Journal of *Marine Science and Engineering*

MDPI

Article

Perspectives on the Cybersecurity of the Integrated Navigation System

Aybars Oruc [1,*], Georgios Kavallieratos [1,2], Vasileios Gkioulos [1] and Sokratis Katsikas [1]

[1] Department of Information Security and Communication Technology, Norwegian University of Science and Technology, 2815 Gjøvik, Norway; georgios.kavallieratos@ntnu.no (G.K.); vasileios.gkioulos@ntnu.no (V.G.); sokratis.katsikas@ntnu.no (S.K.)
[2] Department of Technology Systems, University of Oslo, 2007 Kjeller, Norway
* Correspondence: aybars.oruc@ntnu.no

Abstract: As maritime operations become increasingly reliant on interconnected information technology (IT) and operational technology (OT) systems, ensuring cybersecurity on vessels has become more critical than ever. One of these systems is the Integrated Navigation System (INS), which assists the Officer of Watch (OOW) on the bridge in ensuring safe navigation. The INS comprises several components that may be susceptible to cyber attacks, hence it faces cyber risks that need to be mitigated. Cyber risks are understood differently, depending on perspective. In this paper, we determine the perspective that the research community has of cyber risk, focusing on the INS, and that of professionals representing the maritime industry, and analyze similarities and differences. To this end, we conduct a systematic literature review and interviews with maritime professionals. This study provides useful insights for researchers and professionals seeking to understand the cyber risks of the INS.

Keywords: maritime cybersecurity; cyber risk; Integrated Navigation System (INS); SLR

Academic Editor: Claudio Ferrari

Received: 24 April 2025
Revised: 17 May 2025
Accepted: 23 May 2025
Published: 29 May 2025

Citation: Oruc, A.; Kavallieratos, G.; Gkioulos, V.; Katsikas, S. Perspectives on the Cybersecurity of the Integrated Navigation System. *J. Mar. Sci. Eng.* **2025**, *13*, 1087. https://doi.org/10.3390/jmse13061087

1. Introduction

As vessels handle 80% of the world's trade by volume, maritime transportation has a privileged position compared to other transportation modes [1]. Modern vessels are equipped with many computerized systems for different purposes, including navigation, propulsion, communication, cargo handling, safety, and security. Undoubtedly, the INS is one of the most critical systems onboard ships. An INS improves navigation safety by combining information and integrating functions to prevent geographic, traffic, and environmental hazards [2]. The INS is a combination of 25 types of components, including the Automatic Identification System (AIS), the Global Navigation Satellite System (GNSS), the Multifunctional Display (MFD), the RAdio Detection And Ranging (RADAR), and the Electronic Chart Display and Information System (ECDIS) [3]. Several studies have revealed the cyber threats and vulnerabilities of such components as well as of the INS as a whole [4–6].

The maritime ecosystem has been exposed to cyber attacks. To the best of our knowledge, currently, two cyber incident databases are available specifically for the maritime field. One of them is called the Maritime Cyber Attack Database (MCAD), consisting of 295 cyber incidents [7]. It was developed by researchers at the NHL Stenden University of Applied Sciences. The other one is called the Advanced Dataset of Maritime Cyber Incidents Released for Literature (ADMIRAL) project [8], managed by the non-profit organization France Cyber Maritime [9]. This database lists cyber incidents from 1980 to 2024 in

the maritime ecosystem [10]. It also presents various statistics. According to ADMIRAL, as of 10 October 2024, the maritime industry had experienced publicly disclosed 473 cyber incidents [10]. As shown in Figure 1, the number of disclosed cyber incidents has increased, particularly after 2019. These incidents include a variety of threats, including GNSS attacks, AIS attacks, data leaks, website compromises, and breaches of remote access systems [11].

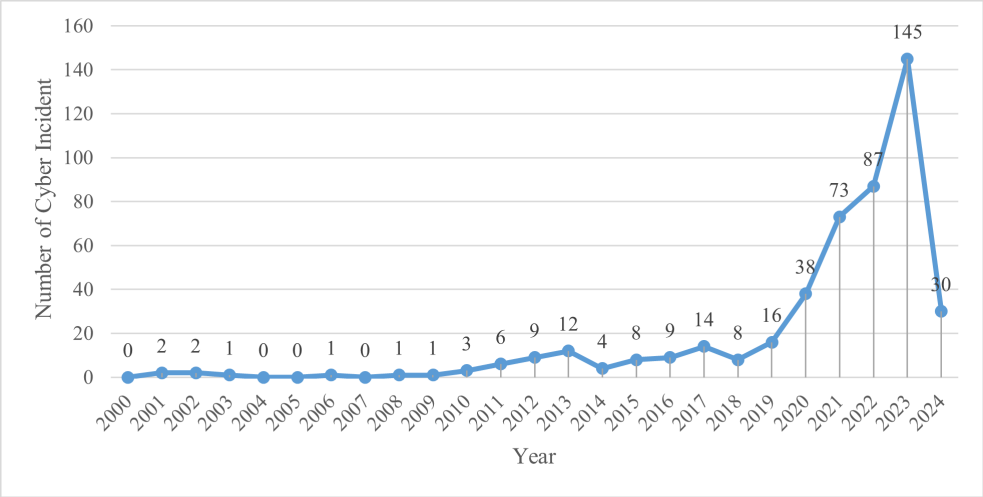

Figure 1. Distribution of publicly disclosed cyber incidents in the maritime sector (2000–2024) (derived from [10]).

In February 2017, for 10 h, malicious actors successfully assumed complete control over the navigation system of an 8250 twenty-foot equivalent unit (TEU) container vessel while it was en route from Cyprus to Djibouti [12]. The primary objective of the attackers was to steer the vessel towards a designated zone [12]. Two years later, in 2019, a tanker near the Naantali Port in Finland fell victim to ransomware as its administration server became infected due to a flash drive [13]. In the same year, an AIS base station in Italy was exposed to an AIS ship-spoofing incident near Elba Island. Incident investigation revealed the creation of 3742 ghost (fake) ships [14]. Cyber incidents continued to occur in the maritime sector in 2020 as well. Three ships experienced their administrative systems being infected by the ransomware *Sodinokibi*, which not only encrypts data but also poses a threat of information leakage, commonly known as ransomtheft [13]. In the same year, an advanced cyber attack disrupted the public website and several online services of the International Maritime Organization (IMO) [15]. In 2021, cyber attacks targeting military vessels were observed. The British warship *HMS Defender* (HMS stands for His/Her Majesty's Ship, representing the United Kingdom (U.K.)'s Royal Navy) was exposed to an AIS spoofing attack while navigating near Russia [16]. Also in 2021, the Dutch warship *HNLMS Evertsen* (HNLMS stands for His/Her Netherlands Majesty's Ship, representing the Dutch Royal Navy) was subjected to Global Positioning System (GPS) jamming in the Black Sea [16]. In 2022, the hacktivist group Anonymous targeted Vladimir Putin's luxury yacht by renaming it *FCKPTN* and leaking its location data. This attack was assumed to be a protest against the military operations of Russia in Ukraine [17]. In 2024, the United States (U.S.) conducted a cyber attack on the Iranian military vessel *M/V Behshad* (M/V stands for motor vessel), which was allegedly used for surveillance and suspected of involvement in attacks on commercial ships. That same year, an IMO employee's mistake led to the accidental exposure of 159 personal and business e-mail addresses, highlighting both human error and technical vulnerability [18].

The increasing number of cyber incidents and the economic importance of the maritime sector have led to rising cybersecurity concerns in the industry [19]. Nevertheless,

the perception of cyber risks and their mitigation measures is not uniform and depends on various factors, such as professional experience and domain-specific knowledge. Therefore, diversity between the perspectives of the academic and professional communities is frequently observed.

The objective of this paper is to understand the perspectives of the research and professional communities on INS cybersecurity, particularly regarding threats, vulnerabilities, mitigation measures, and the practical effectiveness of these measures. The paper analyzes both perspectives and identifies similarities and differences by comparing them. This enables researchers to better understand the practical barriers that hinder the implementation of their proposed solutions by the maritime sector. At the same time, it allows effective practices from the industry to be reflected in the academic literature. Furthermore, this dual perspective guides researchers in scientifically verifying real-world solutions, thereby generating new research questions and contributing to more applicable and impactful cybersecurity research.

To this end, the perspective of the research community was established by performing a systematic literature review (SLR) of the relevant literature. The professional perspective was established by means of interviews with eight active professionals in the maritime industry and two Ph.D. candidates with a professional maritime background studying maritime cybersecurity. Artificial intelligence (AI) writing assistants ProWritingAid [20] and Grammarly Pro [21] were used to enhance the clarity and academic readability of the article. Both writing tools made suggestions for grammar, writing style, sentence, and structural enhancements, therefore contributing to the refining of the paper.

