information

MDPI

Review

Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains

Maria Valentina Clavijo Mesa [1], Carmen Elena Patino-Rodriguez [2,*] and Fernando Jesus Guevara Carazas [3]

[1] Energy Department, Politecnico di Milano, 20156 Milan, Italy; mariavalentina.clavijo@polimi.it
[2] Industrial Engineering, Universidad de Antioquia, Medellín 050010, Colombia
[3] Mechanical Engineering, Universidad Nacional, Medellín 050034, Colombia; fguevarac@unal.edu.co
* Correspondence: elena.patino@udea.edu.co

Abstract: The maritime industry is constantly evolving and posing new challenges, especially with increasing digitalization, which has raised concerns about cyber-attacks on maritime supply chain agents. Although scholars have proposed various methods and classification models to counter these cyber threats, a comprehensive cyber-attack taxonomy for maritime supply chain actors based on a systematic literature review is still lacking. This review aims to provide a clear picture of common cyber-attacks and develop a taxonomy for their categorization. In addition, it outlines best practices derived from academic research in maritime cybersecurity using PRISMA principles for a systematic literature review, which identified 110 relevant journal papers. This study highlights that distributed denial of service (DDoS) attacks and malware are top concerns for all maritime supply chain stakeholders. In particular, shipping companies are urged to prioritize defenses against hijacking, spoofing, and jamming. The report identifies 18 practices to combat cyber-attacks, categorized into information security management solutions, information security policies, and cybersecurity awareness and training. Finally, this paper explores how emerging technologies can address cyber-attacks in the maritime supply chain network (MSCN). While Industry 4.0 technologies are highlighted as significant trends in the literature, this study aims to equip MSCN stakeholders with the knowledge to effectively leverage a broader range of emerging technologies. In doing so, it provides forward-looking solutions to prevent and mitigate cyber-attacks, emphasizing that Industry 4.0 is part of a larger landscape of technological innovation.

Keywords: maritime supply chain; cyber risk; cybersecurity; cyber-attacks; Industry 4.0

check for updates

Citation: Clavijo Mesa, M.V.; Patino-Rodriguez, C.E.; Guevara Carazas, F.J. Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains. *Information* **2024**, *15*, 710. https://doi.org/10.3390/info15110710

Academic Editor: Libing Wu

Received: 26 August 2024
Revised: 23 September 2024
Accepted: 26 September 2024
Published: 6 November 2024

1. Introduction

Maritime transportation is the primary means of global trade, responsible for approximately 80–90% of the transportation of commodities and raw resources, providing significant economic advantages for moving large quantities over extensive distances [1]. A maritime supply chain network (MSCN) comprises essential elements, including freight forwarders, shipping lines, and port terminal operators, all of which play vital roles in optimizing operations to ensure efficient service delivery. Figure 1, adapted from [2], depicts the connections between these pivotal participants.

In recent decades, as globalization and competitiveness have intensified, it has become crucial for maritime industry stakeholders to implement Industry 4.0 technology. The objective of this transition toward greater digitization and automation is to reduce waiting times and increase efficiency, particularly in complex operations such as ship navigation and cargo management [3,4]. Nevertheless, this digital transformation introduces various new risks, specifically cyber-attacks, which have emerged as a significant concern for MSCN agents [5–7]. The classification society "Lloyd Register" has documented an alarming surge in cyber-attacks over the last ten years, with an annual increase of 27%. In 2017, 86% of organizations reported experiencing attacks [8–10], a situation worsened by the COVID-19 pandemic, leading to a four-fold rise in cyber-attacks globally [10–12].

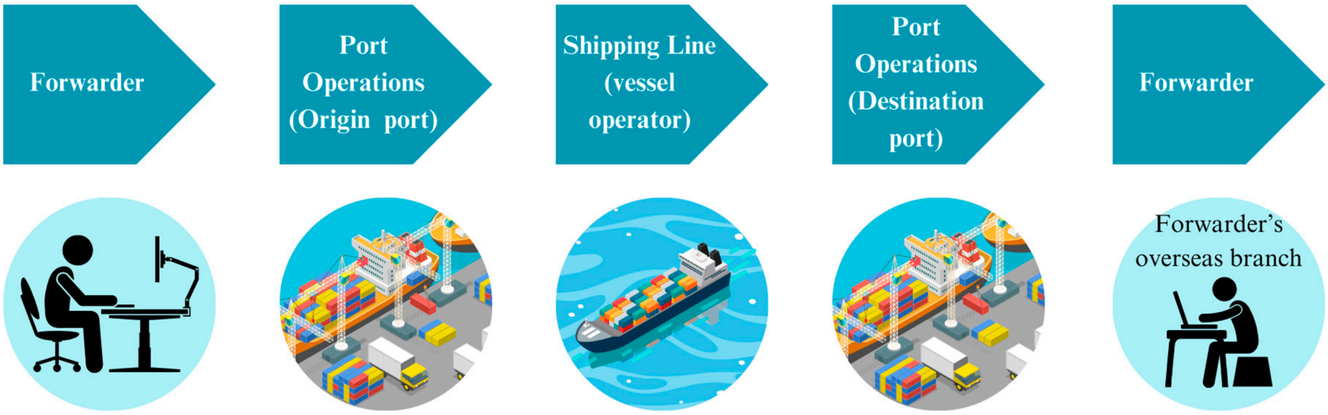
Forwarder
Port Operations (Origin port)
Shipping Line (vessel operator)
Port Operations (Destination port)
Forwarder
Forwarder's overseas branch

Figure 1. MSCN links, adapted from [2].

Considering these challenges, cybersecurity has become a critical concern in the maritime industry. The International Maritime Organization (IMO) mandated in 2021 that shipowners develop cyber risk management strategies [6,13]. Classification societies, such as the American Bureau of Shipping (ABS) and Det Norske Veritas (DNV), have also promoted effective cyber risk management systems to mitigate these threats.

Analyzing cyber-attacks within the MSCN is essential due to the sector's unique operational dynamics and reliance on complex global logistics. The MSCN operates in a highly interconnected environment, where vulnerabilities can rapidly propagate among multiple stakeholders, including shipping companies, port authorities, and logistics providers. This interdependence heightens the risk of systemic failures, resulting in potentially severe consequences from cyber-attacks. Addressing these issues requires a comprehensive understanding of the specific risks and challenges faced by the MSCN, emphasizing the need for tailored strategies to enhance cybersecurity resilience.

The academic community has also made strides in identifying and classifying cybersecurity vulnerabilities in the maritime domain. For instance, ref. [14] explored cyber-attacks on the automatic identification system (AIS) of American vessels using the Parkerian hexad. While this framework provides a valuable lens for evaluating vulnerabilities in specific systems such as the AIS, it lacks a broader application to the entire supply chain and does not offer practical mitigation steps for MSCN agents. Similarly, ref. [7,15] developed classification schemes distinguishing between cyber-attacks on on-board systems and off-board systems, but they do not provide a holistic approach or practical guidance on managing these threats.

Other works, such as ref [16,17], have focused on risks associated with emphasizing the integration of advanced digital technologies such as the Internet of things (IoT), the cloud, blockchains, big data, and artificial intelligence (AI) into cybersecurity frameworks. These technologies are critical to monitoring, detecting, and mitigating cyber risks in increasingly digitized and interconnected maritime systems. While Industry 4.0 encompasses a wide range of innovations, we have focused on those technologies that are directly applicable to strengthening cyber defenses, in line with the core objectives of our study. While these frameworks offer insights into technical vulnerabilities, they often lack recommendations that address the operational complexities and geopolitical impacts unique to maritime operations.

To address these identified gaps and offer a comprehensive framework for the MSCN agents, this study presents a comprehensive approach to understanding and managing cyber-attacks in the maritime industry. Through a systematic literature review (SLR), this study aims to develop a classification model for cyber-attacks based on historical evidence, providing maritime supply chain managers with insights into pre-attack, during-attack, and post-attack measures.

To guide this study, we identified the subsequent research questions (RQs):

1. RQ1: What cyber-attacks in the MSCN have been reported in the academic literature?

This question is essential for understanding the types of threats faced by MSCN agents and how widespread they are across different systems and agents in the MSCN.

2. RQ2: What preventive and mitigating practices for cyber-attacks in the MSCN are reported in the literature?

By answering this question, we aim to identify best practices and proven methods for reducing the impact of cyber-attacks, ensuring that MSCN agents are better equipped to protect their systems and assets.

3. RQ3: What emerging technologies address cyber-attacks in the MSCN?

This question focuses on the future direction of maritime cybersecurity, examining how Industry 4.0 technologies can help prevent or mitigate these evolving threats.

The contributions of this study are multifaceted and address key research questions. First, we develop a comprehensive cyber-attack taxonomy that directly responds to RQ1. By reviewing the existing literature and analyzing incident reports from MSCN actors, we bridge the gap between practical experience and academic knowledge. This taxonomy is essential for understanding the factors associated with cyber-attacks affecting the MSCN. In addition, we present historical cybersecurity evidence that also supports RQ1. This analysis reveals patterns in the most common cyber-attacks in the maritime sector, highlighting the systems and actors that are frequently targeted. These findings inform both the taxonomy and practical recommendations. In furtherance, we compile practical recommendations aligned with RQ2, focusing on prevention and mitigation practices for MSCN cyber-attacks. This compilation provides MSCN stakeholders with actionable strategies based on best practices derived from the literature. Finally, we explore emerging cybersecurity technologies related to RQ3, examining how innovations, including key Industry 4.0 technologies, can effectively combat cyber threats in the MSCN. By equipping stakeholders with essential insights, this study provides robust strategies for preventing and mitigating cyber-attacks.

This paper is structured as follows. After this introduction, the following sections examine cybersecurity in maritime transport, describe the methodology of the SLR, show the results of the review, and explain these findings with regard to the research questions. The final sections provide suggestions for further research and conclude by discussing the wider implications of these findings for global supply chain networks.

PRISMA Statement

The SLR conducted in this study follows the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) framework, a widely accepted methodology for ensuring rigor and transparency in literature reviews. The process was carried out in three key stages: identification, screening, and inclusion. In the identification phase, a comprehensive search was performed using Elsevier's Scopus and Web of Science databases, with a defined set of keywords to capture both cybernetic and maritime components relevant to this study. No time constraints were imposed on the searches.

In the first phase, 1443 papers were identified, of which 116 were shortlisted for inclusion following an automatic filtering process and evaluation by the three authors. Each paper was evaluated under specific inclusion and exclusion criteria, focusing on factors such as the mention of cyber-attacks in the MSCN, historical evidence reports, and risk mitigation or contingency strategies potentially useful for MSCN stakeholders. After removing duplicates and applying quality checks, 110 papers were included in the final review.

This review assessed various risk factors related to MSCN cybersecurity. Through careful analysis and synthesis of the data, insights were generated to inform future research and guide stakeholders in implementing more robust cybersecurity practices. The PRISMA flow diagram (Figure 2) provides an overview of the systemic review process.

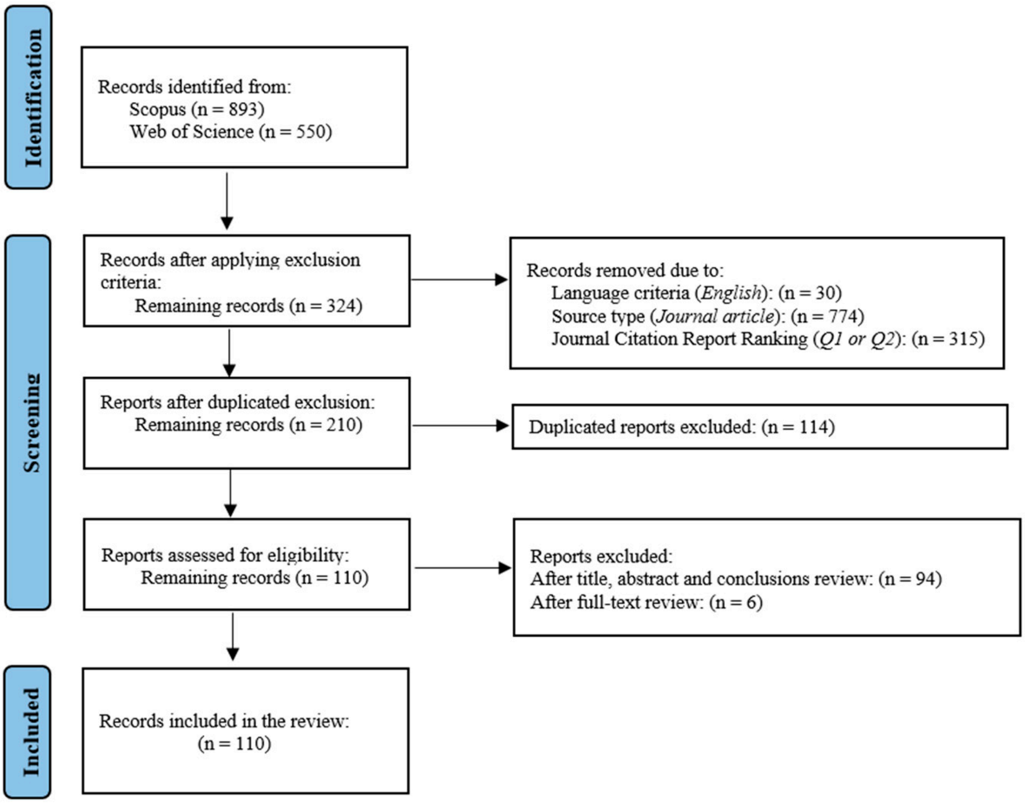
Identification
Screening
Included
Records identified from:
Scopus (n = 893)
Web of Science (n = 550)
Records after applying exclusion criteria:
Remaining records (n = 324)
Records removed due to:
Language criteria (*English*): (n = 30)
Source type (*Journal article*): (n = 774)
Journal Citation Report Ranking (*Q1 or Q2*): (n = 315)
Reports after duplicated exclusion:
Remaining records (n = 210)
Duplicated reports excluded: (n = 114)
Reports assessed for eligibility:
Remaining records (n = 110)
Reports excluded:
After title, abstract and conclusions review: (n = 94)
After full-text review: (n = 6)
Records included in the review:
(n = 110)

Figure 2. SLR Methodology.

