. This approach does not mandate addressing every potential threat but rather evaluating the risk each threat poses to operations, security, and safety, and then managing it accordingly. The IMO also highlights the uniqueness of each organization and recommends tailoring the delivery model to fit the company's performance, needs, and systems effectively. Ultimately, cyber risk assessment aims to ensure the safety and security of shipping operations. To achieve this, the cyber risk assessment methodology should be resilient and adaptable, seamlessly integrating into existing comprehensive control system practices.

[2] https://www.imo.org/en/ourwork/humanelement/pages/ISMCode.aspx

The National Institute of Standards and Technology (NIST) has crafted a cybersecurity framework[3] aimed at safeguarding critical sectors and infrastructure. This framework revolves around five fundamental elements or activities: Identify, Protect, Detect, Respond, and Recover. These elements are further subdivided into 22 categories, offering a blueprint for creating a cybersecurity plan. These activities are relevant also in the context of maritime services security. IMO has integrated these elements, endorsing them as high-level recommendations integral to successful cyber risk assessment. In alignment with this, the Baltic and International Maritime Council (BIMCO) and a coalition of industry bodies have outlined a maritime cyber risk assessment approach, comprising the following steps:

- Identify threats
- Identify vulnerabilities
- Assess risk exposure
- Develop protection and detection measures
- Establish response plans
- Respond to and recover from cybersecurity incidents.

6.2 Integration of risk management within maritime cybersecurity

The Facilitation Committee of the IMO, during its forty-first session from 4 to 7 April 2017, and the Maritime Safety Committee, in its ninety-eighth session from 7 to 16 June 2017, recognizing the critical necessity of enhancing awareness regarding cyber risks and vulnerabilities in maritime operations, endorsed the Guidelines on maritime cyber risk management, outlined in the annex of the Guidelines on Maritime Cyber Risk Management.

- These Guidelines provide high-level recommendations for maritime cyber risk management. For these Guidelines, maritime cyber risk refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.
- Stakeholders should take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping.
- For details and guidance related to the development and implementation of specific risk management processes, users of the Guidelines should refer to specific Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.
- Risk management is fundamental to safe and secure shipping operations. Risk management has traditionally been focused on operations in the physical domain, but greater reliance on digitization, integration, automation and network-based systems has created an increasing need for cyber risk management in the shipping industry.

[3] https://csrc.nist.gov/projects/risk-management/about-rmf

- Predicated on the goal of supporting safe and secure shipping, which is operationally resilient to cyber risks, these Guidelines provide recommendations that can be incorporated into existing risk management processes. In this regard, the Guidelines are complementary to the safety and security management practices established by this Organization **(MSC FAL.1/Circ. 3, 2017, p. 1).**

The annex to Guidelines on Maritime Cyber Risk Management defines also the best practices for implementation of cyber risk practices:

- The approach to cyber risk management described herein provides a foundation for better understanding and managing cyber risks, thus enabling a risk management approach to address cyber threats and vulnerabilities. For detailed guidance on cyber risk management, users of these Guidelines should also refer to Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.
- Additional guidance and standards may include, but are not limited to:
    - The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.
    - ISO/IEC 27001 standard on Information technology – Security techniques –Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
    - United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework).
- Reference should be made to the most current version of any guidance or standards utilized (**MSC FAL.1/Circ.3, 2017, p. 4)**.

6.3 Identification of potential risks in maritime systems

Activities for identifying risks will support the security and safety requirements elicitation. However, the effectiveness of risk identification hinges on the elicitation of requirements, as this process establishes the necessary domain knowledge for risk identification. The elicitation of requirements generates models and requirements, which are then utilized in risk identification activities to pinpoint hazards and threats. These findings are looped back into the requirements elicitation process as safety and security requirements. It is important to note that the domain knowledge about the system and environment is provided during the requirements elicitation process, which is then translated into requirements and models serving as the foundation for system development. These requirements and models are also shared with stakeholders during risk identification activities, but the stakeholder input in these activities is focused on potential system failures within the environment [71].

HAZID [72] is a broad term used to denote an exercise aimed at recognizing hazards and associated events that could lead to significant consequences. For instance, a HAZID of an offshore petroleum facility might be conducted to pinpoint potential hazards that could result in personnel injuries, environmental damage such as oil spills, or financial losses like production delays. The HAZID technique can be applied to different parts of a facility or vessel or even operational procedures. The process typically involves breaking down the system into manageable segments and leading a team through a brainstorming session, often utilizing checklists, to identify potential hazards associated with each segment. This process is usually facilitated by

a team experienced in the design and operation of the facility, with significant hazards prioritized for further evaluation.

The HAZOP [72] analysis technique employs specific guidewords to prompt a seasoned group of individuals to identify potential hazards or operability issues related to equipment or systems. Guidewords describing potential deviations from design intent are created by applying predefined adjectives (e.g., high, low, no) to established process parameters (e.g., flow, pressure, composition). The group then brainstorms potential consequences of these deviations, ensuring appropriate safeguards are in place to prevent them. This analysis primarily generates qualitative results, although some level of quantification is possible. HAZOP is primarily used for identifying safety hazards and operability issues in continuous process systems, especially fluid and thermal systems.

Furthermore, in any hazard identification and risk assessment endeavour, it is crucial to consider the interface between human operators and the systems they operate. Human Factors Engineering (HFE) issues can be integrated into hazard identification, risk assessment, and the determination of safety measure reliability. Understanding human psychology is essential for estimating the effectiveness of procedural controls and emergency response systems. Risk analysts need to be aware of the impact of human factors, and training can enhance their ability to recognize potential human contributions to risk. It is equally vital to acknowledge human contributions to risk even when human activity is implicit in risk control measures. For example, a risk assessment of a boiler would identify "overpressure" as a hazard that could lead to rupture and explosion. Checklists of common errors or audits of the management system for operator training are methods used to address the potential for human error and ensure it is adequately controlled. The purpose of any tool is to identify potential errors and determine how they are prevented [73].