Through this combined approach, a number of findings and recommendations from scientific papers have been verified by industry practices. Additionally, it has facilitated the inclusion of industry practices in the literature. This study unveiled that both communities have concerns about the cyber vulnerabilities of INS components, such as AIS, GNSS, and outdated operating systems of OT components. However, notable differences were identified between the mitigation measures applied. Researchers typically propose advanced technical solutions developed and tested in controlled laboratory environments. However, many studies do not have an evaluation in the real world. In contrast, maritime professionals emphasize the practical limitations of implementing these measures, including compatibility issues and cost constraints. Moreover, many of the solutions proposed by researchers are not commercially available to ship operators. Therefore, ship operators typically follow temporary solutions. This study enables the closure of the gap between literature and industry practices, leading to the emergence of new research questions for researchers. To the best of our knowledge, this is the first analysis of this kind.

The remainder of the paper is organized as follows: Section 2 summarizes various academic and industrial publications about maritime cybersecurity. Section 3 presents the methodology used to perform the SLR and the resulting research community perspective of INS cyber risk. Section 4 presents the methodology used to establish the professional community perspective and the respective findings. In Section 5, the findings obtained from the academic and professional perspectives are analyzed in detail. Last, Section 6 offers our conclusions and possible future research directions.

2. Related Work

The Related Work section summarizes various academic and industrial publications about maritime cybersecurity. Therefore, it provides the current status and research gaps of the field. In this section, literature review studies on maritime cybersecurity are investigated. The subjects, such as threat modeling, risk assessments, and cyber vulnerabilities, are examined in studies. After scientific papers, reports published by the renowned or-

ganizations are analyzed. These publications present real-world insights into emerging threats, attack trends, and operational challenges in the maritime industry. Therefore, the approaches in both academic and industrial publications could be analyzed. By including both scientific studies and industry reports, this section allows a comprehensive understanding of the maritime cybersecurity domain.

Ben Farah et al. [22] conducted an SLR for cybersecurity in the maritime industry, including smart ports and autonomous ships. In this study, the authors investigated cyber attack classification, vulnerabilities onboard ships and in port infrastructures, and the role of new technologies. The paper states the most vulnerable components, cyber incidents, and the potential risks of system interconnectivity. The paper also expresses the need for standardized cybersecurity protocols, improving cybersecurity awareness, and governance practices.

Bolbot et al. [23] performed an SLR and bibliometric analysis of maritime cyber studies. A total of 144 Scopus-indexed papers were reviewed by employing the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) methodology. The authors classified the papers into ten groups, including risk assessment, penetration testing, incident analysis, and training. According to findings, the main contributors are from the institutions in Norway, the UK, France, and the USA, respectively. The study also identified the leading journals and researchers in the field of maritime cybersecurity.

Erbas et al. [24] conducted an SLR on cyber risk assessment and threat modeling for ships. A total of 25 peer-reviewed papers were investigated by employing the PRISMA methodology. The authors identified various methods implemented for different ship systems, such as navigation, engine control, and communication. The authors also present threat types, including RADAR jamming, AIS spoofing, malware infections, phishing attacks, and so on. In the study, methodological inconsistencies and research gaps are highlighted as well.

Clavijo Mesa et al. [25] investigated the impacts of cyber attacks and mitigation measures for maritime supply chains. To this end, a total of 110 peer-reviewed papers were reviewed by the SLR method. The authors identified eight types of essential cyber threats, such as malware, denial of service (DoS), brute force, watering hole, port scanning, and so on. The authors also suggested 18 mitigation measures classified into technical measures, policy recommendations, and training activities.

Dimakopoulou and Rantos [26] analyzed maritime cybersecurity from the perspective of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) v2.0. In the study, a total of 113 scientific papers were reviewed by performing an SLR method. NIST CSF 2.0 consists of six functions, including Govern, Identify, Protect, Detect, Respond, and Recover. The paper maps cybersecurity practices and gaps across these functions. The authors identified various issues, such as inadequate governance, lack of awareness training, and insufficient monitoring.

Scientific studies published by researchers provide theoretical insights and methodological contributions about maritime cybersecurity. On the other hand, reports published by renowned organizations offer a practical perspective on the real-world challenges in the sector.

Maritime Cyber Priority 2024/2025 [27], published by Det Norske Veritas (DNV), offers a global survey with the attendance of 489 maritime professionals and interviews with sector leaders. The report highlights the increasing cyber incidents in the sector and the OT vulnerabilities of ship systems. According to the report, regularity requirements should be improved to force ship owners to the cybersecurity investments. The report also reveals cybersecurity risks in the supply chain. DNV states that cultural change is a significant requirement to prevent cyber attacks.

Maritime Cyber Threat Overview 2023 [28], published by Maritime Computer Emergency Response Team (M-CERT) in collaboration with OWN, offers a global perspective on cyber threats targeting the maritime sector. In 2023, the report identifies 612 cyber incidents. A significant part of these attacks appears to be related to geopolitical conflicts, such as the Russia–Ukraine war and the Israel–Hamas conflict. The report highlights the impact of state-sponsored cyber attacks. According to the report, malicious actors targeted maritime infrastructures, such as ports, terminals, and shipyards. The report also includes types of threats, such as ransomware and watering hole attacks.

Annual Threat Assessment 2025 [29], published by NORMA Cyber, presents an analysis of the cyber threat landscape of the maritime industry. The report includes state-sponsored attacks, ransomware, credential theft, and OT vulnerabilities as core concerns. In accordance with the report, AIS and GNSS spoofing attacks were experienced in the Baltic and Red Seas. The report underscores a growing convergence of physical and cyber threats. NORMA Cyber also invites maritime stakeholders to share more information regarding experienced cyber incidents.

In summary, the reviewed literature and industry reports reveal that cyber threats and vulnerabilities are one of the most critical issues of the maritime industry. The INS and its OT components include various cyber risks. Scientific papers tend to emphasize technical innovations, modeling techniques, and risk assessment applications. Such studies are typically conducted in controlled environments and lack real-world validation. In contrast, industry reports provide threat intelligence and operational insight through practical experience. However, these publications do not have scientific clarity.

Our study presents a novel synthesis by comparing the perspectives of both scientists and maritime professionals on INS cybersecurity. By combining literature review findings and experts' insights, it closes a critical gap between theory and practice. It verifies academic findings with operational practices. Moreover, it reveals operational practices that are currently unavailable in the literature. This study not only enriches the academic literature but also supports the development of more practical cybersecurity solutions for the maritime industry. To the best of our knowledge, this is the first work to explicitly contrast and integrate these two perspectives in the field of maritime cybersecurity.

3. Research Community Perspective

3.1. Methodology

The perspective of the research community on potential cyber risks in the INS was identified through an SLR. The purpose of this review is to synthesize the current state-of-the-art knowledge from academic studies by providing an overview of how researchers perceive and address these risks. To achieve this, relevant vulnerabilities, threats, mitigation techniques, and mechanisms are investigated. An SLR, a secondary study based on primary sources, is conducted to map, identify, critically evaluate, consolidate, and aggregate the findings of related sources on a specific research issue [30]. In this study, the method described by Okoli and Schabram [31] was used to conduct the SLR, as it is formulated to meet the needs of information systems research [32]. This method consists of eight steps, as follows.

1. Identify the purpose;
2. Apply practical screen;
3. Draft protocol and train the team;
4. Search for literature;
5. Appraise quality;
6. Extract data;
7. Synthesize studies;

8. Write the review.

3.1.1. The Purpose of the Literature Review

The essential purpose of this study is to identify and present the current state-of-the-art for potential cyber risks in the INS. This objective is pursued by addressing the following research questions.

- RQ 1. Identifying potential vulnerabilities and threats.
- RQ 2. Determining relevant data sources, hardware, and software tools for research activities.
- RQ 3. Identifying technical measures to mitigate risks.

3.1.2. Practical Screening

Inclusion and exclusion criteria are established to identify only the most relevant publications for further exploration. The inclusion criteria for this study were defined as follows:

- Only publications in English;
- Only scientific publications published in journals, conferences, workshops, and books;
- The publication period: January 2010–15 February 2025.

The defined exclusion criteria include conference abstracts, book reviews, conference information, discussions, editorials, newsletters, and short communications.