2. Cybersecurity in the Maritime Sector

The maritime industry's evolving processes, characterized by their growing complexity, digitalization, and automation, necessitate a fresh and comprehensive approach to managing cybersecurity [18]. This section presents fundamental cybersecurity principles and outlines the crucial cyber risk management frameworks recommended by international maritime organizations.

2.1. Basic Concepts Related to Cyber Risk

The notion of risk may differ among various industries but typically involves evaluating the probability and consequences of potential incidents that could impact assets [19]. In the context of Industry 4.0, risk managers have placed significant emphasis on "cyber risk", which pertains to potential damage arising from vulnerabilities in technological assets. Cyber-attacks are intentional actions carried out by malicious individuals aiming to disrupt the confidentiality, availability, or integrity of information systems [16]. These attacks may target maritime operations such as unauthorized access or deliberate sabotage, resulting in navigational errors or service disruptions [19]. Additionally, managers face cyber-physical risks, which involve the control of physical processes through digital components [17]. These risks arise when malicious actors manipulate computer systems that control physical infrastructure, such as pipelines or valves, potentially causing harm to both property and human lives [20].

Assessing cyber risks entails comprehending the likelihood of incidents and their outcomes, including collisions, operational disruptions, and economic losses [21]. To conduct an effective risk analysis, it is necessary to evaluate both the likelihood and the potential impact of these events. The maritime industry faces unique challenges, in which cyber risks may have significant consequences. Failure can lead to higher expenses, delivery delays, and potential harm to both people and the environment, underscoring the importance of implementing a comprehensive cyber risk management strategy. For example, the 2017 NotPetya malware attack resulted in an estimated USD 300 million of direct economic damage and USD 8.4 billion in losses for stakeholders, demonstrating the serious operational and financial effects of cyber-attacks [22,23].

2.2. Cyber Risk Management Systems

In response to the pressing demand for cybersecurity strategies, maritime organizations have devised initiatives to guide stakeholders in creating efficient cybersecurity management plans. Table 1 summarizes the four key guidelines and relevant maritime studies.

Table 1. Summary of available cybersecurity guidelines.

Organization	Year	Title	Description	Related Studies
IMO	2017	Resolution MSC.428(98)—Maritime Cyber Risk Management in Safety Management Systems [24].	It exposes five functional elements that support effective cyber risk management: Identify—Protect—Detect—Respond—Recover.	Ref. [25] suggests incorporating a cyber risk management framework into maritime ship safety systems (SMS).
				Ref. [26] highlights the importance of adhering to IMO resolutions, focusing on usability, security, and functionality.
NIST	2018	Framework for Improving Critical Infrastructure Cybersecurity (NIST) [27].	The framework is a set of guidelines for mitigating organizational cybersecurity risks and organizes basic cybersecurity activities regarding the five elements proposed by IMO.	Ref. [18] merges the NIST framework with STWC standards to identify crew competencies needed for NIST's core functions.
				Ref. [28] blends IMO guidelines [24] with the NIST framework to differentiate cybersecurity needs between IT and OT systems in maritime assets.
DNV	2016	DNVGL-RP-0496 Cybersecurity resilience management for ships and mobile offshore units in operations [29].	It is composed of four essential steps for cyber risk management: Assessment—Improvement—Verification—Validation.	Ref. [30] reviews eight cybersecurity guidelines and notes the DNV's lack of operational best practices despite its detailed risk assessment guide.
				Ref. [31] emphasizes the DNV's comprehensive cybersecurity suggestions spanning people, processes, and technology.
ABS	2021	Guide for Cybersecurity Implementation for the Marine and Offshore Industries [32].	It contains 27 cybersecurity controls and the recommendations are based on three levels of cybersecurity urgency (Tier 1, Tier 2, and Tier 3).	Ref. [30] finds the ABS guidelines helpful for pinpointing operational best practices for maritime stakeholders.

In summary, various regulatory bodies and international organizations have created guidelines to enhance cyber risk management in the maritime industry. However, investigations into the tangible impacts of these guidelines are still in their early stages. Hence, it is imperative to conduct studies that collect pragmatic solutions and historical data on cyber-attacks to implement these recommendations successfully in practical situations. The subsequent section delineates the SLR methodology employed to evaluate these studies.

3. SLR Methodology

This study adopted the PRISMA framework introduced by ref. [33]. PRISMA is recognized for its structured and comprehensive approach to conducting systematic literature reviews, ensuring rigorous and reproducible research outcomes [34,35]. This methodology aligns with our research questions and provides a transparent process from study identification to data synthesis. Figure 2 illustrates the three stages of the PRISMA methodology applied in this study. The PRISMA flow diagram follows a structured three-step process. (1) Identification: researchers define the research question and systematically search for relevant studies, adhering to predefined inclusion and exclusion criteria. (2) Screening: identified studies are screened for relevance by reviewing titles and abstracts. Those that align with the research question undergo a full-text review. (3) Inclusion: eligible studies are included in the systematic review. Data from these studies are extracted and analyzed, and the findings are synthesized and reported.

3.1. Identification

The first step involved evaluating the existing cybersecurity conditions in the MSCN. This evaluation helped to identify gaps requiring the development of a new taxonomy for cyber-attacks. Subsequently, a research protocol was established, outlining the designated databases, search keywords, and inclusion and exclusion criteria to direct the systematic review. The authors collaboratively established the search equation and defined the specific time frame for the studies included in this review. Additionally, they selected the databases to be searched and outlined the inclusion and exclusion criteria. However, the initial assessment was conducted by one author.

Then, to discover pertinent papers, the authors used Elsevier's Scopus and Web of Science, widely recognized as the most comprehensive scientific databases in the field, to identify relevant papers [35–37]. The search strategy included two sets of keywords: one on cybernetic aspects and the other on maritime components. The Boolean operator 'AND' was used to link the two sets of keywords, while 'OR' was used within each set to extend the search range. Table 2 lists the keywords used in this search. The searches undertaken in June 2024 were not subject to time constraints.

Table 2. Keywords used in the search.

Group 1: Cybernetic Component	Group 2: Maritime Component
Cyber	Maritime
Cybersecurity	Shipping
Digital security	Sea transport
Malware analysis	Marine industry

During this phase, 1443 papers were identified (62% from Scopus and 38% from Web of Science).

3.2. Screening

To ensure the relevance and quality of studies included in the SLR, we established specific eligibility criteria. Since this study involved a review of the published literature, we did not require ethical approval. We divided the screening process into two stages: (1) filtering, which we conducted automatically through databases, and (2) evaluation of research questions, which three authors assessed. During the filtering stage, the author refined search results to ensure that the selected literature met standards for broad dissemination, scientific rigor, and academic excellence. This review assessed the risk of bias in the studies included by examining factors such as study design, sample size, and potential conflicts of interest. The authors paid special attention to methodologies reporting maritime cyber-attack incidents, as inconsistencies in reporting standards could affect findings. This review also considered the influence of funding sources on study outcomes. This process identified 116 studies that explicitly focused on cyber-attacks within the MSCN.

The requirement for English language was satisfied by 99.1% in Scopus and 99.2% in Web of Science. Only papers published in peer-reviewed journals were included to ensure a rigorous evaluation procedure [38]. To ensure the integrity of the research, gray literature, including blogs, government papers, and conference proceedings, was omitted.

Applying the filtering process, 81.3% of papers from Scopus and 71.4% from Web of Science were eliminated. In addition, 114 duplicates were eliminated. The authors assessed various outcomes using appropriate effect measures. In this review, the impact was evaluated by analyzing operational disruption frequencies and comparing the relative vulnerability of shipping companies based on their cybersecurity measures. Additionally, qualitative insights regarding financial implications were examined, focusing on reported losses and recovery times [39,40]. These metrics were selected based on their relevance to the RQs and data types, providing a comprehensive understanding of cyber threats' effects on maritime operations to inform industry stakeholders.

The remaining papers' titles, abstracts, and conclusions were examined to verify whether they aligned with this study's objectives. This process resulted in the identification of 116 studies that explicitly focused on cyber-attacks within the MSCN.

Finally, the authors carefully reviewed the complete texts of 116 papers that successfully passed the initial screening. To facilitate this assessment, Table 3 was used to systematically organize the information from these papers into two main categories: general information and information specifically relevant to addressing RQ1, RQ2, and RQ3, as previously detailed in Section 1.

Table 3. Inclusion and exclusion criteria.

Stage	Criteria	Description
1. Filtering process	Language Peer-reviewed Quality	English language Journals Q1 or Q2 by JCR 2023
2. Research Questions	Cyber-attack events	Does the paper mention cyber-attacks?
		Does the paper mention historical evidence of cyber-attacks?
	Risk analysis	Does the paper mention preventative solutions for cyber-attacks?
		Does the paper mention mitigation solutions for cyber-attacks?
	Industry 4.0	Does the paper apply any Industry 4.0-based technology?
		Does the paper recommend the use of any Industry 4.0 technologies?

3.3. Included

During the final stage of the review process, the information gathered during the eligibility step was analyzed through the qualitative synthesis of each document. The purpose of collecting general information was to identify the key characteristics of each study. After gathering this data, each record and report retrieved was independently screened by four reviewers. All reviewers worked independently during the screening process, ensuring thorough evaluation and minimizing potential bias. No automation tools were used at any stage of this process. Therefore, each document addressed one of the RQs. Studies considered by a reviewer to not adequately address at least one RQ were eliminated. In cases where multiple results were available for the same outcome, the primary outcome as defined by the study authors was prioritized. If studies presented multiple measures or time points for the same outcome, we applied two criteria, (1) the publication date and (2) a comparison of the results across different contexts to identify consistent patterns or discrepancies in the outcomes related to cyber-attacks, to determine which results to collect. This approach ensured consistency and relevance across all included studies. As a result of this procedure, six publications were excluded, leaving a total of 110 papers to form the basis for the analyses in this SLR. Throughout the process, general information is recorded regarding the year of publication, journal name, author's country, country to which the paper is applied, keywords, and MSCN actor.

Figure 3 illustrates a bibliometric summary that contextualizes the results of the search conducted. The visualization includes key data points, including the countries with the highest number of publications, the most recurring themes within those publications, and the years with the highest volume of papers. By highlighting the geographic distribution of scholarly output, this figure underscores the global reach and collaborative nature of research in the field. The data were processed in Bibliometrix R® (R version 4.2.3; Bibliometrix version 4.3.0). [41]

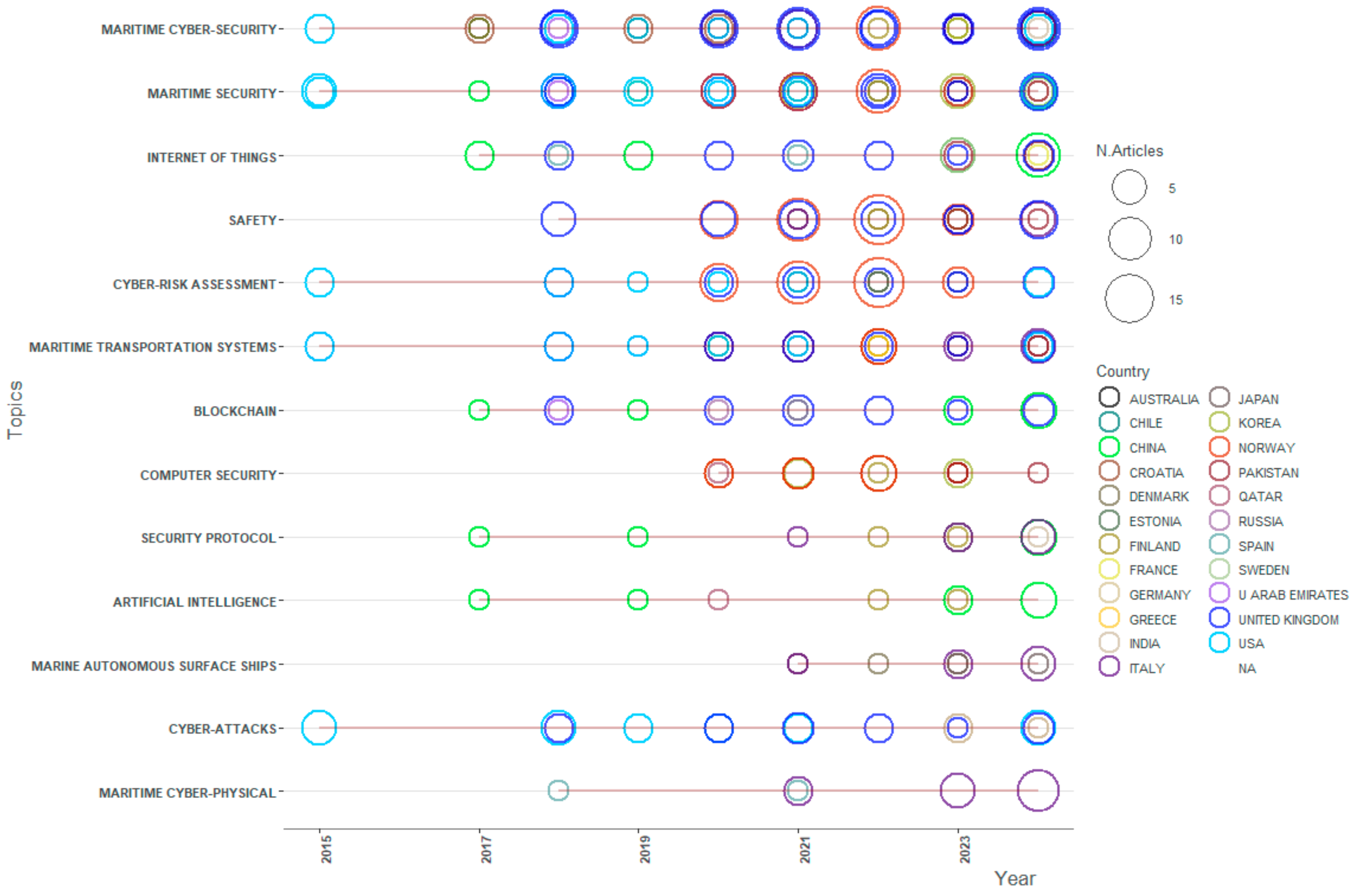

Figure 3. Bibliometric Overview: Geographical Distribution, Recurring Research Topics, and Publication Trends.