6.4 Assessment and prioritization of risks

The risk management process outlined in ISO 31000 consists of five sub-processes [15]:

- Establishing the external and internal context for cyber security risk management involves setting fundamental criteria for cyber security risk management, defining scope and boundaries, and establishing an appropriate organization to oversee cyber security risk management.
- Risks are assessed through identification, quantification, or qualitative description, and prioritization against relevant risk evaluation criteria and organizational objectives, a process known as risk assessment.
- Controls to mitigate, retain, avoid, or transfer risks are selected, and a risk treatment plan is formulated.
- Exchange and sharing of risk information occur between decision-makers and stakeholders.
- Risks and their components are monitored and reviewed to detect early changes and maintain a comprehensive view of the overall risk landscape. This iterative nature of the cyber security risk management process enables continuous assessment and treatment of risks.

The risk identification has been previously addressed, therefore this subchapter will focus on the quantification, or qualitative description, as part of the risk assessment procedure, and the prioritization of risks [74].

Quantitative risk assessment employs mathematical methodologies and regulations to assign a numerical value, typically within the [1-x] range, to each risk. These outcomes are less subjective compared to the quantitative assessment, thus facilitating a more effective selection of controls. However, they may pose challenges in communication to decision-makers who lack technical expertise.

Quantitative risk analysis seeks to attribute tangible numerical values to components of risk assessment, such as impact and likelihood. When evaluating cyber risks based on the probability of potential attacks, the resulting rating numbers and values may lead to confusion and disagreement among stakeholders involved in the risk management process. DREAD aims to address these challenges by quantifying distinct facets (Damage potential, Reproducibility, Exploitability, Affected systems, and Discoverability) of security threats and attacks, employing formulas to assign meaningful numerical values to the risk elements.

$$Impact = \frac{\sum(Damage, Affectedsystems)}{2},$$

$$Likelihood = \frac{\sum(Reproducibility, Exploitability, Discoverability)}{3},$$

$$Risk = \frac{(Impact + Likelihood)}{2}.$$

In contrast, qualitative risk assessment relies on employing non-numerical approaches and assigning a qualitative value to each risk, typically denoted as low, medium, or high. This approach yields a finite set of outcomes, yet these are more easily understood by decision-makers. [75]

One such method is STRIDE, a threat modelling technique encapsulated by the initials of six security threats: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges.

Both impact and likelihood criteria are employed to adequately evaluate identified risks. The categorization of these criteria is outlined in the table below.

Table 8: Impact and likelihood criteria

Impact Criteria	
High	Significant financial damage to the shipping company; or physical damage to the infrastructure; or loss of human life.
Medium	Financial damage to the shipping company; or disruption of operations; or legal sanctions; or breach of the confidentiality, integrity or availability of information.
Low	Delay of non-critical operations; or breach of the confidentiality, integrity or availability of non-sensitive information.
Likelihood Criteria	
Very Likely	Existence of highly motivated and capable attackers and no controls in place; or wide availability of exploits; or high exposure of the system to the internet.
Moderate	Existence of highly motivated and capable attackers and inadequate controls in place; or wide availability of exploits that require physical access; indirect exposure of the system to the internet.
Rare	Absence of highly motivated and capable attackers; or adequate controls in place; no exposure of the system to the internet.

Finally, semi-quantitative risk assessment blends both rules and methodologies to evaluate risk by integrating numerical values and levels. For instance, the [1-x] range can be conveniently transformed into qualitative expressions, facilitating effective risk communication with decision-makers.

Risk prioritization is a crucial aspect of cybersecurity risk management in the maritime industry. It involves assessing and ranking risks based on their potential impact and likelihood of occurrence. Risk prioritization can be approached in maritime cybersecurity through the following steps [76]:

- Impact Assessment:
  - Evaluate the potential consequences of each risk, considering its effects on vessel operations, crew safety, environmental compliance, financial stability, and regulatory adherence.
  - Categorize risks according to their severity, distinguishing between those with low, moderate, and high impacts.
  - Prioritize risks that could cause significant harm or disruption to maritime activities.
- Likelihood Assessment:
  - Gauge the probability of each risk occurring based on various factors, such as historical data, industry trends, threat intelligence, and the effectiveness of current security measures.
  - Assess the likelihood of risks on a scale of low, moderate, and high probabilities.
- Risk Scoring:
  - Assign numerical scores to risks based on both their impact and likelihood assessments.
  - Utilize established scoring systems like CVSS or the DREAD model to quantify and compare risks.
  - Combine impact and likelihood scores to derive an overall risk score for each identified risk.
- Risk Ranking:
  - Arrange risks in order of priority based on their overall risk scores, with higher scores indicating greater urgency for mitigation.
  - Maintain a risk register or matrix to track prioritized risks along with their scores, rankings, and planned mitigation actions.
  - Focus initial efforts on addressing the most critical risks to ensure efficient resource allocation.
- Risk Treatment:
  - Develop and implement tailored risk treatment plans for high-priority risks.
  - Deploy mitigation measures specific to each risk's characteristics and organizational context.
  - Continuously monitor the effectiveness of risk treatments and adjust strategies based on ongoing assessments and reviews.