3.1.3. Defining the Protocol

The appropriate keywords “maritime”, “ship”, and “cybersecurity” were identified for the protocol stage. Then, synonyms of the identified keywords were determined. The synonym identified for “maritime” was “marine”. For “ship”, the synonym was “vessel”, and for “cybersecurity”, it was “cyber security”. Next, “AND” was used to concatenate the keywords, while “OR” was used to combine the synonyms. The following search string was eventually formulated: (("maritime”) OR (“marine”)) AND ((“ship”) OR (“vessel”)) AND ((“cybersecurity”) OR (“cyber security”)). Using this string in Google Scholar returned over 20,000 results. Consequently, the keyword “experiment” was added to refine the search. The resulting string, ((“maritime”) OR (“marine”)) AND ((“ship”) OR (“vessel”)) AND ((“cybersecurity”) OR (“cyber security”)) AND “experiment”, was used exclusively in Google Scholar.

3.1.4. Searching for the Literature

The review was conducted by accessing relevant publications published between January 2010 and 15 February 2025 from publishers’ databases and online libraries, including the Association of Computing Machinery Digital Library (ACM DL), Institute of Electrical and Electronics Engineers (IEEE) Xplore, ResearchGate, Science Direct, Springer Link, TransNav, and Wiley Online Library. Google Scholar was also utilized to access relevant publications available in other databases.

The search string mentioned in Section 3.1.3 was modified as necessary. Where possible, searches were conducted within the title, abstract, keywords, and full text of the publications. Additionally, when applicable, publications were searched within the research fields of engineering, computer science, and other relevant disciplines. The fields of social sciences, political science, business management, law, psychology, and similar areas were excluded from the search parameters. A total of 4520 publications were identified in the initial stage.

3.1.5. Quality Appraisal

The initial screening of the database resulted in a total of 4520 publications. In the quality appraisal phase, another filter was applied to identify the most relevant publications for the research questions. The filter was as follows:

> "Only studies that employed empirical methods (e.g., models, simulations, or practical testing) were considered."

During the literature review, it was observed that many papers include assumptions about cyber vulnerabilities which have not been methodically verified, for example, through penetration testing or mathematical models. By applying this filter, we avoided unsupported or poorly supported threat assumptions. This study focuses on academically verified publications that utilize scientific methods rather than speculative predictions.

The specified filter was applied in three stages. In the first stage, titles and keywords were reviewed, and duplicates were removed. This reduced the number of publications to 162. In the second stage, abstracts and conclusions were assessed. As a result, 80 publications that did not align with the research focus were excluded. Additionally, during the evaluation, the references of the reviewed publications were analyzed for backtracking, leading to the discovery of 28 additional publications that might contribute to the research questions. At the beginning of the third stage, 110 publications remained. The full texts of these publications were thoroughly analyzed, and those deemed non-contributory to the research objectives were excluded. Finally, 57 publications focusing on the cybersecurity of the INS and/or its components were selected for use in this study. Figure 2 illustrates the number of publications at each stage. These publications were analyzed to understand research trends, publishers, the distribution of publication types, and the number of publications per year.

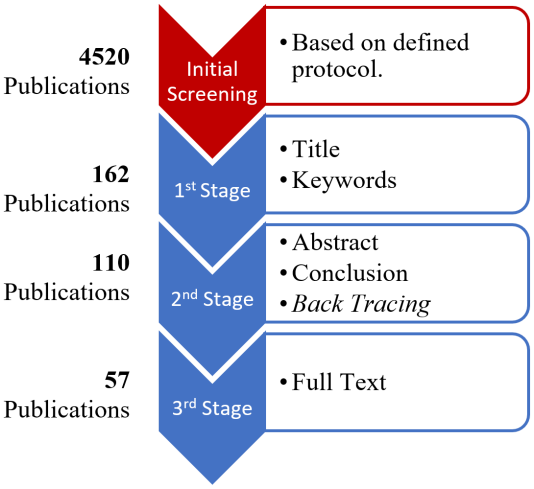

Figure 2. Publication number by stages.

All reviewed publications, along with their publication year, type, and the component studied, are presented in Table A1 in the Appendix A. Among the 57 reviewed publications, 31 were journal articles, 2 were book chapters, and 24 were conference papers, published by 14 different publishers. IEEE became the most prominent publisher by accounting for 20 publications. Springer Link followed with 8 publications. MDPI and TransNav each contributed 6 publications.

Table 1 shows the number of publications by year. GNSS and AIS were the most frequently studied components. However, other components, including RADAR and bridge network systems, have also gained attention in recent years. Accordingly, there is a recognized need for further studies on the cybersecurity of additional components of the

INS, including anemometers, Bridge Navigational Watch Alarm Systems (BNWASs), echo sounders, gyro compasses, and Heading Control Systems (HCSs).

Table 1. Publication number by year and component (until 15 February 2025).

Year	AIS	ECDIS	GNSS	MFD	Network	RADAR	Total
2014	1						1
2015			1				1
2016			1				1
2017	2		3				5
2018			1	1			2
2019	1	4	2	1	2		10
2020	5	1	1			1	8
2021	2	1	1		3	1	8
2022	3		2		2	1	8
2023			2			2	4
2024	2	1	2	1	2	2	10
Last 3 years	5	1	6	1	4	5	22
Total	16	7	16	3	9	7	58

The publications listed in Table 1 each focus on a single component. However, one publication [33] examines both the ECDIS and RADAR components together. Even though the total number of publications is expected to be 57, this overlap leads to a total count of 58 publications.

3.1.6. Data Extraction

The purpose of this step is to gather the necessary data from the selected publications based on the research questions in Section 3.1.1. Information was extracted regarding vulnerabilities, threats, and vulnerable components within the INS, potential tools (both hardware and software) for cybersecurity studies, and technical risk mitigation measures. Additionally, useful definitions were collected to provide further context for the readers. Publication details, including the publisher, type, and year of publication, were also extracted. The extracted information from the reviewed publications was classified. The Citavi software 6.18.0.1 [34] was used to organize the knowledge gathered from the publications.

3.1.7. Synthesis of Studies

This step involves synthesizing the extracted data. The synthesis was organized according to the research questions outlined in Section 3.1.1. The study was further enhanced with supportive elements.

3.1.8. Writing the Review

The final stage of the SLR conducted in this study involves writing a comprehensive review that systematically and thoroughly discusses the explanations. The findings of the study were adequately reported, adhering to standard principles for writing research publications. Sufficient descriptive details are provided, as demonstrated in the following sections.

3.2. Tools and Data Sources for INS Cybersecurity Research

In this section, relevant data sources, hardware, and software tools for cybersecurity research on the INS are discussed. Certain tools mentioned have not been shared publicly because of the risk of weaponization. Additionally, some authors have notified the relevant parties about potential vulnerabilities in their services or products [4].

3.2.1. Hardware

The components onboard ships in service, such as oil/chemical tankers, research vessels, roll-on/roll-off passenger (RoPax) ships, yachts, training vessels, or liquefied natural gas (LNG) carriers, may be used as test environments [5,35–39]. However, finding a vessel in service could be difficult for research purposes. Moreover, the components could be damaged during an experiment, and the vessel might lose her seaworthiness. Accordingly, individual components, such as the AIS, GPS, RADAR, MFD, or ECDIS, may be tested in a controlled environment as well [4,36–38,40–42]. Moreover, simulated components can also be used in research activities [43].

A laptop, personal computer (PC), or server (e.g., HP ProLiant DL380 G7 Server) is required to run software for different purposes [33,38,44]. A laptop also enables mobility for researchers. A USRP X310 is a software-defined radio (SDR) to use in cybersecurity research and it is possible to use it in testing protocols for communication technologies [45,46]. A Raspberry Pi 3B+ board may be used to analyze in real-time NMEA message flow [41]. An Adalm-Pluto [47], which is an RF transmitter and receiver, could be used to demonstrate jamming and spoofing attacks [41]. In addition, 3G/4G routers could be required to enable internet connection in a testbed, such as GlobeSurfer III or GlobeSurfer III+ [44]. As a unified threat management (UTM) component, a Kerio Control NG 100w could be a suitable solution [44]. A ship network may be equipped with a controller (e.g., WAGO PFC200) which can store all control data and encrypt it directly inside via Secure Sockets Layer (SSL) [44]. An antenna may be required to transmit GPS messages to demonstrate a spoofing attack [5].

A test environment against GPS spoofing attacks is illustrated in [48]. A spoofer setup on a superyacht is shown in [5]. A nine-channel single frequency RF front-end (for E1/L1) and NI PXI System with bitgrabber and data streamer are used in [49] to develop a testbed against GNSS spoofing attacks.