In addition, the representation of recurring topics provides insight into the prevailing areas of interest, thereby offering a focused perspective on the major research trends. The temporal distribution of publications, on the other hand, illustrates the dynamic evolution of scholarly attention and identifies specific periods of intensified research activity. Taken together, this bibliometric analysis serves as a foundational reference, enabling a deeper understanding of the subsequent sections and supporting a comprehensive interpretation of the research landscape. This contextual layer is critical for identifying the field's maturity and potential gaps or emerging areas that merit further exploration.

The following sections provide a comprehensive presentation of the outcomes of this step. The analysis was divided into two parts: descriptive statistics based on the general information gathered from the 110 selected papers, and an in-depth examination of each paper concerning the RQs.

4. Descriptive Statistics

This section reviews the general characteristics of the 110 selected papers and analyzes their distribution over time and across various research domains. The data were processed in Bibliometrix R®.

This review assessed the relevance of each paper to key stakeholders in the MSCN by evaluating the specificity and practical value of the information provided. Figure 4 highlights the focus of studies on specific stakeholders (60% on shipping lines, 24% on port operators, and 16% on freight forwarders), indicating that most research on cyber-attacks has focused on shipping lines. By identifying which stakeholders are most studied when it comes to cyber-attacks, Figure 4 provides insight into where incidents are most reported, which helps to address the first research question. Additionally, the cyber-attacks identified in the MSCN are primarily relevant to shipping lines, indicating that this segment faces the highest reported risk. Prevention and mitigation practices vary by stakeholder, with port operators receiving a significant amount of attention, highlighting the critical role of ports in cyber defense strategies. The focus on shipping lines and port operators suggests that emerging technologies to counter cyber-attacks are likely to be directed at securing these areas, reflecting the vulnerabilities highlighted in the literature.

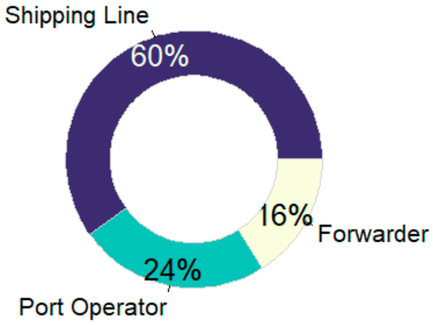

Figure 4. Proportion of papers according to the MSCN actor.

5. Results and Discussion

To deepen our understanding of cyber-attacks within the MSCN, we focus on addressing the three key RQs. This includes formulating a comprehensive taxonomy for cyber-attacks in the MSCN, identifying prevalent cyber-attacks through an exhaustive literature review, investigating Industry 4.0 technologies as potential safeguards against cyber threats, and delineating recommended actions for both pre- and post-cyber-attack scenarios. The results of these investigations are detailed below.

5.1. RQ1: What Cyber-Attacks in the MSCN Have Been Reported in the Academic Literature?

Our SLR identified eight primary categories of cyber-attacks that present substantial risks to the MSCN. These types of assaults include DDoS, malware/ransomware, identity fraud, navigation system attacks such as hijacking, spoofing, and jamming, phishing, spear phishing, social engineering, watering holes, and brute force attacks. The following analysis offers a comprehensive examination of each type of assault, their documented occurrences, and a recently established classification model that effectively addresses these risks.

5.1.1. Cyber-Attacks in the MSCN

DoS/DDoS: These attacks are predominant threats in the MSCN, where attackers overwhelm systems with excessive traffic, resulting in denial of access to online services [42–44]. The threats extend from underwater sensor networks, where bandwidth vulnerabilities are exploited [45,46] to IoT devices used across maritime operations [47,48]. DDoS attacks are particularly notable for their impact on port operations, revealing vulnerabilities in cyber risk assessments [49–51]. Additionally, DDoS threats affect maritime vessel networks, with critical implications for systems such as the AIS, in which approximately 89% of setups are susceptible at the protocol level [52–54]. These insights highlight the urgent need for robust cybersecurity defenses across maritime systems to mitigate the widespread risk of DoS/DDoS attacks.

Malware, ransomware, and Trojans: Research demonstrates that these cyber risks have a substantial influence on multiple aspects of maritime operations, including port infrastructures and onboard systems such as SCADA. Studies have highlighted vulnerabilities in programming logic controllers and the risks associated with insufficient antivirus protection, underscoring the importance of implementing strong cybersecurity measures [47,50,55,56]. Comprehensive strategies are essential, as evidenced by a risk assessment conducted in Turkey's Marmara Region container port, which showed medium vulnerability levels to malware attacks [49,56]. Experts argue in favor of implementing strict security measures and global standards to protect vessel management systems and counteract malware-induced disruptions [15,57,58]. This collective evidence underscores the complex challenge malware poses across the MSCN, necessitating enhanced defenses and standardized cybersecurity frameworks [42,59].

Social engineering, tampering, phishing, and spear phishing: Human vulnerabilities are of utmost importance in maritime cybersecurity because they are exploited through techniques such as phishing, spear phishing, and social engineering to compromise security systems. Cybercriminals frequently employ false emails to obtain sensitive information or lure employees into breaching security protocols through social media interactions [15,35,60]. In addition, manipulating system assets such as disks and networks has substantial dangers, especially for vital systems such as the AIS, which requires strict data security procedures [61]. Port operators and shipping lines are particularly vulnerable to these cyber-attacks, emphasizing the necessity for comprehensive cybersecurity policies that consider human aspects to safeguard all entities within the MSCN [50,62,63]. In this paper, social engineering, tampering, phishing, and spear phishing are grouped due to their common exploitation of human vulnerabilities. These methods manipulate individuals to circumvent security, often through deceptive communications or insider threats. The taxonomy underscores the importance of addressing human factors in cybersecurity, as these vectors exploit human error, not just technical flaws. As the industry digitizes, comprehensive defenses must include technical measures in addition to awareness and training to effectively mitigate these risks.

Brute force, identity fraud, watering hole, and port scanning: These less commonly acknowledged yet serious cyber dangers impact all MSCN agents. The grouping of brute force, identity fraud, watering hole, and port scanning is based on their common goal of exploiting system access points to gain unauthorized access or information within the MSCN. These methods target different aspects of network security but are unified by their focus on identifying and exploiting vulnerabilities. Brute force attacks systematically attempt different combinations of passwords, whereas identity fraud is the theft of identities for illicit purposes [64,65]. Watering hole lures people to access malicious websites [15], whereas port scanning detects vulnerable network endpoints [50]. It is advisable to adopt cyber hygiene practices and utilize TCP wrappers to enhance defenses against diverse attacks.

Hijacking, jamming, and spoofing: These critical cyber-attacks primarily affect shipping companies by compromising vessel navigation systems. These methods share a focus on compromising communication and navigation systems. The attacks disrupt or manipulate critical signals that vessels rely on for safe and efficient operations. The research outlines many strategies, such as radio frequency jamming and spoofing, that generate deceptive signals to covertly alter the GPS or AIS systems of vessels [52,57,66]. These approaches pose a danger to the reliability of navigation controls because spoofing techniques are becoming more advanced by synchronizing with satellite signals to increase the impact of attacks [43,50,67]. The marine industry acknowledges these as the main risks, specifically impacting integrated bridge system elements such as AIS and GNSS, which require a change in cybersecurity strategies [65,66,68,69]. According to risk evaluations, different systems have varied levels of threat, with AIS having moderate risks and the electronic chart display and information system (ECDIS) facing higher risks [61]. Efforts to reduce these dangers involve the creation of secure authentication frameworks, such as Auth-AIS, which utilizes cryptographic technologies to safeguard AIS broadcast messages against spoofing attacks [70]. Grouping them emphasizes their potential to disrupt maritime traffic, navigation, and communication, which can lead to significant operational and safety risks. This study highlights the continuous development of cyber risks and emphasizes the necessity for strong cybersecurity solutions specifically designed to protect maritime navigation systems.

Table 4 summarizes the previous descriptions and presents the sources that may be used to further investigate each cyber-attack.

Table 4. Summary of cyber-attacks identified in the literature review.

Cyber-Attack	Description	Example of Historical Evidence	Frequency	References
DoS /DDoS	DoS attacks overwhelm a target with excessive traffic, thereby impeding functionality. Its variant, DDoS, uses multiple devices to severely disrupt services.	In May 2020, amid Persian Gulf tensions, a DDoS attack reportedly orchestrated by Israel led to the prolonged closure of Iran's Shahid Raji Port.	24	[35,42–47,49–54,57,60,61,64,65,67,71–75].
Malware/Ransomware/Trojans	Malware harms or disables systems. Ransomware encrypts files, demanding a ransom, often via malicious downloads. Trojans, masquerading as legitimate software, steal data or cause damage.	In June 2017, the Petya attack targeted Maersk's servers in Europe and India, encrypting data and disrupting 17 terminals with losses exceeding USD 200 million.	28	[15,19,35,42,44,47,49,50,53,55–59,65,67,69,75–85].
Social engineering/Tampering/Phishing/Spear phishing	These methods manipulate individuals to compromise security. Social engineering and tampering involve the misuse of information. Phishing deceives users to disclose sensitive details through misleading emails, whereas spear phishing targets specific users with tailored messages to steal data.	From June 2011 to 2013, hackers used social engineering and spear phishing to seize control of networks at Belgium's Port of Antwerp, showcasing the sophistication of cyber threats.	10	[15,35,42,44,47,50,61–63,75].
Brute Force	This attack method involves testing all possible passwords or keys until the correct password is found and exploiting weak security to gain unauthorized access.	In October 2018, the Port of Vancouver was hit by a brute force attack, and the second such incident occurred within a few months, during which nearly 225,000 user accounts were probed.	3	[15,52,65].
Identity fraud	This involves illegally obtaining personal information to impersonate someone and conduct fraudulent activities, such as unauthorized transactions or misinformation.	In 2017, the vessel m/v Andrej Longov/Sea Breez 1/Ayda/STS-50 committed identity fraud in the Southern Ocean, falsifying its registry and generating fake signals to appear in nearly 100 different locations while conducting illegal fishing activities.	2	[15,64].
Watering hole	Targets specific groups by planting malware on legitimate websites visited by the group, making detection difficult because of the authenticity of the site.	Historical evidence was not presented in this reference.	2	[15,42].

Table 4. *Cont.*

Cyber-Attack	Description	Example of Historical Evidence	Frequency	References
Port scanning	Scans network ports to identify vulnerabilities and gather information by employing methods such as IP fragmentation to enhance stealth.	Historical evidence was not presented in this reference.	1	[50].
Hijacking/Jamming/Spoofing	Hijacking involves taking control of a ship's systems. Jamming disrupts communications by interfering with signals, while spoofing deceives systems with false data, compromising navigation and safety.	In August 2017, the U.S. Maritime Administration reported an attack in which the GPS of a ship in the Russian port of Novorossiysk indicated incorrect localization. This incident is believed to be a test of a new GPS spoofing system manipulating the ship's navigation signals.	26	[15,19,35,42–44,47,50,52,57,61–65,67–73,79,83–85].

5.1.2. Historical Evidence of Cyber-Attacks in the MSCN

To discern the recurrence of various cyber-attacks in real-world scenarios, the authors conducted a comprehensive literature review, assembling a historical record of reported cyber-related incidents. A total of 68 events were identified, and Figure 5 illustrates the frequency of these events over the last decade. Figure 5 illustrates the number of cyber-attacks in the MSCN over the years, categorized by type of attack. The categories include DoS and DDoS, malware, ransomware, Trojans, social engineering, tampering, phishing, spear phishing, brute force, identity fraud, watering hole, port scanning, hijacking, jamming, and spoofing. The trend shows that DoS attacks initially appeared sporadically in 2012, 2016, and 2020, with a low frequency. However, starting in 2023, there is a notable increase in DoS incidents, indicating a growing prevalence of this type of attack within the MSCN. This escalation suggests that while DoS was previously a less frequent threat, it has become a more significant issue in recent years. In addition, the graph shows that hijacking, jamming, and spoofing incidents have been significant in 12 of the 15 years analyzed, indicating a persistent threat in the MSCN. In addition, the increase in social engineering, tampering, phishing, and spear phishing attacks shows a growing trend over the period analyzed, suggesting an increasing use of human manipulation techniques in cyber-attacks.