6.5 Proposed risk mitigation strategies

To mitigate cybersecurity risks in maritime systems, a comprehensive approach is essential, encompassing various facets of vessel operations, communication networks, navigation systems, and shore-based infrastructure. Presented below are recommended risk mitigation strategies tailored specifically to maritime systems [36], [77], [78], [79], [80]:

- Implementing Secure Network Architectures:

  - Employ network segmentation to segregate critical ship systems from non-critical ones, thereby containing the potential impact of breaches.
  - Utilize firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to monitor and regulate network traffic, detecting and thwarting unauthorized access attempts.
- Enhancing Access Controls:
  - Enforce robust authentication mechanisms like multi-factor authentication (MFA) to restrict access to sensitive systems and data.
  - Implement role-based access control (RBAC) to ensure that users are only granted access to resources and functionalities pertinent to their roles.
- Ensuring Software and Firmware Integrity:
  - Regularly update and patch software and firmware to rectify known vulnerabilities and security flaws.
  - Employ code signing and integrity verification mechanisms to validate the legitimacy and integrity of software/firmware updates before deployment.
- Encrypting Data in Transit and at Rest:
  - Employ strong encryption protocols (e.g., SSL/TLS) to encrypt sensitive data transmitted over communication channels.
  - Implement encryption mechanisms to safeguard data stored on on-board systems and removable media, preventing unauthorized access in the event of physical theft or loss.
- Conducting Regular Security Audits and Assessments:
  - Undertake periodic cybersecurity assessments and penetration testing to pinpoint vulnerabilities and evaluate the efficacy of existing security measures.
  - Conduct security audits of on-board systems, communication networks, and shore-based infrastructure to ensure alignment with industry standards and best practices.
- Enhancing Incident Detection and Response Capabilities:
  - Deploy security monitoring tools, such as Security Information and Event Management (SIEM) systems, and conduct log analysis to identify and respond to cybersecurity incidents in real time.
  - Develop and rehearse incident response plans to facilitate prompt and effective responses to security breaches, minimizing their impact on vessel operations.
- Providing Security Awareness Training:
  - Educate crew members, shore-based staff, and third-party vendors on cybersecurity best practices, encompassing topics like phishing awareness, password hygiene, and safe browsing habits.
  - Foster a culture of cybersecurity awareness and accountability across the maritime organization to encourage proactive risk mitigation endeavours.
- Ensuring Physical Security Measures:
  - Implement physical access controls, surveillance systems, and intrusion detection sensors to safeguard on-board systems and equipment against unauthorized tampering or sabotage.
  - Secure on-board infrastructure, such as communication equipment and navigation systems, against physical threats and environmental hazards.

- Through the implementation of these risk mitigation strategies, maritime organizations can bolster the cybersecurity resilience of their systems and networks, thereby mitigating the likelihood and impact of cyber threats on vessel operations, crew safety, and environmental protection endeavours.

6.6 Case studies or examples demonstrating the application of risk management in maritime cybersecurity

This section delves into how a specific shipping company integrates a systemic approach to cybersecurity, while effectively illustrating how maritime companies can integrate comprehensive cybersecurity strategies into their business models, highlighting the importance of systemic approaches to manage cyber risks within the industry. To this end, a case study is presented to illustrate the practical application of cybersecurity policies and measures within the maritime sector. Key highlights are presented below [70]:

- *Company Background*: The case study focuses on a ship management company specializing in oil tankers and bulk carriers. The fleet is substantial, with over 30 vessels and a significant deadweight capacity. The management operates from a central head office, emphasizing the integration of cybersecurity within their operational framework.
- *Cybersecurity as Part of Integrated Management Systems (IMS)*: The company's cybersecurity management is built on the foundational IMS, ensuring continual improvement through the Plan-Do-Check-Act (PDCA) cycle. Cybersecurity is thoroughly embedded into the company's operations, linking directly with safety, quality, and environmental management systems.
- *PDCA Approach in Detail*: A detailed exploration of how the PDCA cycle is implemented in cybersecurity practices:
  - *Plan*: Identifying cybersecurity objectives and conducting risk assessments.
  - *Do*: Establishing and enforcing cybersecurity policies and procedures.
  - *Check*: Monitoring and evaluating the effectiveness of cybersecurity measures.
  - *Act*: Taking corrective actions and striving for continuous improvement.
- *Risk Assessment*: An in-depth look at how the company conducts cyber risk assessments, which includes identifying threats, estimating risks, and evaluating potential impacts.
- *Three Pillars of Cybersecurity Approach*:
  - *Procedures and Policy*: Documentation and administrative controls are discussed, emphasizing the importance of governance in cybersecurity.
  - *Human Factor*: Covering training programs and the role of human behaviour in maintaining cybersecurity.
  - *Infrastructure and Technical Controls*: Focus on the technical measures implemented to protect the company's digital and physical assets.

- *Cyber Security Campaigns and Audits*: The company’s proactive measures for cybersecurity awareness and compliance are also discussed, highlighting regular audits and campaigns to ensure the system's integrity and security.

7 Research Challenges & Directions

This chapter explores the current landscape of maritime cybersecurity by drawing from established literature and previous chapters. Key sources include "Literature Review on Maritime Cybersecurity: State-of-the-Art [4]," "A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry [11]," "Maritime Cybersecurity Threats: Gaps and Directions for Future Research [5]," and "Maritime Cyber Security: Concepts, Problems, and Models [9]." By combining these insights with earlier findings, this chapter aims to provide a clear analysis of maritime cybersecurity issues, identify significant research gaps, and suggest directions for future research.

7.1 Identification of Key Research Gaps and Challenges

Ship Diversity and Disparate Environments

The maritime industry faces significant challenges due to the diversity of ships and their disparate operating environments. The variations in installed systems, operational requirements, and security protocols across different classes of ships make it difficult to establish standardised cybersecurity measures. The lack of reliable cybersecurity communication protocols for critical ship equipment like GPS and ECDIS, due to the involvement of heterogeneous vendors and manufacturers, further complicates the situation.

Improper Cybersecurity Risk Assessment

There is a considerable shortcoming in the existing risk assessment of cybersecurity threats within the maritime industry. Different nations, particularly within the EU, implement varying security policies and practices, complicating the comparison and standardization of risk assessments. Specifically, there is a need to compare and standardize the risk assessment methods so as to clarify: (a) whether one prevails over the other and (b) whether different requirements and security practices and policies lead to different assessment methods as best as possible. Moreover, the industry suffers from a lack of trained personnel, with many crew members not adequately equipped to handle cyber risks.