3.2.2. Software and Data Sources

Vulnerability scanners (e.g., Nessus Professional) could be executed in passive mode to detect vulnerabilities of components underlying operating systems [36,37,43,50]. Paid or free vulnerability scanning software for Microsoft Windows and Linux operating systems, such as Kali, ImmuniWeb, Netsparker, Acunetix, Nexpose, Core Impact, OpenVAS, NMAP, and Retina, is available in the market [42,43,51–53]. For testing cyber attacks such as DoS, hping3 [54] can be utilized to simulate heavy traffic scenarios and evaluate the resilience of ship network components under stress [55]. Scapy [56], on the other hand, is instrumental for man-in-the-middle (MITM) attack simulations, allowing manipulation and inspection of packets in real time [55]. Fedora Linux [57], known for its stability and versatility, can also be utilized as a robust environment for running various security tools and simulations, such as those involving maritime radar systems and their cybersecurity vulnerabilities [58]. Lockdown software, such as Trend Micro Safe Lock, could be used to restrict access to sensitive functions in operating systems [36,59]. Chart plotters (e.g., OpenCPN) or AIS ship tracking services (e.g., Marine Traffic) could be useful to understand the effect of a potential attack or research [4,33,41,42,53,60–62]. A tool to generate fake AIS messages (i.e., AIVDM sentence) such as AIVDM Encoder shared on GitHub could be required [4,63].

AIS VDM/VDO Decoder [64] (VDM: Vessel Data Message and VDO: Vessel Data Out) is another useful tool that can decode and simulate AIS messages, allowing for the testing of AIS security mechanisms and ensuring message integrity during cybersecurity studies [65]. GNURadio is used to design and implement software-defined radios, and it is possible to adapt it for building an AIS transmitter and an Iridium module [4,45,46]. MATLAB R2025a could be employed for simulations and modeling in AIS cybersecurity studies, such as testing encryption methods or signal interference scenarios [66]. A Sophos XG Firewall may be preferred as a firewall solution in ship networks [44]. A dataset of AIS base station or fleet data of a maritime authority could be required [67]. Bridge Command is a free ship simulator to be used as a training tool for navigation, RADAR, ship handling, and other seamanship skills [68]. Given that Bridge Command transmits mimic NMEA messages, it can be used not only for training but also for cybersecurity studies [53,62,69]. NMEA network traffic can also be captured from a vessel in service [70]. Wireshark [71] is a widely used network protocol analyzer. It can be executed to capture NMEA messages from the network [42,53,55]. The Cinematic RADAR Simulator can be used for RADAR simulations [72]. VMWare ESXi [73] can be used to create virtual machines simulating a ship's network environment, providing a controlled and scalable testing platform for malware and defense mechanism evaluations [69]. To simulate ship power systems in real time and assess control system performance, OPAL-RT [74] is used as a powerful tool, offering hardware-in-the-loop (HIL) capabilities [55].

3.3. Cyber Threats and Vulnerabilities

Several cyber threats and vulnerabilities of the INS have been analyzed in the literature. Most of them solely focus on specific components of the INS or the vulnerabilities inherited by third-party components, such as middleware and the operating system.

3.3.1. AIS

The AIS assists navigators by transmitting and receiving navigation-related information. There are several vulnerabilities and threats associated with the AIS. The AIS lacks any authentication mechanism for the transmitted data [75]. This weakness makes AIS vulnerable to several software-based and radio frequency (RF)-based threats, classified in three classes, namely, spoofing, hijacking, and availability disruption [4]. More specifically, threats such as ship spoofing, AIS-Search and Rescue Transponder (AIS-SART) spoofing, weather forecasting, AIS hijacking, and availability disruption threats (i.e., slot starvation, frequency hopping, and timing attack) have been reported [4]. Klor et al. [76] further demonstrated a stealthy, selective jamming attack on AIS using commercial SDRs, which exploit transmission slot predictability to suppress specific vessel messages and disrupt situational awareness without detection. Additionally, the Maritime Mobile Service Identity (MMSI) number recorded in the AIS could be forged and tampered with [77]. It is also possible to indicate fake vessels in the AIS ship tracking services (e.g., Marine Traffic) [4,78]. The authors of [60] developed the Marine Traffic Simulator to perform the following attacks on the AIS: denial of service (DoS), message fabrication, and faking of essential data [60]. The software was tested on MarineTraffic.com, ECDIS, and OpenCPN software, and the attacks were successfully executed [60]. The AIS system contains a cyber vulnerability that allows attackers to send covert command and control messages to remotely access ship systems [42].

3.3.2. ECDIS

The ECDIS can represent the position of its own vessel by receiving data from an Electronic Position Fixing System (EPFS), such as GNSS. A cyber risk assessment process for the ECDIS is proposed in [35,43]. The process for a vulnerability scan of ECDIS units

is discussed in [35,37,39] and its results are presented in [35,37,39,43,52]. Malware may manipulate the ship position on the ECDIS [6]. The ECDIS might be infected by malware; however, malware may wait for a malicious actor to be triggered. Moreover, mission-specific malware introduced through the Universal Serial Bus (USB) interface of the ECDIS could be used to manipulate rudder angle, potentially altering the vessel's course in a manner that may evade immediate detection [79]. The ECDIS typically receives AIS messages. The malware might be triggered to initiate an attack by transmitting forged AIS messages. RADAR may also be infected by malware and can be triggered by a transmitted malicious command to the RADAR through an electronic attack [33]. Additionally, the vulnerabilities of middleware (e.g., Apache Web Server) are inherited and increase the attack surface of ECDIS [39,43]. Further, the onboard network is vulnerable to person-on-the-side attacks and man-in-the-middle attacks [61].

3.3.3. GNSS

The GNSS provides vessels with critical information related to positioning, speed, and time [80]. The signal strength of GNSS for civilian applications is approximately −160 dBW at sea level [80], which makes it inherently vulnerable to cyber threats. Consequently, GNSS receivers are susceptible to both jamming and spoofing attacks [5,40,45,48,51]. A block diagram illustrating the architecture of GNSS spoofing attacks can be found in [49]. Spoofing attacks mislead GNSS receivers by providing false positioning data [81], whereas jamming attacks interfere with the reception of GNSS signals [82]. The impact of a jamming attack varies depending on the sensitivity of the receiver, the power of the jammer, and the distance between the two [40]. Spoofing attacks are generally considered more dangerous than jamming attacks due to their stealthy nature and the challenges associated with their detection [83]. GNSS technology encompasses various regional systems, including the U.S.'s GPS, Russia's Global'naya Navigatsionnaya Sputnikovaya Sistema (GLONASS), China's BeiDou Navigation Satellite System (BDS), and the European Union's Galileo system [84]. According to experimental data collected in northern Norway, the GLONASS G1 frequency band demonstrates greater resistance to jamming compared to the GPS L1 band [40].

3.3.4. RADAR

The cyber risk assessment process and its results for two RADAR sets are presented in [36]. Longo et al. [69] highlight critical cyber vulnerabilities in maritime RADAR systems by demonstrating the exploitation of unencrypted communication protocols such as National Marine Electronics Association (NMEA) and All-purpose STructured Eurocontrol Surveillance Information Exchange (ASTERIX). These vulnerabilities allow attackers to inject false RADAR echoes or manipulate existing ones, posing serious risks to the ship's situational awareness and navigation safety. In addition, Wolsing et al. [62] reveal similar vulnerabilities in marine RADAR systems, focusing on unprotected User Datagram Protocol (UDP) transmissions in the Navico BR24 protocol, which make these systems susceptible to network-level cyber attacks that can manipulate RADAR images or disrupt communication entirely. Furthermore, Longo et al. [58] emphasize how sophisticated cyber false flag operations can exploit these vulnerabilities by simulating electronic countermeasures to mislead the crew into believing they are facing traditional electronic warfare, thereby complicating attribution and response efforts.

3.3.5. Operating System

Several systems, including the ECDIS, RADAR, and MFD, are supported by various operating systems, such as Microsoft Windows 7 Professional, Microsoft Windows XP, Microsoft Windows Embedded Standard 7, and Linux [35,36,52,85]. The diversity of

operating systems increases the vulnerabilities and the attack surface. The operating systems are updated for different purposes, such as improving performance, releasing new features, and fixing problems or cyber vulnerabilities. However, some operating systems are no longer supported by the vendor [35]. Moreover, even if the operating system is supported by the vendor, the updates may not be timely installed by the ship operator. In this case, the underlying operating system endangers the INS components in terms of cyber vulnerability. For instance, the Server Message Block (SMB) service in Microsoft Windows operating systems provides file and printer sharing [37]. The SMBv1 in the operating system (e.g., Microsoft Windows Embedded Standard 7) might not be up-to-date, so a marine system could be attacked by NotPetya ransomware [36]. Given that signing and security signatures are not required for the SMB service, the component is vulnerable to man-in-the-middle attacks [36]. The Security Account Manager (SAM) is a database used to store the hashed passwords of Microsoft Windows users [86]. A malicious actor may access the SAM database to capture such hashes [37]. An arbitrary remote code vulnerability could exist in the service of Remote Desktop, so the vulnerability may be exploited by a malicious actor executing arbitrary code [38]. Although such vulnerabilities are mitigated by leveraging security patches, the lack of a security plan and of regular software updates on board increase the attack surface.