On the other hand, brute force incidents have remained relatively stable, with no significant change in their percentage share from year to year. This suggests that while brute force attacks remain a constant threat, their prevalence has not significantly increased or decreased throughout the analysis.

The available historical cyber-attack events reveal that hijacking, jamming, and spoofing attacks are the most common, followed closely by malware and ransomware. Importantly, the data suggest an increase in cyber-attacks within the maritime industry over the last decade, despite limited records from 2021 to 2024 in the reviewed literature, as these attacks are generally reported years after their occurrence.

As part of this investigation, the authors also collected data regarding the countries where these cyber-attacks occurred. Figure 6 illustrates that the United States reported the highest number of cyber-attacks, with the United Kingdom and Iran following closely behind.

It is crucial to acknowledge that the true number of cyber-attacks in the maritime industry is probably greater than officially reported. This is because many incidents go unnoticed or unreported as businesses prioritize protecting their interests or preventing customer panic [9,86,87]. The scarcity of public resources dedicated to maritime cybersecurity has hindered advancements in this field [68]. Moreover, the sensitivity surrounding incidents, such as spear phishing attacks in ports, contributes to this underreporting, impacting confidentiality and international economic relations [50].

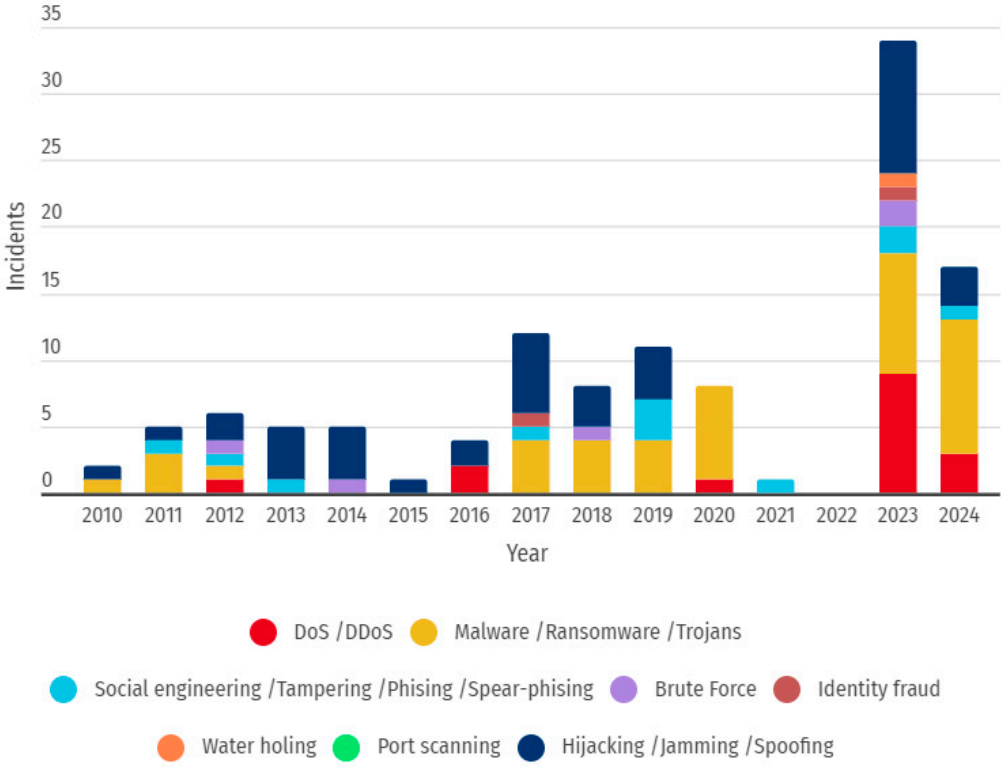

Figure 5. Historical evidence of cyber-attacks reported by year.

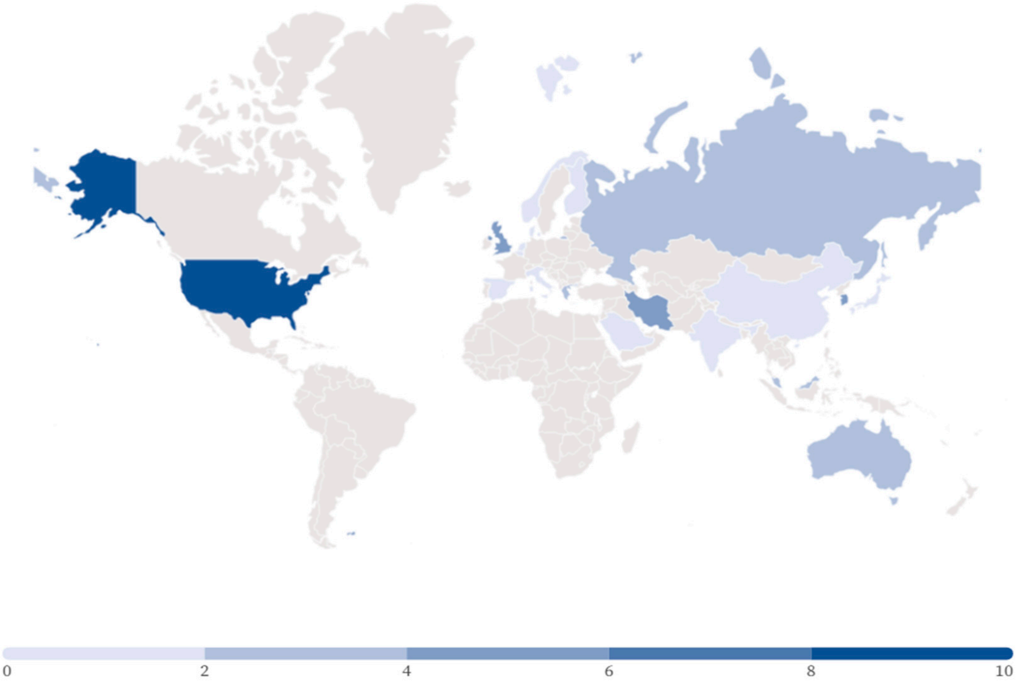

Figure 6. Countries where the reported cyber-attacks occurred.

5.1.3. Taxonomy

To improve the comprehension of cyber-attacks in the MSCN, we created a classification system using 110 research publications. This taxonomy specifically focuses on the distinct issues faced by the maritime sector in contrast to more general cyber threats. A taxonomy, as defined by ref. [88], systematically classifies concepts and, in this context, categorizes cyber-attacks according to various distinct factors (Figure 7).

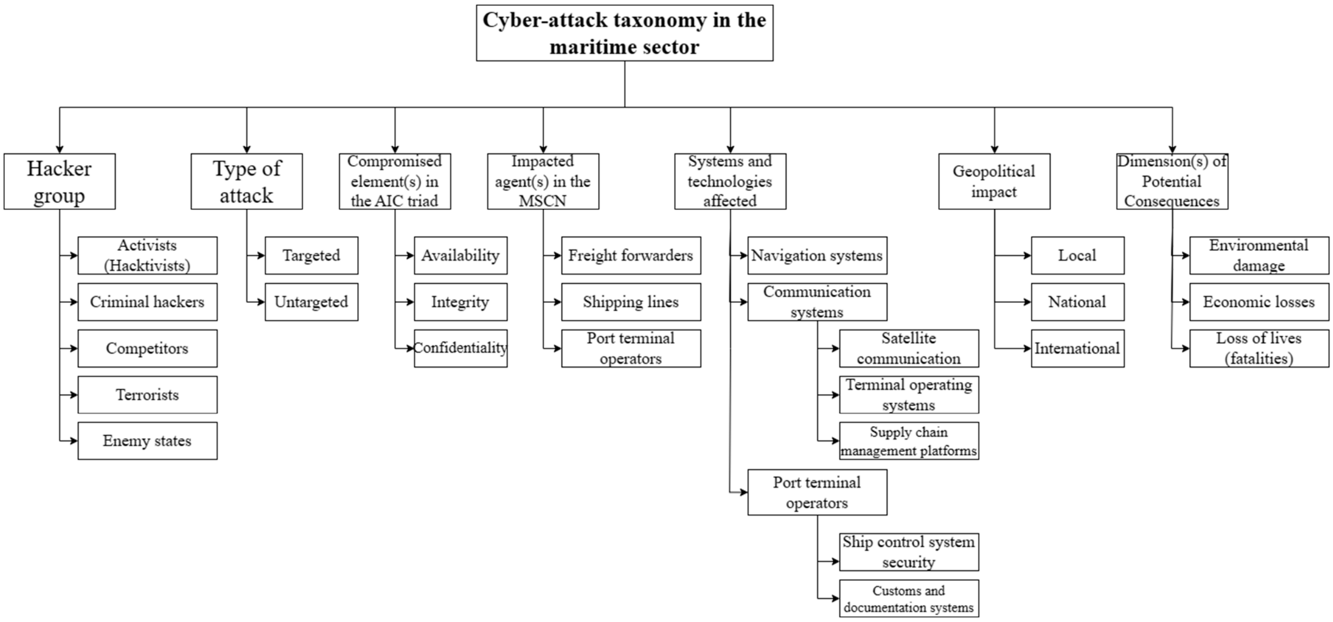

Figure 7. Cyber-attack Taxonomy for the MSCN.

Our taxonomy includes seven key factors: (1) the hacker group, (2) the type of attack, (3) compromised elements of the availability, integrity, and confidentiality (AIC) triad, (4) the affected MSCN agent, (5) systems and technologies affected, (6) geopolitical impact, and (7) potential consequences. Each factor aids in understanding the nuances of cyber-attacks specific to the maritime industry.

Hacker group: Research identifies a range of potential adversaries, including criminals, terrorists, hacktivists, competitors, and state actors, each with distinct motivations, ranging from financial gain to geopolitical influence [7,89].

Type of attack: Attacks vary from untargeted attacks exploiting common vulnerabilities to targeted, sophisticated attacks aimed at specific entities within the supply chain [90,91].

AIC triad compromise: This classification focuses on threats to data availability, integrity, and confidentiality, which are essential for maintaining operational trust and security across maritime systems [49,62].

Affected agents: This taxonomy identifies which MSCN agents are impacted, including freight forwarders, shipping lines, and port terminal operators, to tailor cybersecurity measures accordingly.

Systems and technologies affected: This study examined the impact on navigation, communication, and control systems within the MSCN. Special attention is given to systems such as satellite communications and terminal operating systems, which are integral to all maritime actors [69,92].

Geopolitical impact: Cyber-attacks are categorized by their scope (local, national, or international), highlighting the breadth of their impact and the scale of required response measures [16].

Potential consequences: The taxonomy explores the broad consequences of attacks, ranging from ecological harm to financial setbacks and loss of human life, emphasizing the urgent requirement for strong defenses [93].

While our proposed taxonomy is customized to address the specific challenges of the maritime sector, we acknowledge that it is not the only possible approach for categorizing cyber risks. Other frameworks, such as the MITRE ATT&CK framework, focus primarily on attack techniques and the specific tactics and procedures used by attackers. This framework provides a valuable and technical breakdown of the methods used in cyber-attacks, offering deep insights into specific tactics [94]. However, it does not fully address the multi-dimensional risks in the MSCN, such as geopolitical considerations and the operational impacts on maritime agents.

Incident-based taxonomies, such as the one presented in ref. [7], provide insights into real-world cyber-attacks affecting onboard systems, ports, and communication infrastructures, offering a historical perspective by categorizing incidents based on the system affected. Similarly, the work in ref. [50] focuses on technological vulnerabilities that are integrated into technologies in the maritime sector, highlighting technical risks. However, both approaches share common limitations: they fail to capture the broader geopolitical dimensions, hacker group motivations, and global consequences of cyber-risks—key elements necessary for understanding and mitigating the full scope of risks in the MSCN.

In addition to comparing our taxonomy with alternative classification systems, it is important to link it with established cybersecurity guidelines, such as those presented in Table 1. As detailed in Section 2.2, the NIST cybersecurity framework outlines five core functions (identify, protect, detect, respond, and recover), which serve as the foundation for mitigating cybersecurity risks. Our taxonomy directly supports these functions by offering a detailed method for identifying and classifying the specific risks associated with cyber-attacks in the maritime sector.

For example, the categorization of hacker groups and attack types in our taxonomy aligns with the identify function of NIST, helping stakeholders understand who might be targeting their systems and what methods they might use. Similarly, the focus on systems and technologies affected and the AIC triad helps maritime agents develop targeted protect and detect strategies. The inclusion of geopolitical impact and potential consequences provides insights into how maritime stakeholders should respond and recover from cyber-attacks, especially when dealing with nation-state actors or attacks that have broader geopolitical ramifications.

The IMO guidelines, particularly IMO Resolution MSC.428(98), also emphasize the importance of cyber risk management within the safety management systems of maritime organizations. The five functional elements of the IMO's cyber risk management strategy (identify, protect, detect, respond, and recover) are aligned with the NIST framework and further supported by our taxonomy, which breaks down the risk landscape into specific, actionable categories. By mapping cyber risks across factors such as compromised systems, maritime agents impacted, and global consequences, our taxonomy provides a detailed tool for applying the IMO's guidelines in real-world maritime cybersecurity scenarios.