Lack of Real-World Testing and Training

The maritime sector lacks robust real-world testing systems for analysing the impact of cyber-attacks, as well as the efficiency and effectiveness of the known counter-measures. This deficiency makes it difficult to perform comprehensive risk assessments and develop effective mitigation strategies. Additionally, there is a significant gap in the training and education of maritime professionals regarding cybersecurity. The current

curriculum does not adequately cover the latest cyber threats, leaving personnel unprepared for potential cyber incidents.

Inadequate Laws and Policies

Existing laws and regulations at both national and international levels are insufficient to address the unique challenges of maritime cybersecurity. The abstract and general nature of current legislation does not provide clear directives for ship owners and managers on how to effectively implement cybersecurity measures. This gap leads to vulnerabilities that could be exploited by cyber attackers. Furthermore, the current legislation is not uniformly stringent enough to effectively deter cyber-criminals from carrying out maritime cyber-attacks.

Increased Dependence on Cyber Technology

The growing dependence on cyber technology in the maritime industry has increased its vulnerability to cyber-attacks, since the attack surface is now greater. Recent automation and digitisation have integrated IT and OT systems more closely, exposing critical operations to various cyber threats. The integration of IT and OT is not perfect, leading to security gaps where outdated operational technology (OT) may not be adequately protected by traditional IT security measures. Additionally, the non-secure development of systems, software, and services is a major issue. Many systems are deployed with vulnerabilities due to rushed development cycles or insufficient security testing, making the industry an attractive target for cyber attackers

7.2 Promising Research Directions for Addressing These Gaps

Development of Standardized Cybersecurity Protocols

To address the diversity and disparate environments of ships, research should focus on developing standardized cybersecurity protocols that can be adapted to different classes of ships and operating conditions, such as network security protocols, authentication and access control protocols, endpoint security protocols, data protection protocols, incident response protocols, supply chain security protocols, OT security protocols, training and awareness protocols. This includes creating robust security measures for critical equipment like GPS and ECDIS, ensuring consistent protection across all vessels, including their physical equipment and data.

Enhanced Risk Assessment Models

Improving risk assessment models is crucial for accurately and adequately evaluating cyber threats in the maritime sector. Future research should develop targeted risk assessment procedures that consider the interconnected nature of maritime logistics and supply chain (MLSC) infrastructure. This includes creating comprehensive frameworks for evaluating the cyber resilience of maritime operations and incorporating advanced technologies for real-time risk assessment.

Implementation of Real-World Testing Systems

Investing in real-world testing systems, specific to maritime systems, is essential for understanding the impact of cyber-attacks and developing effective defences. Research should focus on creating dynamic testing

environments that simulate real-world conditions, allowing for thorough penetration testing and vulnerability assessment. Additionally, promoting ethical hacking and the use of penetration testing systems can help prepare for future cyber threats.

Strengthening Training and Education Programs

Updating and expanding cybersecurity education and training programs for maritime professionals is vital. This includes incorporating comprehensive cybersecurity courses into the curriculum of maritime academies and universities, and developing specialized training programs for practical skills in preventing, detecting, and responding to cyber-attacks. Collaboration between educational institutions and industry is also necessary to ensure that training programs are aligned with real-world needs and scenarios.

Legislative and Policy Improvements

Research should focus on reviewing and revising existing laws and policies to make them more specific and descriptive, providing clear directives for maritime operators. This involves establishing detailed cybersecurity standards and responsibilities, promoting existing international cybersecurity standards, and developing regulations that address the unique challenges of maritime cybersecurity. Additionally, enhancing the legal framework to support effective risk assessment and mitigation strategies, as well as impose harsher sentences for cyber-criminals is crucial.

Adoption of Emerging Technologies

Exploring the potential of emerging technologies like AI, satellite IoT[4] and high-altitude platform (HAP)[5] solutions can significantly enhance maritime cybersecurity. These technologies can provide supplementary communication channels, reducing the reliance on vulnerable systems, such as GPS, and improving overall resilience. Research should focus on integrating these technologies into maritime operations and evaluating their effectiveness in mitigating cyber risks.

Collaborative Efforts and Information Sharing

Promoting better collaboration and information sharing among stakeholders in the maritime industry is essential for enhancing cybersecurity measures. Research should develop frameworks for sharing threat intelligence and best practices, and encourage public-private partnerships to leverage resources, expertise, and technologies. Creating platforms for real-time information sharing and coordinated responses to cyber threats can significantly improve the industry's resilience.

[4] Satellite IoT refers to the use of satellite communication technology to connect Internet of Things (IoT) devices, enabling data transmission and connectivity in remote and geographically isolated areas where traditional terrestrial networks are unavailable.

[5] High-altitude platform solutions involve the use of aircraft, balloons, or airships positioned in the stratosphere to provide communication services and network coverage, acting as a bridge between satellites and ground-based networks to enhance connectivity in underserved regions.

By addressing these research directions, the maritime industry can build a robust cybersecurity framework that effectively mitigates risks and ensures the safety and security of maritime operations in the digital age.

8 *Conclusions*

This thesis makes significant contributions to the field of maritime cybersecurity by providing a comprehensive analysis of the current cybersecurity landscape within the maritime sector. First, it offers a detailed taxonomy of maritime cybersecurity vulnerabilities, threats, and attacks. Second, it includes an extensive classification and comparison of identified countermeasures and risk management techniques to assist in their selection based on organizational requirements and preferences as well as the identification of key research gaps and the presentation of promising research directions, aiming to enhance the development of safer and more resilient maritime systems. By integrating cybersecurity implementation requirements into the regulatory framework, this research highlights the critical role of cybersecurity in ensuring maritime safety and security.

Through this research, valuable experience has been gained in understanding the complexities and challenges associated with maritime cybersecurity. The process involved a thorough review of existing literature, a detailed analysis of real-world cyber incidents, and an evaluation of current countermeasures and risk management techniques. This experience has underscored the importance of a multidisciplinary approach, combining insights from cybersecurity, maritime operations, and regulatory frameworks to address the unique challenges faced by the maritime industry.