3.3.6. Other Threats and Vulnerabilities

An INS architecture and the results of a vulnerability scan are presented in [38]. The feasibility of displaying fake ships using OpenCPN and the Cinematic RADAR Simulator is demonstrated in [33], which also introduces attack models targeting RADAR and ECDIS/AIS integration. A method for integrating RADAR imagery with AIS data is proposed in [87]. Furthermore, simulation-based attacks have revealed vulnerabilities in ship networks, particularly within the industrial control systems (ICSs) responsible for navigation. These attacks demonstrate how tampering with critical ICS data can lead to operational anomalies and compromise navigational safety [88]. Additionally, Visky et al. [89] demonstrated that the MFD is vulnerable to cyber attacks such as eavesdropping, spoofing, and DoS.

3.4. Risk Mitigation Measures

3.4.1. AIS

A risk assessment of AIS messages is proposed by Iphar et al. [67]. For instance, the relevance of received messages can be evaluated by comparing the vessel type with the cargo type. To verify the accuracy of the broadcasted MMSI number via AIS, the authors suggest comparing the MMSI with the registration authority's dataset. Several encryption methods have been proposed to enhance AIS message security [46,65,75,90–92]. A digital certificate-based identity authentication scheme (IAS) is introduced by Su et al. [77]. Additionally, Shyshkin [66] presents a method to ensure AIS message authentication and integrity through the use of message authentication codes (MACs) and digital watermarking, offering full compatibility with existing AIS functionality while mitigating the risks of spoofing and message manipulation. Silonosov and Henesey [93] propose the use of attribute-based encryption (ABE) to ensure AIS data confidentiality. Moreover, the reliability of AIS information can be enhanced by correlating RADAR imagery with AIS data [87].

3.4.2. GNSS

IRIDIUM is the satellite platform used to initiate and receive IRIDIUM calls [45]. GNSS spoofing attacks may be detected by analyzing IRIDIUM Ring Alert (IRA) messages [45]. For GNSS spoofing attacks, the Nomoto model for the steering dynamics of a vessel and ex-

ploiting tools from linear control theory is proposed in [94]. A pseudo-random noise (PRN) code construction method based on a chaotic-form logistic map against GNSS spoofing is proposed in [95]. A set of mitigation algorithms are introduced against GNSS spoofing, multipath and radio frequency interference (RFI) in [49]. An integration of GNSS with the inertial navigation system facilitates the detection of position anomalies [96,97]. GPS anomalies can be detected by leveraging machine learning techniques [41]. The carrier-to-noise ratio (C/No) is utilized to detect GPS spoofing attacks [48]. Additionally, a low-cost GPS spoofing detection framework called MANA (MAritime Nmea-based Anomaly detection) has been proposed, which leverages anomaly detection by monitoring NMEA-0183 sentences. MANA combines various software-based methods, such as pairwise distance monitoring (PDM) and clock drift monitoring (CDM), enabling real-time spoofing detection without requiring expensive hardware upgrades [98]. A further mitigation strategy against GNSS spoofing involves using differential GNSS (DGNSS) systems, where correction signals from fixed reference stations with known geodesic accuracy are used to detect spoofing attacks [99]. By comparing the real-time positions calculated using GNSS signals and the corrected positions from DGNSS, discrepancies can be identified, indicating potential spoofing. Moreover, a convolutional neural network (CNN)-based approach has been proposed to detect anomalies in GNSS data received by vessels, enhancing cybersecurity in maritime communication systems. This approach supports real-time monitoring and automatic detection of spoofed signals, leveraging deep learning techniques to improve accuracy over traditional methods [100]. Furthermore, Singh et al. [101] proposed a GNSS spoofing detection and mitigation approach that integrates an auxiliary navigation component with receiver autonomous integrity monitoring (RAIM) and a genetic algorithm.

The resilience of GPS against jamming attacks is improved by leveraging a combination of GPS and GLONASS receivers [40]. To mitigate the impact of GNSS jamming attacks, a method based on Bayesian inference and correlation of AIS messages has been proposed [102]. This method analyzes AIS broadcasts to detect GNSS coordinate loss across multiple vessels, helping to confirm jamming attacks and providing a remote monitoring capability using standard maritime equipment. By comparing the status of vessel coordinates within a monitored area, the method identifies patterns of coordinate loss, allowing for early detection and response to GNSS jamming incidents.

3.4.3. RADAR

It is crucial to secure communication protocols used within the INS, such as NMEA and ASTERIX, by implementing cryptographic protections like encryption and message authentication. This will prevent unauthorized manipulation of RADAR data, as demonstrated in recent cyber vulnerability research [69]. Network-based anomaly detection tools, as proposed by Basels et al. [103], can also be utilized to identify anomalies that may occur in RADAR systems as a result of cyber attacks. Furthermore, intrusion detection systems (IDSs) such as Kitsune, SteadyTime, and Snort can be employed to detect cyber threats targeting RADAR systems by analyzing network traffic and identifying suspicious patterns [104].

3.4.4. Operating Systems

Updating operating systems and patching against security vulnerabilities provides significant protection for onboard systems [36,37]. Further, lockdown software is used to restrict sensitive functions of operating systems as a proactive safeguard against unknown threats and vulnerabilities [36,59]. Access control and role-based authentication mechanisms protect system functions and operations [6]. If the component runs on Windows operating systems, the service of Windows Script Host may be disabled [6].

3.4.5. Network

Even though the International Electrotechnical Commission (IEC)'s 61162 standard is referred to only as footnotes in the IMO documents, most marine components comply with the requirements of that standard [105]. IEC 61162 is divided into five parts [106], and IEC 61162-450 [107] for internal communication among bridge components is typically used on contemporary vessels. Authentication mechanisms compatible with IEC 61162-450 can prevent common cyber attacks. Even though IEC 61162-460 [108] brings cybersecurity measures for the ship network, such as firewalls, network access control, and security monitoring, it has not been used widely yet [61]. The authors of [109] proposed a stochastic game model to establish the ship network security defense strategy selection method.

Several authentication techniques have been proposed to protect the ship networks [70,110]. MARitime multi-Message Authentication Code (MARMAC) based on symmetric cryptography and SIGnatures for MARitime systems (SIGMAR) based on asymmetric cryptography are low-cost solutions for retrofit authentication [70,110]. MARMAC outperforms SIGMAR in transmission delay [70].

Physical network isolation is of importance for a proactive solution [37]. The network segmentation of the IT and OT infrastructure is proposed in [44]. Another proposal for a more secure network onboard is to create a software-defined network (SDN) [111]. The ship IT and OT networks, such as guest network, administration network, and OT network, may be partitioned using a UTM hardware appliance [44]. The internet connection to the INS should not be established if it is not required [38]. However, the INS may be connected to the internet for the update of the Electronic Navigation Chart (ENC) in ECDIS, even if an Internet connection is not the only way for the update to occur.

Vu et al. [55] presented the development and experimental evaluation of a Cyber-Hardware-in-the-Loop (Cyber-HIL) platform designed to test control operations in ship cyber physical systems under communication issues and cyber attacks, aiming to identify security vulnerabilities. By utilizing this platform, the ship network can be rigorously tested under real-world conditions, ensuring that potential weaknesses are identified and mitigated before they can be exploited in actual scenarios.

Furthermore, real-time anomaly detection systems utilizing machine learning, as demonstrated in [88], can provide effective risk mitigation for ship networks by identifying abnormal activities in ICS, such as tampering with navigation data. These systems can proactively detect and respond to cyber threats, helping to safeguard critical ship operations.

Several anomalies in an NMEA message, such as unexpected value, under-reporting, over-reporting, incorrect value, conformity issue, nonexistent value, and sudden unexpected change, can be detected by ad hoc software [53].

3.4.6. Other Mitigation Measures

Although the components underlying the operating system (e.g., MFD) commonly come without antivirus software, they could be useful in detecting malware [6]. The vulnerabilities of a component should be regularly scanned with vulnerability scanning software [36]. Hardware interfaces should be blocked to ensure security [38]. Default passwords should be changed to prevent unauthorized access [38]. Portable storage devices, including those used for ENC updates, should be kept under control [38]. Middleware, which may be required for various components, should be updated regularly, but caution should be taken as such updates could damage the component's functionality. It is recommended to obtain confirmation from the manufacturer of the component before proceeding with any updates [39]. Proposed defense solutions should be tested in different scenarios to ensure their effectiveness [111]. Performance tests for proposed encryption

solutions should also be carried out [46]. Actual ship and environmental (e.g., weather) data should be used instead of a mimic dataset to make the testing more accurate and representative [60].