5.2. RQ2: What Preventive and Mitigating Practices for Cyber-Attacks in the MSCN Are Reported in the Literature?

The impact of cyber-attacks on MSCN agents has led to several studies identifying effective prevention and mitigation practices. This literature review identifies 18 practices, which are classified into three sections according to the framework developed by ref. [95]: managing information security, informing security policy, and raising cybersecurity awareness and training. Mitigation practices aim to decrease the likelihood of cyber risks before incidents occur, whereas contingency practices focus on minimizing the repercussions after an event has taken place [96].

5.2.1. Practices to Manage Information Security

Nine significant practices were identified during the review of information security management practices in the MSCN. Table 5 presents a concise summary of these practices, and we provide further explanations for each below:

Risk Management Tools: Techniques such as those developed by ref. [97,98] use opacity and dual-layer mechanisms to protect ship information systems. The authors of ref. [99] introduced MITIGATE, a risk management methodology that facilitates collaboration between maritime industry actors and scientists in detecting potential attack paths under specific conditions. The authors of ref. [94] adapted the FMECA and the MITRE ATT&CK framework to assess risks in marine systems, particularly for an inertial navigation system (INS), identifying numerous risks associated with different components.

Programming digital tools to guarantee cybersecurity during the use of the IoT: In the programming field, academics have emphasized the need for creating specialized computational tools that can effectively integrate the IoT into the MSCN. For instance, ref. [100] proposed a physically unclonable function for mutual authentication between mobile users and IoT devices via a cloud gateway. The authors of ref. [47] developed a security-by-design algorithm for the IoT in port vehicle transport supply chains. Additionally, ref. [101] designed a network attack detection system to defend against DoS attacks, whereas ref. [63,102] advanced the cyber-ship-IoT framework, with a particular emphasis on automated cyber-attack mitigation and network-level defense for ship communication networks.

Detection-blocking techniques: The authors of ref. [53] developed an encryption algorithm for ship propulsion systems to ensure that access is limited to authorized systems. The authors of ref. [103] developed an algorithm for detecting anomalies in National Marine Electronics Association (NMEA) signals used in maritime communications. The authors of ref. [104] improved communication within vehicles by implementing cryptographic techniques, whereas ref. [70] presented Auth-AIS, a secure protocol for AIS communication. On the other hand, ref. [105] supported the adoption of blockchain technology in Latin American ports, suggesting the implementation of the CrowdBC framework to integrate cyber-technological, social, and cognitive components to enhance the efficiency of port operations.

Multi-factor authentication: To enhance email security in marine supply chains, it is crucial to implement strong passwords and multi-factor authentication [97], which are essential for preventing security breaches given the interrelated nature of enterprises [99]. Additionally, the importance of antivirus solutions in protecting maritime industry software has been highlighted [83,106]. The authors of ref. [107] developed a framework for conducting software security testing in naval combat systems, covering various system components to enhance cybersecurity measures for complex weapons systems.

Physical barriers, advanced antivirus solutions, and control access communication in port interfaces: Implementing physical barriers in control systems for ports and vessels is essential to enhance cybersecurity [35,57,61]. These measures effectively reduce cyber-physical attacks by utilizing intelligent sensors to regulate access to communication interfaces at the ports.

Radio frequency identification (RFID) technology management: Efficient management of RFID technologies is critical for protecting the personal information of watchkeeping officers and captains [92]. A detailed assessment of shipboard systems identifies potential vulnerabilities, improving security measures and reducing the risk of cyber-attacks on AIS systems [52].

Use of virtual private networks (VPNs): The use of VPNs, hard disk drive encryption, and intrusion detection systems are advocated to bolster maritime cybersecurity [108]. The authors of ref. [25] discussed the specific challenges and solutions for implementing these technologies in maritime environments, emphasizing the need for tailored solutions to overcome the limited bandwidth and intermittent connectivity.

Table 5. Practices for managing information security.

Best Practices	Mitigation	Contingency	MSCN Actor	Frequency	References
Develop computational tools for risk management	X	X	All actors	30	[11,13,15,43,51,56,57,61, 65,66,71,74,76,77,79,82, 85,92,96–99,109–116].
Program digital tools to ensure IoT cybersecurity	X	X	All actors	13	[43,46–48,52,54,63,99, 100,102,117–119].
Program digital tools to ensure IoT cybersecurity	X	X	All actors	13	[43,46–48,52,54,63,99, 100,102,116–118].
Implement detection–blocking techniques to restrict network access to authorized systems	X	X	Shipping line	13	[48,53,57,61,73,75,102, 107,108,120–123].
Secure email accounts with strong passwords and multi-factor authentication	X		All actors	4	[81,83,97,99].
Install physical barriers, surveillance cameras, and rapid-response alarms in control rooms	X		Shipping line, Port operators	6	[28,35,57,84,109,124].
Deploy advanced intrusion detection systems and antivirus software	X		All actors	6	[25,35,105,125–127].
Monitor, control, or block access to communication interface port(s)	X		Port operators	2	[57,104].
Manage RFID usage to protect the personal data of watchkeeping officers and captains	X		Shipping line	5	[59,70,72,92,128].
Use VPNs on remote working laptops	X		All actors	2	[25,107].

5.2.2. Practices Towards an Information Security Policy

The literature suggests various practices for an information security policy in the MSCN, as presented in Table 6.

Collaboration between agents in the MSCN: The literature underscores the importance of cooperation among MSCN stakeholders to improve cybersecurity capabilities. Effective collaboration involves the exchange of crucial information, including the documentation of cyber-attacks, strategies for mitigating them, and instruments for managing cyber risk. The studies conducted by [23,121] emphasized the effectiveness of collaborative workshops and shared platforms in enhancing collective cyber resilience in the maritime sector, particularly during periods of new regulatory changes and crises, such as COVID-19. On the other hand, de la Peña [15,129] highlights the crucial role of collaborative data-sharing platforms in effectively combating cyber-attacks within the MSCN.

Collaboration between international MSCN stakeholders: International partnerships are crucial, particularly among countries that share similar risk perceptions, to avoid the misallocation of resources and the amplification of incidents, as noted by [62,89]. Nevertheless, differences in risk profiles may limit the effectiveness of such alliances, underscoring the need for collaboration between countries that possess similar capabilities and perspectives on cybersecurity threats [57,128].

Integration of clear and acceptable cybersecurity practices: The standardization of cybersecurity practices within the MSCN is urgently required. Although frameworks such as ISO/EIC 27.001 and NIST recommendations already exist, there are still difficulties in obtaining complete standardization. Establishing partnerships between maritime and scientific communities is essential for advancing cybersecurity. These collaborations focus on training personnel, developing new techniques to mitigate risks, and creating tools to detect vulnerabilities [21,22,57,75].

Establishing a certification authority for maritime mobile service identity (MMSI) pseudonyms: To protect the identities of ships, there is a proposal to use pseudonyms for MMSI, overseen by a certification authority. This approach would enhance privacy and security by preventing unauthorized access to sensitive information about ship movements and cargo, which have been previously targeted by hackers. The certification authority is responsible for the distribution of public keys to guarantee secure communication and verify identities [52,130].

Table 6. Practices for an information security policy.

Best Practices	Mitigation	Contingency	MSCN Actor	Frequency references	
Collaborate among MSCN agents to share protocols and reduce cyber-attack impacts	X	X	All actors	6	[15,23,62,76,109,128].
Foster international collaboration among maritime stakeholders with aligned risk perceptions	X	X	All actors	9	[23,51,57,62,73,80,84,89,128].
Integrate standardized, clear cybersecurity practices	X		All actors	15	[22,28,44,49,61,66,73,75,77,83, 109,116,128,130,131]
Establish a certification authority to oversee the creation of pseudonyms for ship MMSI to protect identities	X		Shipping line	2	[52,129].

5.2.3. Practices to Raise Awareness and Training on Cybersecurity

The literature review revealed five crucial practices for cybersecurity awareness and training within the MSCN, as summarized in Table 7.

Table 7. Practices to raise awareness of cybersecurity.

Best Practices	Mitigation	Contingency	MSCN Actor	Frequency References	
Develop training courses and platforms to enhance operator knowledge in technology and attack prevention	X	X	All actors	18	[3,15,25,28,35,44,53, 60,69,93,99,110,121, 129,132–134].
Create a risk assessment library to share mitigating measures and risk experiences		X	All actors	2	[13,117].
Define a common glossary of cyber terms to ensure clarity and precision in communication	X		All actors	3	[10,69,121].
Introduce a 'port cyber resilience officer' role to enforce cybersecurity awareness in and around ports	X		Port operators	1	[129].
Regular apply cyber hygiene practices	X		Forwarder, Port operators	5	[25,69,76,129,135].

Development of training platforms: A common approach is to establish extensive training programs for MSCN workers. This involves developing specialized courses and training platforms to boost the technical knowledge of MSCN staff, addressing weaknesses in their ability to respond to cyber-attacks. Recent cyber incidents have highlighted the importance of structured security awareness training as they have exposed the shortcomings of many personnel in properly dealing with such threats [93,132].

Risk assessment library: Establishing a risk assessment library is essential for exchanging information about the identified risks and sharing strategies to mitigate them. The objective of this program is to reduce knowledge gaps, specifically among crew members aboard, by creating a centralized repository of clearly defined cyber-attack vectors and prevention strategies. This approach helps minimize unintentional vulnerabilities caused by inadequately informed staff [129].

Common glossary of cyber terms: The creation of a common glossary specifically designed for the maritime environment is essential for eliminating communication inaccuracies and ambiguities. Using a common set of terms improves comprehension among professionals with different backgrounds, promoting a unified approach to managing cybersecurity threats across the maritime industry [10,69].

Port cyber resilience officer: A proposal was made to enhance cybersecurity supervision in ports by introducing a dedicated 'port cyber resilience officer'. This position is dedicated to promoting and enforcing a thorough understanding of cybersecurity among all individuals associated with the port, acknowledging that the duty to maintain cybersecurity goes beyond that of any single individual [129].

Regular application of cyber hygiene: Encouraging consistent adherence to cyber hygiene standards is an essential approach to decreasing the occurrence of cyber-attacks. Cyber hygiene involves performing regular tasks, such as utilizing robust passwords, often updating operating systems, implementing multi-factor authentication, safeguarding satellite connections, and creating backups of data. These practices improve the general well-being of systems and strengthen online security throughout the organization [25,69,129].

5.3. RQ3: What Emerging Technologies Address Cyber-Attacks in the MSCN?

During the SLR, the authors identified various emerging technologies used by MSCN agents to mitigate or prevent cyber-attacks. This section is divided into two parts: the first covers Industry 4.0 technologies already in use within the MSCN, while the second part explores newer trends that show significant potential for future applications in the MSCN.

5.3.1. Industry 4.0 Technologies in Maritime Cybersecurity

The core principles of Industry 4.0—interconnectivity, automation, real-time data processing, and systems integration—fundamentally change how MSCN stakeholders address cybersecurity threats. These principles enable more adaptive, predictive, and responsive defenses, which are particularly valuable in the maritime sector. Given the complex and interconnected nature of maritime logistics, the ability to process vast amounts of data in real-time and integrate systems across diverse stakeholders is critical. This enables more effective identification and mitigation of cyber-attacks, ultimately improving the resilience of the entire supply chain (Figure 8).

Cloud computing, which is essential in modern e-navigation systems, faces challenges such as securing data transfers despite advancements such as Hamburg Port's implementation of cloud-based smart seaport logistics [136]. According to authors of ref. [134], the use of onboard cloud computing has the potential to offer numerous benefits, including improved data accessibility and improved ship navigation through the integration of mobile devices.

IoT technology, recognized for its ability to improve productivity in the maritime industry, also poses substantial cybersecurity threats. Programming protocols for secure data transmission and emphasizing interoperability are vital [100,134]. However, the high cost of IoT implementation and the escalating threat landscape highlight the need for robust cybersecurity measures [47,137].

Big Data is a pivotal Industry 4.0 technology in the maritime sector that facilitates comprehensive analyses for estimating accident risks, determining voyage durations, and reducing ship carbon emissions [137]. A notable application was demonstrated by ref. [103], who conducted an extensive analysis of navigational NMEA messages that were supported by all GPS manufacturers and carried data from various sensors. This analysis leveraged a large volume of maritime data for deep insights and enhanced the standardization and reliability of maritime communications. The authors of ref. [138] noted the evolution of NMEA standards, which regulate the structure and method of message exchange between devices, thus enhancing the data exchange framework in the maritime industry.