Key Findings

- *Diversity and Complexity of Maritime Systems*: The maritime industry comprises a diverse range of systems and environments, making it difficult to establish standardized cybersecurity measures. This complexity is exacerbated by the integration of legacy systems with modern technologies.
- *Significant Rise in Cyberattacks*: There has been a 900% increase in cybersecurity breaches targeting operational technology in the maritime sector over the past few years, highlighting the urgent need for robust cybersecurity measures.
- *Lack of Proper Cybersecurity Training*: The current curriculum in maritime training institutions is insufficiently aligned with modern cybersecurity challenges, leading to a significant knowledge gap among maritime professionals.
- *Insufficient Legal and Regulatory Frameworks*: Existing national and international laws are inadequate for addressing the unique challenges of maritime cybersecurity.
- *Emerging Technologies and their Impact*: The integration of emerging technologies, such as satellite IoT and high-altitude platform solutions, can enhance maritime cybersecurity but might also introduce new vulnerabilities that need to be identified and addressed.

Research Priorities for the Immediate Future

- *Development of Standardized Cybersecurity Protocols*: Future research should focus on developing and implementing standardized cybersecurity protocols tailored to the diverse range of maritime

systems and operating conditions. Key protocols are network security protocols, authentication and access control protocols, endpoint security protocols, data protection protocols, incident response protocols, supply chain security protocols, OT security protocols, training and awareness protocols.

- *Enhanced Cybersecurity Training Programs*: There is an urgent need to update and expand cybersecurity education and training programs for maritime professionals. Collaboration between educational institutions and industry is essential to ensure that training programs are aligned with real-world needs and scenarios.
- *Improvement of Legal and Regulatory Frameworks*: Research should aim to review and revise existing laws and regulations to provide clearer and more specific directives for maritime operators. This includes promoting the adoption of international cybersecurity standards and best practices.
- *Adoption of Emerging Technologies*: Exploring the potential of emerging technologies, such as AI, satellite IoT and high-altitude platform solutions, to enhance maritime cybersecurity. Research should evaluate the effectiveness of these technologies in mitigating cyber risks and integrating them into maritime operations. It should also investigate whether the integration of such technologies might lead to new vulnerabilities and devise proper solutions to resolve them.
- *Promotion of Collaborative Efforts*: Enhancing collaboration and information sharing among stakeholders in the maritime industry is crucial. Developing frameworks for real-time information sharing and coordinated responses to cyber threats can significantly improve the industry's resilience.

By addressing these research priorities, the maritime industry can build a robust cybersecurity framework that effectively mitigates risks and ensures the safety and security of maritime operations in the digital age.

Bibliography

[1] F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, and M. Michaloliakos, "Cybersecurity Challenges in the Maritime Sector," *Network*, vol. 2, no. 1, pp. 123–138, Mar. 2022, doi: 10.3390/network2010009.

[2] T. Koukaki and A. Tei, "Innovation and maritime transport: A systematic review," *Case Studies on Transport Policy*, vol. 8, no. 3, pp. 700–710, Sep. 2020, doi: 10.1016/j.cstp.2020.07.009.

[3] A. Androjna, T. Brcko, I. Pavic, and H. Greidanus, "Assessing Cyber Challenges of Maritime Navigation," *JMSE*, vol. 8, no. 10, p. 776, Oct. 2020, doi: 10.3390/jmse8100776.

[4] H. Yu, Q. Meng, Z. Fang, and J. Liu, "Literature review on maritime cybersecurity: state-of-the-art," *J. Navigation*, vol. 76, no. 4–5, pp. 453–466, Jul. 2023, doi: 10.1017/S0373463323000164.

[5] M. Afenyo and L. D. Caesar, "Maritime cybersecurity threats: Gaps and directions for future research," *Ocean & Coastal Management*, vol. 236, p. 106493, Apr. 2023, doi: 10.1016/j.ocecoaman.2023.106493.

[6] Joint Task Force Interagency Working Group, "Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, Sep. 2020. doi: 10.6028/NIST.SP.800-53r5.

[7] K. Wolsing, L. Roepert, J. Bauer, and K. Wehrle, "Anomaly Detection in Maritime AIS Tracks: A Review of Recent Approaches," *JMSE*, vol. 10, no. 1, p. 112, Jan. 2022, doi: 10.3390/jmse10010112.

[8] A. Amro, A. Oruc, V. Gkioulos, and S. Katsikas, "Navigation Data Anomaly Analysis and Detection," *Information*, vol. 13, no. 3, p. 104, Feb. 2022, doi: 10.3390/info13030104.

[9] S. Lagouvardou, "Maritime Cyber Security: concepts, problems and models".

[10] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electronics*, vol. 12, no. 6, p. 1333, Mar. 2023, doi: 10.3390/electronics12061333.

[11] I. Ashraf *et al.*, "A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry," *IEEE Trans. Intell. Transport. Syst.*, pp. 1–14, 2022, doi: 10.1109/TITS.2022.3164678.

[12] M. A. Ben Farah *et al.*, "Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends," *Information*, vol. 13, no. 1, p. 22, Jan. 2022, doi: 10.3390/info13010022.

[13] J. I. Alcaide and R. G. Llave, "Critical infrastructures cybersecurity and the maritime sector," *Transportation Research Procedia*, vol. 45, pp. 547–554, 2020, doi: 10.1016/j.trpro.2020.03.058.

[14] A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," *Procedia Economics and Finance*, vol. 28, pp. 24–31, 2015, doi: 10.1016/S2212-5671(15)01077-1.

[15] G. Kavallieratos, "Security of the Cyber Enabled Ship".

[16] R. E. Rey-Charlo, J. L. Cueto, and F. Piniella, "Analyzing Port State Control Data to Explore Future Improvements to GMDSS Training," *JMSE*, vol. 11, no. 12, p. 2379, Dec. 2023, doi: 10.3390/jmse11122379.