4. Professional Community Perspective

4.1. Methodology

The professional community perspective was established through interviews with maritime professionals. We contacted 20 different ship operators to gather information about their cybersecurity practices. Among the ship operators we contacted, all of them had a cybersecurity plan that included a cyber risk assessment. However, many operators lacked effective cybersecurity practices beyond the cybersecurity requirements issued by the IMO [112]. Therefore, we interviewed 8 out of the 20 ship operators who had implemented practices beyond the cybersecurity regulations. Additionally, we interviewed two research fellows who had previous experience in the maritime industry and have written their doctoral theses on maritime cybersecurity. Both of them had a strong connection with professionals in the maritime industry and provided significant insights into industry practices. Consequently, as shown in Table 2, we conducted online interviews with a total of 10 individuals. The discussions focused on the cybersecurity awareness of personnel onboard, the technical and procedural measures implemented to mitigate cyber risks, and general observations and experiences regarding cybersecurity in the maritime sector.

Table 2. List of interviewees in the focus group.

#	Role & Organization	Competency	Reason for Interview
1	2nd Officer (dry cargo operator)	Oceangoing Watchkeeping Officer	Ship Cybersecurity Officer; Giving training onboard to seafarers about the cyber risks of ships.
2	Consultant (independent)	Oceangoing Chief Engineer	Maritime cybersecurity consultant; (Ex) Company Cybersecurity Officer; Developing cybersecurity plan, including risk assessment; Giving training onboard and at the office to seafarers about the cyber risks of ships.
3	Maritime Pilot (private port)	Oceangoing Master	Completed M.Sc. thesis on maritime cybersecurity.
4	DPA/CSO (dry cargo operator)	Oceangoing Master	Developing a cybersecurity plan, including risk assessment.
5	Technical Superintendent (tanker & container operator)	Oceangoing Chief Engineer	Experienced in safety risk assessments.
6	Training Superintendent (tanker operator)	Oceangoing Master	Giving training at the office to seafarers about the cyber risks of ships.
7	Marine Superintendent (tanker operator)	Oceangoing Chief Officer	Developing cybersecurity plan, including risk assessment.
8	Chief Officer (dry cargo operator)	Oceangoing Chief Officer	Ship Cybersecurity Officer; Giving training onboard to seafarers about the cyber risks of ships.
9	Research Fellow (university)	(Ex) Oceangoing Watchkeeping Officer	Ongoing Ph.D. thesis on maritime cybersecurity.
10	Research Fellow (university)	(Ex) Oceangoing Watchkeeping Officer	Ongoing Ph.D. thesis on maritime cybersecurity.

DPA: Designated Person Ashore. CSO: Company Security Officer.

A semi-systematic interview approach was employed to explore the perspectives of professionals within the maritime community. The interview began with three open-ended questions designed to elicit participants' general views. Based on their responses, additional follow-up questions were posed to gain deeper insights into the current state of cybersecurity within the industry. The initial guiding questions were as follows:

- How is cybersecurity awareness of the employed seafarers improved?

- What technical and procedural measures are implemented against cyber risks?
- What observations do you have regarding cybersecurity?

The following sections present our findings from the interviews with the maritime professionals. It covers technical and procedural mitigation measures implemented by shipping companies against cyber risks, as well as other observations made by our interviewees.

4.2. Cybersecurity Officer (CySO)

Ship Cybersecurity Officer (SCySO) and Company Cybersecurity Officer (CCySO) are the main cybersecurity roles that the maritime industry adopts. Designating SCySO and CCySO is not mandatory according to IMO requirements. We invited the interviewees to state the reasons for doing so. The reasoning provided is as follows:

- Recommendations of International Association of Classification Societies (IACS) member class societies;
- Better compliance with IMO and vetting requirements related to cybersecurity;
- Recommendation from another ship operator;
- Preparation for potential future IMO or vetting requirements.

Chief mates, second officers, or third officers are generally assigned as SCySOs. No ship operator in this study assigns IT staff as a CCySO. A DPA in the ship operator is typically nominated as the CCySO, who is supported by the in-house IT departments or third parties. We asked for the reasons for this decision, and the replies were similar. According to the office staff among interviewees, IT staff are not familiar with OT systems onboard ship. They are aware of the functions of a few bridge components, such as GPS, ECDIS, RADAR, and AIS, but are relatively unaware of the connections of such components. For instance, modern oily water separators (OWS) in the engine room are connected to GPS to store discharge position information as proof, even though it is not mandatory as per maritime regulations in force [113]. IT staff might not be aware of this connection and related regulations in the International Convention for the Prevention of Pollution from Ships (MARPOL). Vettings conducted in company offices (e.g., Tanker Management and Self-Assessment (TMSA)) are another reason for not assigning IT staff as CCySOs. IT staff are typically excluded from safety management systems (SMSs) and, therefore, are not subject to office vettings. During vettings, office staff are evaluated in terms of their familiarity with company procedures. IT staff are typically not familiar with company policies and procedures, and this could lead to a deficiency in familiarization. Therefore, due to the lack of OT knowledge, unawareness of maritime regulations, and unfamiliarity with the company SMSs, ship operators in this study do not assign IT staff as CCySOs.

4.3. Awareness and Training

To further improve cyber awareness within the company, many shipping companies have identified training as a core factor in preventing cyber threats, especially with vetting requirements in place [114]. Requirements regarding cybersecurity in safety familiarization training content after the seafarer's joining the vessel may be added. Further, posters published by recognized maritime organizations (e.g., International Association of Independent Tanker Owners (INTERTANKO)) regarding cybersecurity pave the way towards maritime cybersecurity training [115,116]. Training for cybersecurity can be delivered in person or through video training at the office of the ship operator, the office of manning agents, or onboard the ship. Those responsible for delivering in-person training include officers onboard, training staff, and SCySO or CCySO. Additionally, seafarers may receive training through distance learning platforms during their leave periods. Third-party providers or company staff may also deliver training to seafarers through seminars within the company.

Training may be provided once or on a recurring basis, e.g., yearly. Some companies may also administer exams to ensure that employed seafarers have adequate cyber awareness. If a seafarer fails the exam, the course is repeated. Maritime companies aim to train personnel for both safety and cybersecurity issues by conducting ship-shore combined drills. These drills aim to increase the awareness of seafarers and office staff, improve the accuracy of company procedures, and assess the condition of equipment. Third parties, such as flag states, class societies, and consultancy companies, may also attend the drills to observe real reactions in case of emergency situations. Any deficiencies detected during the drills are followed up and corrected by a given deadline. As a result, several ship operators have implemented various training policies to enhance the cybersecurity awareness of their seafarers.

4.4. Technical Measures

Ship operators consider different technical measures against cyber risks onboard ships. Several cybersecurity mitigation techniques are identified. Antivirus and firewall software are installed on computers of OT systems (e.g., ECDIS, RADAR, and MFD). A dedicated memory stick is used for ENC updates of ECDIS. The USB and ethernet (i.e., RJ45) ports are physically blocked to prevent unauthorized access, while in some cases, dedicated software is used to lock such ports. A temporary password is given from the office to unlock them for a short period. Computer cases of OT systems are locked as well, and Bluetooth connections might be disabled. In-house IT staff or a third-party cybersecurity company provides support for cybersecurity onboard. Software and operating systems of marine systems are typically updated by third parties if the ship operator requests.

It is a known fact that vessels off the coast of Russia are exposed to GPS attacks [117]. According to an interviewee, GLONASS is not affected by these attacks. Accordingly, ship operators have started equipping their vessels with GLONASS receivers. The track control system (TCS) in some brands can be controlled through an ECDIS. However, ship operators do not activate this feature due to the potential risk of GPS spoofing attacks.

Visitors onboard, such as surveyors, may request to print out various documents, including draft survey reports. In some shipping companies, printing onboard is strictly prohibited for visitors. Instead, visitors send the report to the vessel via e-mail to be printed out. Some vessels, however, have a dedicated computer attached to a dedicated printer that is only used by visitors to take a printout.

4.5. Procedural Measures

Ship operators establish plans, policies, and risk assessments for cybersecurity. These plans include definitions of terms such as virus, firewall, and risk, as well as roles and responsibilities, stages of a cyber attack, potential risks such as e-mail threats and social engineering, protection measures, contingency plans, response plans, and cyber incident investigation procedures. Such documents are typically issued by a DPA and the Health, Safety, Environment and Quality (HSEQ) manager. Based on the results of the interviews, it was found that some shipping companies purchase cybersecurity plans from maritime consulting firms, while others admit to copying plans from other shipping companies.