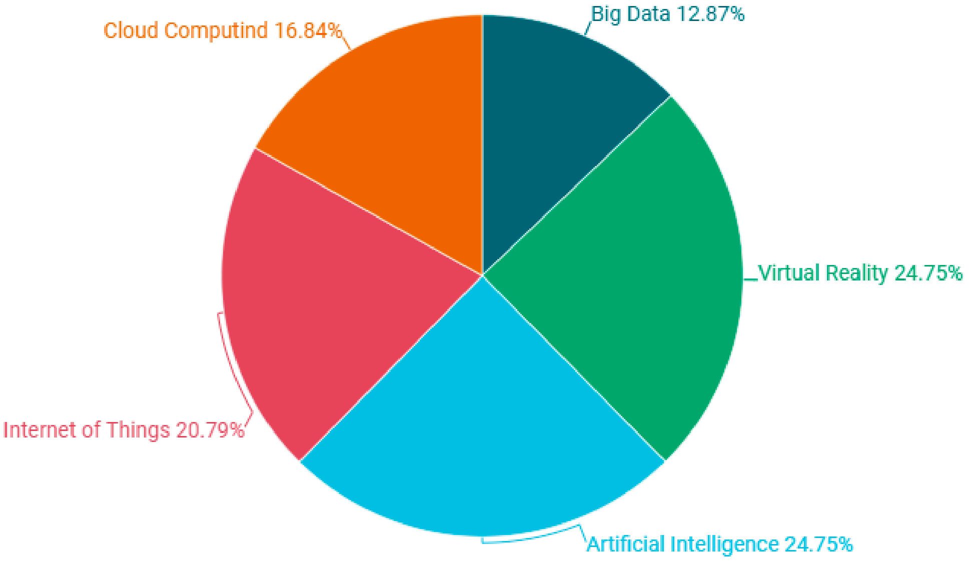

Figure 8. Industry 4.0 technologies identified in the literature review.

AI and VR are rapidly becoming revolutionary technologies in the maritime industry. AI applications play a vital role in detecting cyber vulnerabilities and improving security measures. Illustrative instances encompass AI algorithms designed to identify patterns of hacking and deep learning systems employed to forecast land transport behavior, showcasing AI's versatility in operational and security contexts [59,137]. Meanwhile, VR technology, used in training and simulation, offers substantial benefits in preparing maritime staff for emergency scenarios and in improving decision-making processes. An example of this can be seen in the simulation lab of the University of São Paulo, where maneuvers in restricted waters were analyzed [139].

Collectively, these Industry 4.0 technologies are instrumental in advancing cybersecurity measures within the MSCN, supporting a comprehensive strategy for cyber risk prevention and mitigation aligned with the goals of Industry 4.0 integration in the maritime domain [140,141].

5.3.2. Future Trends in Maritime Cybersecurity

As maritime cybersecurity evolves, generative AI and large language models (LLMs) are emerging as transformative technologies capable of addressing various cyber-attacks, from social engineering to data integrity threats. Unlike traditional Industry 4.0 technologies, which focus on improving operational efficiency, generative AI and LLMs offer new capabilities for automating attack detection, generating adaptive defenses, and responding to increasingly sophisticated threats.

For example, authors of ref. [142] discusses the role of LLMs in creating adaptive cybersecurity systems that can detect anomalous traffic patterns and mitigate DoS/DDoS attacks in real-time. By leveraging the pattern recognition and reasoning capabilities of LLMs, these systems can identify subtle variations in network activity, enabling them to prevent service disruptions more effectively than traditional methods. Additionally, in ref. [143], the authors demonstrate how model-based attack detection and mitigation techniques can be applied to protect against data integrity attacks such as malware and ransomware. These AI-driven models allow for early detection and intervention, and when integrated into vessel and port operations, they offer the potential for real-time threat detection, significantly improving the speed and accuracy of defensive measures.

In the context of autonomous vessels and unmanned surface vehicles (USVs), generative AI is opening new possibilities for secure navigation and monitoring. The authors of ref. [144] highlight how machine learning methods, specifically generative adversarial imitation learning (GAIL), can be applied to prevent spoofing, jamming, and hijacking attacks. By learning from expert navigation patterns, these AI-driven systems can adapt to changing environments and detect unusual behavior in real-time, enhancing the security of autonomous maritime operations. Furthermore, authors of ref. [145] explores the application of generative AI and ship design, showing how early integration of risk assessments and security features during the design phase can reduce vulnerabilities. This approach improves the overall resilience of vessels by embedding cybersecurity measures directly into the design process, offering long-term protection against potential threats.

Finally, generative AI also plays a pivotal role in defending against social engineering attacks, such as phishing and spear phishing. The authors of ref. [146] examine how AI-generated content can be exploited to create highly convincing phishing campaigns, increasing the likelihood of maritime personnel being deceived. However, these same technologies can also be used defensively. By analyzing communication patterns and identifying deceptive content in real-time, natural language processing (NLP) models can detect phishing attempts and prevent identity fraud. The authors of ref. [147] further support this by demonstrating how generative AI can mimic human communication styles, making phishing attacks more difficult to detect. In response, NLP models trained in malicious communication patterns can serve as critical tools for protecting the MSCN from increasingly sophisticated social engineering attacks.

6. Conclusions

Analyzing cyber-attacks within the MSCN is critical due to the sector's unique operational dynamics and reliance on interconnected logistics. Unlike other industries, the MSCN operates in an environment where vulnerabilities can propagate rapidly among stakeholders such as shipping companies, port authorities, and logistics providers. This interdependence increases the risk of systemic failures, making the consequences of cyber-attacks particularly severe. The MSCN also faces unique challenges, including outdated legacy systems, varying levels of cybersecurity maturity among stakeholders, and complex regulatory frameworks. Understanding these factors is essential to developing tailored cybersecurity strategies that address specific maritime risks. By focusing on cyber threats within the MSCN, we can gain valuable insights into critical assets and unique threat vectors. This specialized analysis allows us to establish best practices that consider the sector's regulatory environment, enabling stakeholders to implement targeted defenses and response protocols.

While our taxonomy provides a comprehensive framework for classifying cyber risks in the MSCN, we recognize that it is not the only available option. Other frameworks, such as MITRE ATT&CK and incident-based taxonomies, focus on attack techniques or historical data but do not fully capture the multi-dimensional risks specific to the maritime context. Moreover, existing cybersecurity standards, such as the NIST cybersecurity framework or IMO guidelines, provide valuable guidelines for cyber risk management, but our taxonomy adds further granularity by incorporating factors such as geopolitical impact and the motivations of hacker groups, which are critical for assessing cyber risks in a globalized maritime industry.

The findings underscore the critical need for heightened cybersecurity awareness and collaborative efforts among MSCN stakeholders and the scientific community. Shared knowledge, innovative protocols, and novel solutions are pivotal strategies for reducing the frequency and impact of cyber-attacks. Notably, this study emphasizes the often-overlooked human factor in MSCN cybersecurity, elevating training programs for personnel to the forefront of the recommended practices.

In general terms, MSCN agents should prioritize countering distributed denial of service (DoS/DDoS) and malware, supported by evidence from this literature review. Shipping lines are advised to focus on safeguarding themselves against hijacking, spoofing, and jamming.

To support cyber risk identification, the proposed taxonomy categorizes each cyber-attack under seven characteristics: hacker group, type of attack, compromised element of the AIC triad, affected MSCN agent, systems and technologies affected, geopolitical impact, and potential consequences. This multi-dimensional approach provides a structured means for understanding the complex risks faced by the maritime sector.

The authors acknowledge the limitation of relying solely on journal-reported cyber-attacks, recognizing the existence of unregistered events. Future research could benefit from inclusive surveys that capture the cyber risk perceptions of major industry players, offering a broader perspective.

Finally, it is imperative to note that our methodology, reliant on past publications, introduces an inherent time lag due to the publication process. As the cybersecurity landscape evolves rapidly, readers are urged to consider this temporal aspect. To supplement insights from historical publications, we encourage future researchers to explore real-time data and industry reports and engage directly with stakeholders. This dynamic approach ensures up-to-date comprehension of the ever-evolving cyber-attack panorama within the MSCN, especially as generative AI and LLMs continue to reshape the threat landscape.

Author Contributions: Conceptualization, M.V.C.M.; methodology, M.V.C.M., C.E.P.-R. and F.J.G.C.; validation: M.V.C.M., C.E.P.-R. and F.J.G.C.; writing-original draft preparation, M.V.C.M.; writing-review and editing, C.E.P.-R. and F.J.G.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare that they have no known competing financial interests or personal relationships that could have influenced the work reported in this study.

References

1. Canepa, M.; Ballini, F.; Dalaklis, D.; Vakili, S.; Colmenares Hernandez, L.M. CR CyberMar as a solution path towards Cybersecurity soundness in maritime logistics domain. *Trans. Marit. Sci.* **2021**, *10*, 147–153. [CrossRef]
2. Valentin, L. *What Is the Maritime Supply Chain?* SINAY Maritime Data Solution: Caen, France, 2022.
3. Senarak, C. Cybersecurity knowledge and skills for port facility security officers of international seaports: Perspectives of IT and security personnel. *Asian J. Shipp. Logist.* **2021**, *37*, 345–360. [CrossRef]
4. Kanwal, K.; Shi, W.; Kontovas, C.; Yang, Z.; Chang, C.H. Maritime cybersecurity: Are onboard systems ready? *Marit. Policy Manag.* **2024**, *51*, 484–502. [CrossRef] [PubMed]
5. Alop, A. The main challenges and barriers to the successful "smart shipping". *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2019**, *13*, 521–528. [CrossRef]
6. Hemminghaus, C.; Bauer, J.; Padilla, E. BRAT: A BRidge attack tool for cyber security assessments of maritime systems. *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2021**, *15*, 35–44. [CrossRef]
7. Meland, P.H.; Bernsmed, K.; Wille, E.; Rødseth, Ø.J.; Nesheim, D.A. A retrospective analysis of maritime cyber security incidents. *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2021**, *15*, 519–530. [CrossRef]
8. Lloyd's Register. *Building Resilience Against New Risks—Cyber Security for an Era of Innovation*; Lloyd's Register: London, UK, 2018.
9. Mraković, I.; Vojinović, R. Maritime cyber security analysis—how to reduce threats? *Trans. Marit. Sci.* **2019**, *8*, 132–139. [CrossRef]
10. Bocayuva, M. Cybersecurity in the European Union port sector in light of the digital transformation and the COVID-19 pandemic. *WMU J. Marit. Aff.* **2021**, *20*, 173–192. [CrossRef]
11. British Ports Association. *Managing Ports' Cyber Risks—White Paper*; British Ports Association: London, UK, 2020.
12. INMARSAT. *Cyber Security Requirements for IMO 2021—White Paper*; INMARSAT: London, UK, 2020.
13. Xing, B.; Jiang, Y.; Liu, Y.; Cao, S. Risk data analysis based anomaly detection of Ship Information System. *Energies* **2018**, *11*, 3403. [CrossRef]
14. Kessler, G.C.; Craiger, P.; Haass, J.C. A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system. *TransNav Int. J. Mar. Navig. Saf. Sea. Transp.* **2018**, *12*, 429–437. [CrossRef]

15. Ashraf, I.; Park, Y.; Hur, S.; Kim, S.W.; Alroobaea, R.; Zikria, Y.B.; Nosheen, S. A survey on cyber security threats in IoT-enabled maritime industry. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 2677–2690. [CrossRef]
16. Li, Y.; Liu, Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Rep.* **2021**, *7*, 8176–8186. [CrossRef]
17. Tyagi, A.K.; Sreenath, N. Cyber Physical Systems: Analyses, challenges and possible solutions. *Internet Things Cyber-Phys. Syst.* **2021**, *1*, 22–33. [CrossRef]
18. Hopcraft, R. Developing Maritime Digital Competencies. *IEEE Commun. Stand. Mag.* **2021**, *5*, 12–18. [CrossRef]
19. Sardi, A.; Rizzi, A.; Sorano, E.; Guerrieri, A. Cyber risk in health facilities: A systematic literature review. *Sustainability* **2020**, *12*, 7002. [CrossRef]
20. Arghandeh, R.; von Meier, A.; Mehrmanesh, L.; Mili, L. On the definition of cyber-physical resilience in power systems. *Renew. Sustain. Energy Rev.* **2016**, *58*, 1060–1069. [CrossRef]
21. Pallis, P.L. Port risk management in container terminals. *Transp. Res. Procedia.* **2017**, *25*, 4411–4421. [CrossRef]
22. Eichenhofer, J.O.; Heymann, E.; Miller, B.P.; Kang, A. An in-depth security assessment of maritime container terminal software systems. *IEEE Access* **2020**, *8*, 128050–128067. [CrossRef]
23. Karamperidis, S.; Kapalidis, C.; Watson, T. Maritime cyber security: A global challenge tackled through distinct regional approaches. *J. Mar. Sci. Eng.* **2021**, *9*, 1323. [CrossRef]
24. IMO. *Maritime Cyber Risk Management in Safety Management Systems. Resolution MSC.428(98)*; IMO: London, UK, 2017.
25. Yoo, Y.; Park, H.-S. Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship. *J. Mar. Sci. Eng.* **2021**, *9*, 565. [CrossRef]
26. Hopcraft, R.; Tam, K.; Dorje Palbar Misas, J.; Moara-Nkwe, K.; Jones, K. Developing a maritime cyber safety culture: Improving safety of operations. *Marit. Technol. Res.* **2022**, *5*, 258750. [CrossRef]
27. National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018.
28. Progoulakis, I.; Rohmeyer, P.; Nikitakos, N. Cyber physical systems security for maritime assets. *J. Mar. Sci. Eng.* **2021**, *9*, 1384. [CrossRef]
29. Veritas, D.N.; Lloyd, G. *Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation*; DNVGL-RP-0496; DNV-GL: Bærum, Norway, 2016.
30. Drazovich, L.; Brew, L.; Wetzel, S. Advancing the state of maritime cybersecurity guidelines to improve the resilience of the maritime transportation system. In Proceedings of the IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 26–28 July 2021.
31. Tuomala, V. *Maritime Cybersecurity. Before the Risks Turn into Attacks*; South-Eastern Finland University of Applied Sciences: Kouvola, Finland, 2021.
32. ABS. *Guide for Cybersecurity Implementation for the Marine and Offshore Industries*; ABS CyberSafety: Spring, TX, USA, 2021; Volume 2.
33. Liberati, A.; Altman, D.G.; Tetzlaff, J.; Mulrow, C.; Gøtzsche, P.C.; Ioannidis, J.P.A.; Clarke, M.; Devereaux, P.J.; Kleijnen, J.; Moher, D. The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration. *Ann. Intern. Med.* **2009**, *151*, W65–W94. [CrossRef] [PubMed]
34. Booth, A.; Sutton, A.; Papaioannou, D. *Systematic Approaches to a Successful Literature Review*; Sage Publications: Oaks, CA, USA, 2016.
35. Bolbot, V.; Theotokatos, G.; Boulougouris, E.; Vassalos, D. A novel cyber-risk assessment method for ship systems. *Saf. Sci.* **2020**, *131*, 104908. [CrossRef]
36. Alshehri, J.; Alhamed, A.; Hafizur Rahman, M.M. A systematic literature review on cybersecurity risk management in smart cities. In Proceedings of the Internationl Conference on Artificial Intelligence in Information and Communication (ICAIC), Osaka, Japan, 19–22 February 2024. [CrossRef]
37. Sardi, A.; Sorano, E.; Cantino, V.; Garengo, P. Big data and performance measurement research: Trends, evolution and future opportunities. *Meas. Bus. Excell.* **2023**, *27*, 531–548. [CrossRef]
38. Clarivate Analytics. *Journal Citation Reports*; Clarivate: Philadelphia, PA, USA, 2024.
39. Yuan, Z.; Yu, X.; Jiang, Y.; Sun, J.; Liu, Z.; Li, B. Current status and governance of data assets monetization in the global maritime industry: A comparative study of the United States, Europe, and China. *Ocean Coast Manag.* **2024**, *251*, 107078. [CrossRef]
40. Wang, Q.; Zhang, H.; Hu, C. China's competition regulation in the maritime industry: Regulatory concerns, problems and potential implications. *Ocean Coast Manag.* **2024**, *251*, 107082. [CrossRef]
41. Aria, M.; Cuccurullo, C. bibliometrix: An R-tool for comprehensive science mapping analysis. *J. Informetr.* **2017**, *11*, 959–975. [CrossRef]
42. Hossain, N.U.I.; Nur, F.; Hosseini, S.; Jaradat, R.; Marufuzzaman, M.; Puryear, S.M. A Bayesian network based approach for modeling and assessing resilience: A case study of a full service deep water port. *Reliab. Eng. Syst. Saf.* **2019**, *189*, 378–396. [CrossRef]
43. Juvonen, A.; Costin, A.; Turtiainen, H.; Hamalainen, T. On Apache Log4j2 Exploitation in Aeronautical, Maritime, and Aerospace Communication. *IEEE Access* **2022**, *10*, 86542–86557. [CrossRef]
44. Park, C.; Kontovas, C.; Yang, Z.; Chang, C.-H. A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean. Coast. Manag.* **2023**, *235*, 106480. [CrossRef]