[17] I. Surinov and D. S. Shumilov, "Cybersecurity of the Processes of Manoeuvring in Confined Waters," *TransNav*, vol. 17, no. 3, pp. 723–732, 2023, doi: 10.12716/1001.17.03.25.

[18] R. Skoglund, "Perceived Information Security in the Maritime Sector".

[19] A. Thomas, "Maritime Cybersecurity: AIS Manipulation Motivations in the Maritime Domain".

[20] O. Soner, G. Kayisoglu, P. Bolat, and K. Tam, "Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks," *Applied Ocean Research*, vol. 142, p. 103855, Jan. 2024, doi: 10.1016/j.apor.2023.103855.

[21] G. Longo, E. Russo, A. Armando, and A. Merlo, "Attacking (and Defending) the Maritime Radar System," *IEEE Trans.Inform.Forensic Secur.*, vol. 18, pp. 3575–3589, 2023, doi: 10.1109/TIFS.2023.3282132.

[22] B. Svilicic, D. Brčic, S. ŽuŁkin, and D. Kalebic, "Raising Awareness on Cyber Security of ECDIS," *TransNav*, vol. 13, no. 1, pp. 231–236, 2019, doi: 10.12716/1001.13.01.24.

[23] Constanta Maritime University, R. Zagan, G. Raicu, Constanta Maritime University, A. Sabau, and Constanta Maritime University, "STUDIES AND RESEARCH REGARDING VULNERABILITIES OF MARINE AUTONOMOUS SURFACE SYSTEMS (MASS) AND REMOTELY OPERATED VESSELS (ROVS) FROM POINT OF VIEW OF CYBERSECURITY," *IJMMT*, vol. 14, no. 3, pp. 310–318, Dec. 2022, doi: 10.54684/ijmmt.2022.14.3.310.

[24] W. C. Leite Junior, C. C. De Moraes, C. E. P. De Albuquerque, R. C. S. Machado, and A. O. De Sá, "A Triggering Mechanism for Cyber-Attacks in Naval Sensors and Systems," *Sensors*, vol. 21, no. 9, p. 3195, May 2021, doi: 10.3390/s21093195.
[25] N. Dimitrov, C. Alexandrov, and M. Todorov, "CYBER SECURITY ANALYSIS OF MARITIME SURVEILLANCE SYSTEMS".
[26] A. Oruc, V. Gkioulos, and S. Katsikas, "Towards a Cyber-Physical Range for the Integrated Navigation System (INS)," *JMSE*, vol. 10, no. 1, p. 107, Jan. 2022, doi: 10.3390/jmse10010107.
[27] X.-Y. Zhou, Z.-J. Liu, F.-W. Wang, and Z.-L. Wu, "A system-theoretic approach to safety and security co-analysis of autonomous ships," *Ocean Engineering*, vol. 222, p. 108569, Feb. 2021, doi: 10.1016/j.oceaneng.2021.108569.
[28] M. S. K. Awan and M. A. Al Ghamdi, "Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS)," *JMSE*, vol. 7, no. 10, p. 350, Oct. 2019, doi: 10.3390/jmse7100350.
[29] G. Kayisoglu, P. Bolat, and K. Tam, "Evaluating SLIM-based human error probability for ECDIS cybersecurity in maritime," *J. Navigation*, vol. 75, no. 6, pp. 1364–1388, Nov. 2022, doi: 10.1017/S0373463322000534.
[30] B. Svilicic, M. Kristić, S. Žuškin, and D. Brčić, "Paperless ship navigation: cyber security weaknesses," *J Transp Secur*, vol. 13, no. 3–4, pp. 203–214, Dec. 2020, doi: 10.1007/s12198-020-00222-2.
[31] B. Svilicic, I. Rudan, V. Frančić, and M. Doričić, "Shipboard ECDIS Cyber Security: Third-Party Component Threats," *Pomorstvo (Online)*, vol. 33, no. 2, pp. 176–180, Dec. 2019, doi: 10.31217/p.33.2.7.
[32] K. Tam and K. D. Jones, "Situational Awareness: Examining Factors that Affect Cyber-Risks in the Maritime Sector," *IJCSA*, vol. 4, no. 1, pp. 40–68, Dec. 2019, doi: 10.22619/IJCSA.2019.100125.
[33] B. Svilicic, I. Rudan, A. Jugović, and D. Zec, "A Study on Cyber Security Threats in a Shipboard Integrated Navigational System," *JMSE*, vol. 7, no. 10, p. 364, Oct. 2019, doi: 10.3390/jmse7100364.
[34] J. Wang, Y. Xiao, T. Li, and C. L. P. Chen, "A Survey of Technologies for Unmanned Merchant Ships," *IEEE Access*, vol. 8, pp. 224461–224486, 2020, doi: 10.1109/ACCESS.2020.3044040.
[35] S. D. Ilcev, "Software Solutions for GMDSS Network and Equipment," *TransNav*, vol. 16, no. 3, pp. 463–472, 2022, doi: 10.12716/1001.16.03.07.
[36] I. Progoulakis, P. Rohmeyer, and N. Nikitakos, "Cyber Physical Systems Security for Maritime Assets," *JMSE*, vol. 9, no. 12, p. 1384, Dec. 2021, doi: 10.3390/jmse9121384.
[37] N. A. R. Al Ali, A. A. Chebotareva, and V. E. Chebotarev, "Cyber security in marine transport: opportunities and legal challenges," *Pomorstvo (Online)*, vol. 35, no. 2, pp. 248–255, Dec. 2021, doi: 10.31217/p.35.2.7.
[38] S. Karamperidis, C. Kapalidis, and T. Watson, "Maritime Cyber Security: A Global Challenge Tackled through Distinct Regional Approaches," *JMSE*, vol. 9, no. 12, p. 1323, Nov. 2021, doi: 10.3390/jmse9121323.
[39] V. Koshevyy and A. Shishkin, "Standardization of Interface for VHF, MF/HF Communication Using DSC within Its Integration with INS in the Framework of e-Navigation Concept," *TransNav*, vol. 13, no. 3, pp. 593–596, 2019, doi: 10.12716/1001.13.03.15.
[40] J. Pawelski, "Cyber Threats for Present and Future Commercial Shipping," *TransNav*, vol. 17, no. 2, pp. 261–267, 2023, doi: 10.12716/1001.17.02.01.
[41] O. Onishchenko, K. Shumilova, S. Volyanskyy, Y. Volyanskaya, and Y. Volianskyi, "Ensuring Cyber Resilience of Ship Information Systems," *TransNav*, vol. 16, no. 1, pp. 43–50, 2022, doi: 10.12716/1001.16.01.04.
[42] I. Progoulakis, N. Nikitakos, D. Dalaklis, A. Christodoulou, A. Dalaklis, and R. Yaacob, "Digitalization and Cyber Physical Security Aspects in Maritime Transportation and Port Infrastructure," in *Smart Ports and Robotic Systems*, T. M. Johansson, D. Dalaklis, J. E. Fernández, A. Pastra, and M. Lennan, Eds., in Studies in National Governance and Emerging Technologies. , Cham: Springer International Publishing, 2023, pp. 227–248. doi: 10.1007/978-3-031-25296-9_12.
[43] K. Kanwal, W. Shi, C. Kontovas, Z. Yang, and C.-H. Chang, "Maritime cybersecurity: are onboard systems ready?," *Maritime Policy & Management*, vol. 51, no. 3, pp. 484–502, Apr. 2024, doi: 10.1080/03088839.2022.2124464.
[44] G. Kalogeras, "Navigating the Waters of Maritime Cybersecurity with BIMCO's Guidelines: Identifying Vulnerabilities and Mitigating Threats to IT and OT Systems".
[45] Y. Jo, O. Choi, J. You, Y. Cha, and D. H. Lee, "Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework," *Sensors*, vol. 22, no. 5, p. 1860, Feb. 2022, doi: 10.3390/s22051860.
[46] T. Pseftelis and G. Chondrokoukis, "A Study about the Role of the Human Factor in Maritime Cybersecurity," vol. 71, no. 1, 2021.