Shipping companies typically use the traditional formula of $Risk = Severity \times Likelihood$ for cyber risk assessment. Among our interviewees, tanker operators assess cyber risks separately for assets, people, environment, and reputation. However, the interviews revealed that the severity and likelihood aspects of cyber risks were not systematically selected, resulting in insufficient risk assessment.

4.6. Other Observations

Cybersecurity requirements are verified in Safety Management Certificate (SMC) audit, Ship Inspection Report (SIRE) program, Chemical Distribution Institute (CDI), and RightShip vettings onboard. Such requirements are analyzed in [114]. Cybersecurity requirements in SIRE were improved on 2 September 2024 with SIRE 2.0 [118,119]. Policy, procedures, training, and risk assessment are currently required for vettings and audits. Maritime companies are struggling to meet such requirements.

Vetting inspectors may request to print out the vetting report via a memory stick as a way to test the awareness of seafarers and office staff in implementing company procedures. Seafarers are usually familiar with such tricky requests, but some office staff may not be. If an office employee accepts the memory stick to print out the report, it is noted as a deficiency in the implementation of company procedures.

According to an interviewee, the top management of a shipping company decided to assess the cyber resilience capability of their vessels after the Maersk cyber incident, which resulted in a loss of USD 300 million [120]. The in-house cybersecurity department suggested obtaining services from a third party with experience in cyber risks onboard. The top management decided to hire an IACS member class society for a cybersecurity assessment onboard ship. Although the company received a large report concerning the cyber risks onboard, the report did not satisfy the company management. The report included common risks and suggestions, such as an active wireless fidelity (Wi-Fi) connection of a printer and missing hard disk disposal procedures. Although the service was expensive, the noted observations were mostly regarding IT vulnerabilities onboard, which could be informed by a lower-cost cybersecurity consultant or an in-house cybersecurity department. The expectation of company managers was to receive specific recommendations concerning the threats and vulnerabilities in the OT infrastructure onboard.

Third parties and company superintendents may observe various cybersecurity deficiencies during their inspections. For instance, extension cables for USB ports are sometimes plugged into IT and OT components to facilitate operations onboard. However, USB locks are plugged into such extension cables instead of USB ports directly on the component. This incorrect implementation increases the risk of unauthorized access. In addition, default passwords are often used for OT systems due to concerns about password loss, and these passwords are sometimes posted near the component. This mistake makes them easily accessible to unauthorized personnel. User passwords for ship management software are also typically shared among the personnel, which can compromise the security of the system. While OT components may be protected by leveraging component-specific protection mechanisms and boxes, the keys for such boxes are usually stored by the master. However, in some vessels, the keys are kept in a place easily accessible by anyone. This increases the risk of unauthorized access to these systems. Another issue is that when GPS signals disappear, the ship crew rarely informs the company office. This is often because of temporary losses caused by environmental factors, such as mountainous terrain, adverse weather, or ionospheric disturbances. The GPS signal typically returns within a couple of hours. However, during this period, the vessel may in fact be under a GPS jamming attack without realizing it.

5. Discussion

5.1. Research Community Perspective

Although numerous articles discuss the potential cyber risks faced by the maritime industry, studies based on experimental results remain limited. There seems to be a stronger focus on the AIS and GNSS systems compared to other components of the INS. However,

in recent years, research on the INS network and RADAR systems has also been increasing, reflecting a broader interest in securing these critical elements of maritime operations.

By employing empirical methods, cyber vulnerabilities have been identified in the AIS, ECDIS, GNSS, RADAR, MFD, and INS networks. However, an INS is not limited to only these components. An INS consists of a total of 25 different components, such as an echo sounder, gyro compass, HCS, speed and distance measurement equipment (SDME), and TCS [3]. Such components are also crucial for the safe navigation of a ship. However, these contemporary components are also computerized and susceptible to cyber attacks. An article on cyber risk assessment of the INS revealed that 22 out of the 25 of these components are subject to cyber risks [121], including loss of availability, spoof reporting message, and data destruction. This theoretical study unveils the need for performing experimental cybersecurity studies in controlled environments to verify potential threats and vulnerabilities of the remaining INS components.

GNSS attacks not only affect ships in the impact range of the attack but also GNSS receivers in other devices and transportation vehicles. The impact of GNSS jamming attacks varies with the GNSS receiver, the force of the jammer, and the distance between the victim receiver and the jammer [40]. Most probably, the same criteria affect the success of GNSS spoofing attacks of malicious actors.

Leite Junior et al. [33] reported that malware can be triggered in an ECDIS via the AIS. According to IMO requirements, RADAR should be able to receive data from AIS [122]. An MFD, other than ECDIS and RADAR, is typically connected to AIS. Therefore, malware hosted in an MFD and RADAR might be triggered by the AIS. A NAVigational TEleX (NAVTEX) is a potential component in the context of an INS for receiving messages and is typically connected to an ECDIS and MFD. Thus, theoretically, malware hosted in an ECDIS and MFD might also be triggered through NAVTEX.

A significant gap in the literature is available regarding cybersecurity research conducted on a live vessel. While much research is conducted in laboratory environments, conducting research on live vessels could improve research quality. However, technical studies for INS should be performed while the vessel is moored to avoid compromising its seaworthiness. Longer-duration periods at the harbor or dock, such as intermediate or special surveys, should be preferred when possible to minimize the risk of financial loss to the shipping company.

Particularly for AIS (Section 3.4.1) and GNSS (Section 3.4.2), various cyber risk mitigation measures are proposed based on encryption. However, some significant barriers exist to implementing them in the real world. Because of the operational principles of these systems, existing onboard receivers can not decrypt such encrypted signals. Therefore, these receivers should be globally replaced with new ones that are capable of doing so. Moreover, implementing certain encryption methods requires the establishment of centralized infrastructures that serve secure communication between transmitters and receivers. On the other hand, IMO regulations may need to be revised. The INS and its components have technical standards identified by the IMO [3]. Some of the proposed mitigation measures may conflict with these existing requirements. Moreover, the articles do not discuss whether the proposed measures, if implemented, would continue to comply with the performance standards mandated by the IMO. These regulatory and technical matters represent a major obstacle to translating proposed solutions into practice.

5.2. Professional Community Perspective

Given that each vessel does not have continuous broadband internet access, such as Very Small Aperture Terminal (VSAT), the operating systems and antivirus software are not updated regularly. They are typically updated via mobile internet while the ship is at shore.

Therefore, OT components running on operating systems, such as ECDIS, RADAR, and MFD, are vulnerable to cyber attacks. However, the operating systems of these components are not regularly upgraded or updated by all ship operators due to the risk of system crashes. As a result, components using outdated operating systems such as Windows XP are still available onboard ships. These old operating systems are no longer supported by vendors for security updates and patches, making them more vulnerable to cyber attacks.

Training is provided either by office staff or an officer onboard, but the quality and level of knowledge are questionable. We asked about additional training for CCySO and SCySO. Even though both of them give the training to the ship crew onboard or in the office, SCySOs do not take any additional training other than the ordinary training given to the ship crew. CCySO might take additional training and seminar. We discussed the quality of training. According to our interviewees, the training given covers only ordinary cybersecurity topics, such as phishing attacks and malware infections. Maritime-specific risks are not mentioned in training, such as GNSS jamming or AIS ship spoofing. SCySOs do not typically have any responsibilities other than cybersecurity training.

IMO and vetting requirements force ship operators to issue a cybersecurity plan. We examined the cybersecurity plans of six ship operators and noticed that five of these were developed by copying information from [123], which is an IMO-recommended guideline. Given that plans are typically copied from another company or guidelines, the plans include provisions incompatible with the components onboard ship. Even though the plans include protection measures, they are not implemented efficiently. Risk assessment is also an IMO requirement, but interviewees admitted that the severity and likelihood dimensions of the traditional risk assessment formula for cyber risks were randomly selected, and their risk assessments were not effective.

IACS has issued unified requirements for cybersecurity, known as UR E26 [124] and UR E27 [125], which came into effect on 1 July 2024. These requirements impact newly built ships and must be uniformly implemented by IACS societies for ships contracted for construction on or after 1 July 2024. For other ships, they may serve as non-mandatory guidance. The "contracted for construction" date refers to the signing of the shipbuilding contract between the shipowner and the builder. During our discussions, we realized that, except for research fellows, interviewees were unaware of these requirements, which may be due to the lack of new shipbuilding projects.