45. Hu, C.; Pu, Y.; Yang, F.; Zhao, R.; Alrawais, A.; Xiang, T. Secure and efficient data collection and storage of IoT in smart ocean. *IEEE Internet Things J.* **2020**, *7*, 9980–9994. [CrossRef]
46. Kumar, P.; Gupta, G.P.; Tripathi, R.; Garg, S.; Hassan, M.M. DLTIF: Deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2021**, *24*, 2472–2481. [CrossRef]
47. Mouratidis, H.; Diamantopoulou, V. A security analysis method for industrial internet of things. *IEEE Trans. Ind. Inform.* **2018**, *14*, 4093–4100. [CrossRef]
48. Liu, W.; Xu, X.; Wu, L.; Qi, L.; Jolfaei, A.; Ding, W.; Khosravi, M.R. Intrusion detection for maritime transportation systems with batch federated aggregation. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 2503–2514. [CrossRef]
49. Gunes, B.; Kayisoglu, G.; Bolat, P. Cyber security risk assessment for seaports: A case study of a container port. *Comput. Secur.* **2021**, *103*, 102196. [CrossRef]
50. Ben Farah, M.A.; Ukwandu, E.; Hindy, H.; Brosset, D.; Bures, M.; Andonovic, I.; Bellekens, X. Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information* **2022**, *13*, 22. [CrossRef]
51. Potamos, G.; Stavrou, E.; Stavrou, S. Enhancing maritime cybersecurity through operational technology sensor data fusion: A comprehensive survey and analysis. *Sensors* **2024**, *24*, 3458. [CrossRef]
52. Khandker, S.; Turtiainen, H.; Costin, A.; Hamalainen, T. Cybersecurity attacks on software logic and error handling within AIS implementations: A systematic testing of resilience. *IEEE Access* **2022**, *10*, 29493–29505. [CrossRef]
53. Song, Z.; Skuric, A.; Ji, K. A recursive watermark method for hard real-time industrial control system cyber-resilience enhancement. *IEEE Trans. Autom. Sci. Eng.* **2020**, *17*, 1030–1043. [CrossRef]
54. Liu, P.M.; Guo, X.G.; Wang, J.L.; Xie, X.P.; Yang, F.W. Fully distributed hierarchical ET intrusion-and fault-tolerant group control for MASs with application to robotic manipulators. *IEEE Trans. Autom. Sci. Eng.* **2024**, *21*, 2868–2881. [CrossRef]
55. Sahay, R.; Estay, D.A.S.; Meng, W.; Jensen, C.D.; Barfod, M.B. A comparative risk analysis on CyberShip system with STPA-Sec, STRIDE and CORAS. *Comput. Secur.* **2023**, *128*, 103179. [CrossRef]
56. Aerts, G.; Mathys, G. Discovering trends in the digitalization of shipping: An exploratory study into trends using natural language processing. *J. Mar. Sci. Eng.* **2024**, *12*, 618. [CrossRef]
57. Caprolu, M.; Pietro, R.D.; Raponi, S.; Sciancalepore, S.; Tedeschi, P. Vessels cybersecurity: Issues, challenges, and the road ahead. *IEEE Commun. Mag.* **2020**, *58*, 90–96. [CrossRef]
58. Sharma, L. Maritime cybersecurity in the Indo-Pacific: Envisioning a role for the Quad. *J. Indian Ocean. Reg.* **2024**, 1–23. [CrossRef]
59. Leite Junior, W.C.; de Moraes, C.C.; de Albuquerque, C.E.P.; Machado, R.C.S.; de Sá, A.O. A triggering mechanism for cyber-attacks in naval sensors and systems. *Sensors* **2021**, *21*, 3195. [CrossRef] [PubMed]
60. Kampourakis, V.; Gkioulos, V.; Katsikas, S. A systematic literature review on wireless security testbeds in the cyber-physical realm. *Comput. Secur.* **2023**, *133*, 103383. [CrossRef]
61. Kavallieratos, G.; Diamantopoulou, V.; Katsikas, S.K. Shipping 4.0: Security requirements for the cyber-enabled ship. *IEEE Trans. Industr. Inform.* **2020**, *16*, 6617–6625. [CrossRef]
62. Tusher, H.M.; Munim, Z.H.; Notteboom, T.E.; Kim, T.E.; Nazir, S. Cyber security risk assessment in autonomous shipping. *Marit. Econ. Logist.* **2022**, *24*, 208–227. [CrossRef]
63. Tabish, N.; Chaur-Luh, T. Maritime autonomous surface ships: A review of cybersecurity challenges, countermeasures, and future perspectives. *IEEE Access* **2024**, *12*, 17114–17136. [CrossRef]
64. Wang, Y.; Chen, P.; Wu, B.; Wan, C.; Yang, Z. A trustable architecture over blockchain to facilitate maritime administration for MASS systems. *Reliab. Eng. Syst. Saf.* **2022**, *219*, 108246. [CrossRef]
65. Yoo, J.; Jo, Y. Formulating cybersecurity requirements for autonomous ships using the SQUARE methodology. *Sensors* **2023**, *23*, 5033. [CrossRef] [PubMed]
66. Longo, G.; Martelli, M.; Russo, E.; Merlo, A.; Zaccone, R. Adversarial waypoint injection attacks on Maritime Autonomous Surface Ships (MASS) collision avoidance systems. *J. Mar. Eng. Technol.* **2024**, *23*, 184–195. [CrossRef]
67. Longo, G.; Russo, E.; Armando, A.; Merlo, A. Attacking (and defending) the maritime radar system. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 3575–3589. [CrossRef]
68. Awan, M.S.K.; Al Ghamdi, M.A. Understanding the vulnerabilities in digital components of an integrated bridge system (IBS). *J. Mar. Sci. Eng.* **2019**, *7*, 350. [CrossRef]
69. Androjna, A.; Brcko, T.; Pavic, I.; Greidanus, H. Assessing cyber challenges of maritime navigation. *J. Mar. Sci. Eng.* **2020**, *8*, 776. [CrossRef]
70. Sciancalepore, S.; Tedeschi, P.; Aziz, A.; Di Pietro, R. Auth-AIS: Secure, flexible, and backward-compatible authentication of vessels AIS broadcasts. *IEEE Trans. Dependable Secure Comput.* **2022**, *19*, 2709–2726. [CrossRef]
71. Enoch, S.Y.; Lee, J.S.; Kim, D.S. Novel security models, metrics and security assessment for maritime vessel networks. *Comput. Netw.* **2021**, *189*, 107934. [CrossRef]
72. Wimpenny, G.; Šafář, J.; Grant, A.; Bransby, M. Securing the Automatic Identification System (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility. *J. Navig.* **2022**, *75*, 333–345. [CrossRef]
73. Longo, G.; Orlich, A.; Musante, S.; Merlo, A.; Russo, E. MaCySTe: A virtual testbed for maritime cybersecurity. *SoftwareX* **2023**, *23*, 101426. [CrossRef]

74. Lee, C.; Lee, S. Overcoming the DDoS attack vulnerability of an ISO 19847 shipboard data server. *J. Mar. Sci. Eng.* **2023**, *11*, 1000. [CrossRef]
75. Erbas, M.; Khalil, S.M.; Tsiopoulos, L. Systematic literature review of threat modeling and risk assessment in ship cybersecurity. *Ocean Eng.* **2024**, *306*, 118059. [CrossRef]
76. Kayisoglu, G.; Bolat, P.; Tam, K. A novel application of the CORAS framework for ensuring cyber hygiene on shipboard RADAR. *J. Mar. Eng. Technol.* **2024**, *23*, 67–81. [CrossRef]
77. Afenyo, M.; Caesar, L.D. Maritime cybersecurity threats: Gaps and directions for future research. *Ocean. Coast. Manag.* **2023**, *236*, 106493. [CrossRef]
78. Longo, G.; Lupia, F.; Pugliese, A.; Russo, E. Physics-aware targeted attacks against maritime industrial control systems. *J. Inf. Secur. Appl.* **2024**, *82*, 103724. [CrossRef]
79. Fenton, A.J. Preventing catastrophic cyber–physical attacks on the global maritime transportation system: A case study of hybrid maritime security in the Straits of Malacca and Singapore. *J. Mar. Sci. Eng.* **2024**, *12*, 510. [CrossRef]
80. Uflaz, E.; Sezer, S.I.; Tunçel, A.L.; Aydin, M.; Akyuz, E.; Arslan, O. Quantifying potential cyber-attack risks in maritime transportation under Dempster–Shafer theory FMECA and rule-based Bayesian network modelling. *Reliab. Eng. Syst. Saf.* **2024**, *24*. [CrossRef]
81. Hopcraft, R.; Harish, A.V.; Tam, K.; Jones, K. Raising the standard of maritime voyage data recorder security. *J. Mar. Sci. Eng.* **2023**, *11*, 267. [CrossRef]
82. Guo, J.; Guo, H. Real-time risk detection method and protection strategy for intelligent ship network security based on cloud computing. *Symmetry* **2023**, *15*, 988. [CrossRef]
83. Soner, O.; Kayisoglu, G.; Bolat, P.; Tam, K. Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks. *Appl. Ocean Res.* **2024**, *142*, 103855. [CrossRef]
84. Paraskevas, A.; Madas, M.; Zeimpekis, V.; Fouskas, K. Smart ports in industry 4.0: A systematic literature review. *Logistics* **2024**, *8*, 28. [CrossRef]
85. Algarni, A.; Acarer, T.; Ahmad, Z. An edge computing-based preventive framework with machine learning- integration for anomaly detection and risk management in maritime wireless communications. *IEEE Access* **2024**, *12*, 53646–53663. [CrossRef]
86. Bolbot, V.; Kulkarni, K.; Brunou, P.; Banda, O.V.; Musharraf, M. Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *Int. J. Crit. Infrastruct. Prot.* **2022**, *39*, 100571. [CrossRef]
87. Cimpean, D.; Meire, J.; Bouckaert, V.; Stijn, V.C.; Pelle, A.; Hellebooge, L. *Analysis of Cyber Security Aspects in the Maritime Sector*; ENISA: Attiki, Greece, 2011.
88. Anderson, L.W.; Peter, W.; Airasian, K.; Cruikshank, D.R. *A Taxonomy for Learning, Teaching, and Assessing*; Longman: Harlow, UK, 2001.
89. Karim, M.S. Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat? *Mar. Policy* **2022**, *143*, 105138. [CrossRef]
90. BIMCO. *The Guidelines on Cyber Security Onboard Ships*; BIMCO: Bagsværd, Denmark, 2021.
91. Larsen, M.H.; Lund, M.S. Cyber risk perception in the maritime domain: A systematic literature review. *IEEE Access* **2021**, *9*, 144895–144905. [CrossRef]
92. Svilicic, B.; Rudan, I.; Frančić, V.; Mohović, D. Towards a cyber secure shipboard radar. *J. Navig.* **2020**, *73*, 547–558. [CrossRef]
93. Kapalidis, C.; Karamperidis, S.; Watson, T.; Koligiannis, G. A vulnerability centric System of Systems Analysis on the maritime transportation sector most valuable assets: Recommendations for port facilities and ships. *J. Mar. Sci. Eng.* **2022**, *10*, 1486. [CrossRef]
94. Oruc, A.; Amro, A.; Gkioulos, V. Assessing cyber risks of an INS using the MITRE ATT & CK framework. *Sensors* **2022**, *22*, 8745. [CrossRef]
95. Soomro, Z.A.; Shah, M.H.; Ahmed, J. Information security management needs more holistic approach: A literature review. *Int. J. Inf. Manag.* **2016**, *36*, 215–225. [CrossRef]
96. Puisa, R.; McNay, J.; Montewka, J. Maritime safety: Prevention versus mitigation? *Saf. Sci.* **2021**, *136*, 105151. [CrossRef]
97. Xing, B.; Dai, J.; Liu, S. Enforcement of opacity security properties for ship information system. *Int. J. Nav. Archit. Ocean Eng.* **2016**, *8*, 423–433. [CrossRef]
98. Kotis, K.; Stavrinos, S.; Kalloniatis, C. Review on semantic modeling and simulation of cybersecurity and interoperability on the Internet of Underwater Things. *Future Internet* **2022**, *15*, 11. [CrossRef]
99. Polatidis, N.; Pavlidis, M.; Mouratidis, H. Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Comput. Stand. Interfaces.* **2018**, *56*, 74–82. [CrossRef]
100. Mahmood, K.; Ferzund, J.; Saleem, M.A.; Shamshad, S.; Das, A.K.; Park, Y. A provably secure mobile user authentication scheme for big data collection in IoT-enabled maritime intelligent transportation system. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 2411–2421. [CrossRef]
101. Gyamfi, E.; Ansere, J.A.; Kamal, M.; Tariq, M.; Jurcut, A. An adaptive network security system for IoT-enabled maritime transportation. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 2538–2547. [CrossRef]
102. Sahay, R.; Meng, W.; Estay, D.A.S.; Jensen, C.D.; Barfod, M.B. CyberShip-IoT: A dynamic and adaptive SDN-based security policy enforcement framework for ships. *Future Gener. Comput. Syst.* **2019**, *100*, 736–750. [CrossRef]
103. Amro, A.; Oruc, A.; Gkioulos, V.; Katsikas, S. Navigation data anomaly analysis and detection. *Information* **2022**, *13*, 104. [CrossRef]