[47] B. Mednikarov, Y. Tsonev, and A. Lazarov, "Analysis of Cybersecurity Issues in the Maritime Industry," *ISIJ*, vol. 47, no. 1, pp. 27–43, 2020, doi: 10.11610/isij.4702.
[48] K. Aboul-Dahab, "DEMONSTRATING THE CYBER VULNERABILITIES OF SIGNIFICANT MARITIME TECHNOLOGIES TO THE PORT FACILITIES AND ON BOARD OF VESSELS," *SSRN Journal*, 2020, doi: 10.2139/ssrn.3816734.
[49] A. Bielawski and A. Lazarowska, "Discussing cybersecurity in maritime transportation," *Marit. Technol. Res.*, vol. 4, no. 1, p. 252151, Aug. 2021, doi: 10.33175/mtr.2022.252151.
[50] A. Androjna and M. Perkovič, "Impact of Spoofing of Navigation Systems on Maritime Situational Awareness," *Trans. Marit. Sci.*, vol. 10, no. 2, pp. 361–373, Oct. 2021, doi: 10.7225/toms.v10.n02.w08.
[51] Senior researcher, Korea Maritime Institute, Busan, 49111, Korea, S. Park, Y. Chang, and Y. Park, "Importance–Performance Analysis (IPA) of Cyber Security Management: Focused on ECDIS User Experience," *J. Korean Soc. Mar. Environ. Saf.*, vol. 27, no. 3, pp. 429–438, May 2021, doi: 10.7837/kosomes.2021.27.3.429.
[52] F. Martínez, L. E. Sànchez, A. Santos-Olmo, D. G. Rosado, and E. Fernàndez-Medina, "Maritime cybersecurity: protecting digital seas," *Int. J. Inf. Secur.*, vol. 23, no. 2, pp. 1429–1457, Apr. 2024, doi: 10.1007/s10207-023-00800-0.
[53] P. J. Harju, "Cyber Threats in Maritime Container Terminal Automation Systems".
[54] G. Potamos, S. Theodoulou, E. Stavrou, and S. Stavrou, "Maritime Cyber Threats Detection Framework: Building Capabilities," in *Information Security Education - Adapting to the Fourth Industrial Revolution*, vol. 650, L. Drevin, N. Miloslavskaya, W. S. Leung, and S. Von Solms, Eds., in IFIP Advances in Information and Communication Technology, vol. 650. , Cham: Springer International Publishing, 2022, pp. 107–129. doi: 10.1007/978-3-031-08172-9_8.
[55] O. Polikarovskykh, Y. Daus, D. Larin, and M. Tkachenko, "Systematization of Cyber Threats in Maritime Transport," *SISIOT*, no. 1, p. 01008, Jun. 2023, doi: 10.31861/sisiot2023.1.01008.
[56] M. Caprolu, R. D. Pietro, S. Raponi, S. Sciancalepore, and P. Tedeschi, "Vessels Cybersecurity: Issues, Challenges, and the Road Ahead," *IEEE Commun. Mag.*, vol. 58, no. 6, pp. 90–96, Jun. 2020, doi: 10.1109/MCOM.001.1900632.
[57] S. Khandker, H. Turtiainen, A. Costin, and T. Hamalainen, "Cybersecurity Attacks on Software Logic and Error Handling Within AIS Implementations: A Systematic Testing of Resilience," *IEEE Access*, vol. 10, pp. 29493–29505, 2022, doi: 10.1109/ACCESS.2022.3158943.
[58] G. Longo, A. Merlo, A. Armando, and E. Russo, "Electronic Attacks as a Cyber False Flag against Maritime Radars Systems," in *2023 IEEE 48th Conference on Local Computer Networks (LCN)*, Daytona Beach, FL, USA: IEEE, Oct. 2023, pp. 1–6. doi: 10.1109/LCN58197.2023.10223370.
[59] J. Spravil, C. Hemminghaus, M. Von Rechenberg, E. Padilla, and J. Bauer, "Detecting Maritime GPS Spoofing Attacks Based on NMEA Sentence Integrity Monitoring," *JMSE*, vol. 11, no. 5, p. 928, Apr. 2023, doi: 10.3390/jmse11050928.
[60] V. Bolbot, O. Methlouthi, O. V. Banda, L. Xiang, Y. Ding, and P. Brunou, "Identification of cyber-attack scenarios in a marine Dual-Fuel engine," in *Trends in Maritime Technology and Engineering Volume 1*, 1st ed., London: CRC Press, 2022, pp. 503–510. doi: 10.1201/9781003320272-56.
[61] P. Björnlund and F. Faqiri, "Survey of ongoing and Next- Generation Cybersecurity of Maritime Communication Sys- tems".
[62] A. Yousaf and J. Zhou, "From sinking to saving: MITRE ATT &CK and D3FEND frameworks for maritime cybersecurity," *Int. J. Inf. Secur.*, vol. 23, no. 3, pp. 1603–1618, Jun. 2024, doi: 10.1007/s10207-024-00812-4.
[63] C. Hemminghaus, J. Bauer, and E. Padilla, "BRAT: A BRidge Attack Tool for Cyber Security Assessments of Maritime Systems," *TransNav*, vol. 15, no. 1, pp. 35–44, 2021, doi: 10.12716/1001.15.01.02.
[64] A. Oruc, A. Amro, and V. Gkioulos, "Assessing Cyber Risks of an INS Using the MITRE ATT&CK Framework," *Sensors*, vol. 22, no. 22, p. 8745, Nov. 2022, doi: 10.3390/s22228745.
[65] A. Oruc and M. M. MIMarEST, "Claims of State-Sponsored Cyberattack in the Maritime Industry".
[66] A. Nganga, G. Nganya, M. Lützhöft, S. Mallam, and J. Scanlan, "Bridging the Gap: Enhancing Maritime Vessel Cyber Resilience through Security Operation Centers," *Sensors*, vol. 24, no. 1, p. 146, Dec. 2023, doi: 10.3390/s24010146.
[67] I. Mraković and R. Vojinović, "Maritime Cyber Security Analysis – How to Reduce Threats?," *ToMS*, vol. 8, no. 1, pp. 132–139, Apr. 2019, doi: 10.7225/toms.v08.n01.013.
[68] G. Kavallieratos, V. Diamantopoulou, and S. K. Katsikas, "Shipping 4.0: Security Requirements for the Cyber-Enabled Ship," *IEEE Trans. Ind. Inf.*, vol. 16, no. 10, pp. 6617–6625, Oct. 2020, doi: 10.1109/TII.2020.2976840.