104. Solnør, P.; Volden, Ø.; Gryte, K.; Petrovic, S.; Fossen, T.I. Hijacking of unmanned surface vehicles: A demonstration of attacks and countermeasures in the field. *J. Field Robot.* **2022**, *39*, 631–649. [CrossRef]
105. Duran, C.A.; Fernandez-Campusano, C.; Carrasco, R.; Vargas, M.; Navarrete, A. Boosting the decision-making in smart ports by using blockchain. *IEEE Access* **2021**, *9*, 128055–128068. [CrossRef]
106. Albalawi, A.M.; Almaiah, M.A. Assessing and reviewing of cyber-security threats, attacks, mitigation techniques in IoT environment. *J. Theor. Appl. Inf. Technol.* **2022**, *100*, 2988–3011.
107. Yi, C.G.; Kim, Y.G. Security testing for naval ship combat system software. *IEEE Access* **2021**, *9*, 66839–66851. [CrossRef]
108. Kechagias, E.P.; Chatzistelios, G.; Papadopoulos, G.A.; Apostolou, P. Digital transformation of the maritime industry: A cybersecurity systemic approach. *Int. J. Crit. Infrastruct. Prot.* **2022**, *37*, 100526. [CrossRef]
109. Kalogeraki, E.M.; Apostolou, D.; Polemi, N.; Papastergiou, S. Knowledge management methodology for identifying threats in maritime/logistics supply chains. *Knowl. Manag. Res. Pract.* **2018**, *16*, 508–524. [CrossRef]
110. Kavallieratos, G.; Katsikas, S.; Gkioulos, V. SafeSec Tropos: Joint security and safety requirements elicitation. *Comput. Stand. Interfaces* **2020**, *70*, 103429. [CrossRef]
111. Svilicic, B.; Kamahara, J.; Rooks, M.; Yano, Y. Maritime cyber risk management: An experimental ship assessment. *J. Navig.* **2019**, *72*, 1108–1120. [CrossRef]
112. Zhou, X.Y.; Liu, Z.J.; Wang, F.W.; Wu, Z.L. A system-theoretic approach to safety and security co-analysis of autonomous ships. *Ocean Eng.* **2021**, *222*, 108569. [CrossRef]
113. Dghaym, D.; Hoang, T.S.; Turnock, S.R.; Butler, M.; Downes, J.; Pritchard, B. An STPA-based formal composition framework for trustworthy autonomous maritime systems. *Saf. Sci.* **2021**, *136*, 105139. [CrossRef]
114. Jo, Y.; Choi, O.; You, J.; Cha, Y.; Lee, D.H. Cyberattack models for ship equipment based on the MITRE ATT&CK framework. *Sensors* **2022**, *22*, 1860. [CrossRef]
115. Nganga, A.; Nganya, G.; Lützhöft, M.; Mallam, S.; Scanlan, J. Bridging the gap: Enhancing maritime vessel cyber resilience through security operation centers. *Sensors* **2023**, *24*, 146. [CrossRef] [PubMed]
116. Palbar Misas, J.D.; Hopcraft, R.; Tam, K.; Jones, K. Future of maritime autonomy: Cybersecurity, trust and mariner's situational awareness. *J. Mar. Eng. Technol.* **2024**, *23*, 224–235. [CrossRef]
117. Autsadee, Y.; Jeevan, J.; Mohd Salleh, N.H.B.; Othman, M.R.B. Digital tools and challenges in human resource development and its potential within the maritime sector through bibliometric analysis. *J. Int. Marit. Saf. Environ. Aff. Shipp.* **2023**, *7*, 2286409. [CrossRef]
118. Lee, C.; Lee, S. Evaluating the vulnerability of YOLOv5 to adversarial attacks for enhanced cybersecurity in MASS. *J. Mar. Sci. Eng.* **2023**, *11*, 947. [CrossRef]
119. Schinas, O.; Metzger, D. Cyber-seaworthiness: A critical review of the literature. *Mar. Policy* **2023**, *151*, 105592. [CrossRef]
120. Kavallieratos, G.; Katsikas, S. Managing cyber security risks of the cyber-enabled ship. *J. Mar. Sci. Eng.* **2020**, *8*, 768. [CrossRef]
121. Fischer-Hübner, S.; Alcaraz, C.; Ferreira, A.; Fernandez-Gago, C.; Lopez, J.; Markatos, E.; Islami, L.; Akil, M. Stakeholder perspectives and requirements on cybersecurity in Europe. *J. Inf. Secur. Appl.* **2021**, *61*, 102916. [CrossRef]
122. Oruc, A.; Gkioulos, V.; Katsikas, S. Towards a Cyber-Physical Range for the Integrated Navigation System (INS). *J. Mar. Sci. Eng.* **2022**, *10*, 107. [CrossRef]
123. Freire, W.P.; Melo Jr, W.S.; do Nascimento, V.D.; Nascimento, P.R.; de Sá, A.O. Towards a secure and scalable Maritime Monitoring System using blockchain and low-cost IoT technology. *Sensors* **2022**, *22*, 4895. [CrossRef]
124. Spravil, J.; Hemminghaus, C.; von Rechenberg, M.; Padilla, E.; Bauer, J. Detecting maritime GPS spoofing attacks based on NMEA sentence integrity monitoring. *J. Mar. Sci. Eng.* **2023**, *11*, 928. [CrossRef]
125. Söner, Ö.; Kayisoglu, G.; Bolat, P.; Tam, K. Cybersecurity risk assessment of VDR. *J. Navig.* **2023**, *76*, 20–37. [CrossRef]
126. Lim, J.H.; Kim, J.H.; Huh, J.H. Recent trends and proposed response strategies of international standards related to shipbuilding equipment big data integration platform. *Qual. Quant.* **2023**, *57*, 863–884. [CrossRef]
127. Illiashenko, O.; Kharchenko, V.; Babeshko, I.; Fesenko, H.; Di Giandomenico, F. Security-informed safety analysis of autonomous transport systems considering AI-powered cyberattacks and protection. *Entropy* **2023**, *25*, 1123. [CrossRef]
128. Svilicic, B.; Rudan, I.; Jugović, A.; Zec, D. A study on cyber security threats in a shipboard integrated navigational system. *J. Mar. Sci. Eng.* **2019**, *7*, 364. [CrossRef]
129. De la Peña Zarzuelo, I.; Soeane, M.J.F.; Bermúdez, B.L. Industry 4.0 in the port and maritime industry: A literature review. *J. Ind. Inf. Integr.* **2020**, *20*, 100173. [CrossRef]
130. Creech, J.A.; Ryan, J.F. AIS the cornerstone of national security? *J. Navig.* **2003**, *56*, 31–44. [CrossRef]
131. Bueger, C.; Liebetrau, T. Critical maritime infrastructure protection: What's the trouble? *Mar. Policy* **2023**, *155*, 105772. [CrossRef]
132. Kayisoglu, G.; Bolat, P.; Tam, K. Evaluating SLIM-based human error probability for ECDIS cybersecurity in maritime. *J. Navig.* **2022**, *75*, 1364–1388. [CrossRef]
133. Hareide, O.S.; Jøsok, Ø.; Lund, M.S.; Ostnes, R.; Helkala, K. Enhancing navigator competence by demonstrating maritime cyber security. *J. Navig.* **2018**, *71*, 1025–1039. [CrossRef]
134. Liu, J.; Li, C.; Bai, J.; Luo, Y.; Lv, H.; Lv, Z. Security in IoT-enabled digital twins of maritime transportation systems. *IEEE Trans. Intell. Transp. Syst.* **2021**, 1–9. [CrossRef]
135. Amro, A.; Gkioulos, V. Evaluation of a cyber risk assessment approach for cyber–physical systems: Maritime- and energy-use cases. *J. Mar. Sci. Eng.* **2023**, *11*, 744. [CrossRef]

136. Mohd Salleh, N.H.; Selvaduray, M.; Jeevan, J.; Ngah, A.H.; Zailani, S. Adaptation of Industrial Revolution 4.0 in a seaport system. *Sustainability* **2021**, *13*, 10667. [CrossRef]
137. Sepehri, A.; Vandchali, H.R.; Siddiqui, A.W.; Montewka, J. The impact of shipping 4.0 on controlling shipping accidents: A systematic literature review. *Ocean Eng.* **2022**, *243*, 110162. [CrossRef]
138. Luft, L.A.; Anderson, L.; Cassidy, F. NMEA 2000: A digital interface for the 21st century. In Proceedings of the 2002 National Technical Meeting of The Institute of Navigation, San Diego, CA, USA, 28–30 January 2002; pp. 796–807.
139. Maturana, M.C.; De Abreu, D.; Martins, M.R. Preliminary hazard analysis of vessel maneuvers in access channels to port terminals. In *Trends in Maritime Technology and Engineering*; CRC Press: Boca Raton, FL, USA, 2022.
140. Tang, C.S.; Veelenturf, L.P. The strategic role of logistics in the industry 4.0 era. *Transp. Res. Part E Logist. Transp. Rev.* **2019**, *129*, 1–11. [CrossRef]
141. Chang, C.H.; Kontovas, C.; Yu, Q.; Yang, Z. Risk assessment of the operations of maritime autonomous surface ships. *Reliab. Eng. Syst. Saf.* **2021**, *207*, 107324. [CrossRef]
142. Pleshakova, E.; Osipov, A.; Gataullin, S.; Gataullin, T.; Vasilakos, A. Next gen cybersecurity paradigm towards artificial general intelligence: Russian market challenges and future global technological trends. *J. Comput. Virol. Hacking Tech.* **2024**. [CrossRef]
143. Sridhar, S.; Govindarasu, M. Model-Based Attack Detection and Mitigation for Automatic Generation Control. *IEEE Trans. Smart Grid* **2014**, *5*, 580–591. [CrossRef]
144. Tsapin, D.; Pitelinskiy, K.; Suvorov, S.; Osipov, A.; Pleshakova, E.; Gataullin, S. Machine learning methods for the industrial robotic systems security. *J. Comput. Virol. Hacking Tech.* **2023**. [CrossRef]
145. Grech, A.; Simpson, P.; Zammit, R. Exploring the opportunities of generative artificial intelligence in concept ship design. In Proceedings of the 15th International Marine Design Conference, Amsterdam, The Netherlands, 2–6 June 2024.
146. Wolf, M.J.; Grodzinsky, F.; Miller, K.W. Generative AI and Its Implications for Definitions of Trust. *Information* **2024**, *15*, 542. [CrossRef]
147. Alowibdi, J.S. Gender Prediction of Generated Tweets Using Generative AI. *Information* **2024**, *15*, 452. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.