[69] K. Hiekata, S. Wanaka, T. Mitsuyuki, R. Ueno, R. Wada, and B. Moser, "Systems analysis for deployment of internet of things (IoT) in the maritime industry," *J Mar Sci Technol*, vol. 26, no. 2, pp. 459–469, Jun. 2021, doi: 10.1007/s00773-020-00750-5.
[70] E. P. Kechagias, G. Chatzistelios, G. A. Papadopoulos, and P. Apostolou, "Digital transformation of the maritime industry: A cybersecurity systemic approach," *International Journal of Critical Infrastructure Protection*, vol. 37, p. 100526, Jul. 2022, doi: 10.1016/j.ijcip.2022.100526.
[71] C. Raspotnig and A. Opdahl, "Comparing risk identification techniques for safety and security requirements," *Journal of Systems and Software*, vol. 86, no. 4, pp. 1124–1151, Apr. 2013, doi: 10.1016/j.jss.2012.12.002.
[72] D. N. A. Siddiqui, A. Nandan, M. Sharma, and A. Srivastava, "Risk Management Techniques HAZOP & HAZID Study," vol. 1, no. 1.
[73] S. Lampreia, V. Lobo, and V. Vairinhos, "Cybersecurity Risk Assessment: the Ship Maintenance Databases' Case Study," vol. 5, no. 2, 2022.
[74] A. Oruc, G. Kavallieratos, V. Gkioulos, and S. Katsikas, "Cyber Risk Assessment for SHips (CRASH)," *TransNav*, vol. 18, no. 1, pp. 115–124, 2024, doi: 10.12716/1001.18.01.10.
[75] G. Kavallieratos and S. Katsikas, "Managing Cyber Security Risks of the Cyber-Enabled Ship," *JMSE*, vol. 8, no. 10, p. 768, Sep. 2020, doi: 10.3390/jmse8100768.
[76] Joint Task Force Transformation Initiative, "Guide for conducting risk assessments," National Institute of Standards and Technology, Gaithersburg, MD, NIST SP 800-30r1, 2012. doi: 10.6028/NIST.SP.800-30r1.
[77] K. Dittmann and M. Blanke, "Risk mitigation by design of autonomous maritime automation systems: Design of autonomous maritime systems," *at - Automatisierungstechnik*, vol. 70, no. 5, pp. 469–481, May 2022, doi: 10.1515/auto-2021-0151.
[78] R. Puisa, J. McNay, and J. Montewka, "Maritime safety: Prevention versus mitigation?," *Safety Science*, vol. 136, p. 105151, Apr. 2021, doi: 10.1016/j.ssci.2020.105151.
[79] J. Shen, X. Ma, and W. Qiao, "A Model to Evaluate the Effectiveness of the Maritime Shipping Risk Mitigation System by Entropy-Based Capability Degradation Analysis," *IJERPH*, vol. 19, no. 15, p. 9338, Jul. 2022, doi: 10.3390/ijerph19159338.
[80] P. Vistiaho, "Maritime Cyber Security Incident Data Reporting for Autonomous Ships".