Several class societies, such as American Bureau of Shipping (ABS) [126], Bureau Veritas (BV) [127], Nippon Kaiji Kyōkai (known by its brand name ClassNK) [128], DNV [129], Korean Register (KR) [130], and Lloyd's Register (LR) [131] offer cybersecurity class notation to shipping companies. The interviewees are informed about these notations; however, the companies they work for do not plan to obtain the notation. We asked them for the reason behind their decision. The first reason is that cybersecurity notation is not mandatory for ship operators. Moreover, obtaining the notation requires additional costs and effort. Additionally, it does not offer a financial benefit to shipping companies. For example, the International Organization for Standardization (ISO) 14001 Environmental Management System [132] is not mandatory for shipping companies according to international requirements. However, some shipping companies may choose to obtain it to receive discounts in several ports.

Although ship operators may use tools or software mechanisms to lock USB ports, RJ-45 ports are generally not locked. Our interviewees revealed that password management is a significant problem in the maritime industry. The default passwords of OT components are commonly used, a practice that makes them vulnerable to cyber attacks.

In future works, researchers could investigate a potential correlation between the size of ship operators and their cyber readiness. To this end, researchers should interview

a broader range of company representatives by considering different operator sizes. At the initial stage of the study, the definition of the "size" should be well defined. All potential definitions should be evaluated, such as the number of vessels in the fleet, the total deadweight tonnage of the fleet, or the economic value of the fleet. Ideally, as much as possible, all variables (except for size) between ship operators in the study should be the same or similar. Tankers are subject to vetting programs, including cybersecurity requirements. For this reason, differences between the ship types operated may even lead to inaccurate research findings.

5.3. Comparing and Merging Perspectives

The literature identifies several technical measures that can be taken to improve the cybersecurity of ships. However, ship operators may not be able to implement such precautions because of various reasons, including the unavailability of end products in the market, the need for third-party infrastructure, or the requirement for changing performance standards.

Ship operators also face the challenge of outdated software and operating systems on their OT components. They typically avoid updating them because of the risk of system crashes. A case in the literature supports the concerns of ship operators, where a navigation system was lost because an update was incompatible with an outdated operating system in the OT component [123]. A technical representative of a manufacturer updated navigation software in the INS. During the voyage, nearly all navigation capacity was lost. The ship sailed with only RADAR for surveillance for two days. After arrival at the port, it was understood that the update was incapable of running with an outdated operating system in the OT component. The costs of the delays were high. Therefore, ship operators should request confirmation from the manufacturers about the compatibility of the underlying operating system with the new version of the software. However, manufacturers may not be aware of potential version conflicts, as seen in this case. The occurred incident, papers in the literature, and our interviewees revealed that outdated operating systems for the OT components are in operation onboard ships.

The most common aerial positioning system for commercial vessels is GNSS, which includes GPS, GLONASS, Galileo, and BeiDou. GNSS provides space-based position, velocity, and time information [133]. However, as GNSS receivers require firmware to operate, they may be vulnerable to malware. Therefore, to verify the accuracy of timing and positioning information received from GNSS, a redundant GNSS receiver can be used. An AIS also includes an internal GNSS, which can be used for position verification. However, in case of a GNSS spoofing attack, redundant GNSS receivers and AIS may provide the same forged information. To verify the information received, another GNSS provider can be used. For example, position and time information received from GPS can be verified by GLONASS. Ship operators started to equip their vessels with GLONASS receivers during the Russia and Ukraine war in 2022, as GLONASS receivers can still provide accurate position information in the Black Sea when GPS cannot, allegedly due to Russia targeting GPS [134]. Some GNSS receivers and antennas support multi-GNSS, which combines GPS and GLONASS. Using multi-GNSS is suggested in the literature as a mitigation measure against GNSS jamming attacks [40], and switching between providers can help verify information received. Both research and professional perspectives support the use of multi-GNSS against GNSS vulnerabilities.

Terrestrial systems can also be used for positioning and timing verification. eLoran is one of the potential solutions [135]. It is currently being operated, developed, and extended by countries such as China, Russia, and South Korea [136]. Ships equipped with an eLoran receiver can obtain position information while in water areas where eLoran is available.

Another potential component for position verification is the Inertial Navigation System [96,97]. It was mentioned in an interview that ship operators in the U.K. have started equipping their vessels with an Inertial Navigation System for position verification because of GNSS vulnerabilities. The industry is verifying the legitimacy of such a suggestion in the literature.

The DGNSS signal is used to improve the accuracy of position information by sending error-corrective messages to a GNSS receiver [99]. However, it is vulnerable to jamming and spoofing attacks. GNSS receivers operate in two essential modes, such as auto (e.g., GPS+DGPS) and manual (e.g., GPS/DGPS). According to an interviewee, ship operators in the U.K. started switching the operation modes of GPS receivers from auto to manual and disabled receiving DGPS signals when GPS receivers were giving incorrect position information. After taking this action, GPS receivers started to obtain position information only from GPS satellites and gave accurate readings. Although we could not find any research to support this potential mitigation measure, it may theoretically work in the case of DGPS attacks.

We did not come across any research that explains how navigators can compare various types of information obtained from different components. RADAR and ECDIS provide geographical information (e.g., shorelines) using different working principles. By comparing the information provided by each system, navigators can verify the accuracy of the information. Similarly, gyro compasses and magnetic compasses provide heading information using different principles. Almost all GNSS receivers provide heading information, and comparing the information provided by each component can help verify the accuracy of the heading. A GNSS also provides speed over ground (SOG) information [122]. The speed information of the vessel provided by GNSS can be compared to SDME. Furthermore, RADAR and AIS can detect vessels near the ship using different working principles, and the targets can be verified by comparing data from these systems. This method is also useful for detecting AIS ship spoofing attacks (i.e., creating fake vessels on AIS).

The Guidelines on Cyber Security Onboard Ships [123], which is one of the recommended materials by the IMO [137], provides an example of mapping roles, responsibilities, and tasks in a matrix. According to this matrix, the ship IT manager is responsible for conducting the cyber risk assessment for OT and IT systems onboard ships. As discussed in Section 4.2, ship operators typically assign the CCySO role to DPAs, and they conduct such risk assessments in practice. Even though this example matrix does not include a task for the DPA role, the following sections of the guideline contain recommendations for the DPA role. DPAs typically do not have IT or cybersecurity expertise. In case of a cyber attack targeting ship systems, they may face challenges in responding effectively. Therefore, support for DPAs is recommended by the guideline either internally or through external means, such as an external Cyber Emergency Response Team (CERT). Maritime cybersecurity is a multidisciplinary field combining maritime, IT, and cybersecurity expertise. That is why we argue that a cross-disciplinary effort is required to effectively prevent cyber incidents onboard ships.

More comprehensive and multidimensional studies can be conducted by considering both findings in the literature and practices in the maritime industry. Therefore, the complex cybersecurity issues of the INS and its components can be addressed. To this end, several systemic tools can be employed. First, systems thinking [138] provides a holistic approach to analyzing both technical and human factors together. For instance, several components, such as ECDIS, depend on information received from the GNSS receiver [3]. In case of a GNSS spoofing attack, the ECDIS also displays incorrect positioning data. This may lead to inaccurate or delayed decisions by the navigator. Second, scenario planning [139] can be utilized to simulate realistic cyber incidents, such as AIS spoofing, to

examine the effectiveness of cyber response plans, including vessel and office staff behavior, policies, procedures, and technical capabilities. Furthermore, soft systems methodology (SSM) [140] is well suited for identifying communication gaps between office staff and ship crew. Lastly, cross-impact analysis [141] can support the prioritization of mitigation measures by assessing the interrelations among cyber vulnerabilities, IMO regulations, and organizational constraints.

While conducting such comprehensive and multidimensional studies, it is essential to ensure precise definitions and clear system boundaries. Currently, there is no standardized architectural model for the INS provided by the IMO [3]. Therefore, it is required to define an INS architecture including components, sub-components (i.e., hardware and software), data flows, connections, and dependencies. A similar challenge applies to the human element. Organizational structures, roles, and responsibilities can vary significantly onboard ships and at the office [142]. For this reason, researchers should carefully consider these technical and organizational variables during the study design phase. Thus, studies can produce more accurate and practically applicable findings to strengthen the cybersecurity of the INS.

6. Conclusions

Contemporary ships have a significant role in global trade. However, computerized systems onboard ships, such as the INS, lead to the raising of cybersecurity concerns. In this article, we looked at these risks from both scientific and professional perspectives. This article provides a comprehensive analysis of the potential cyber risks and mitigation measures of the INS by performing the SLR methodology. Moreover, this study investigates cybersecurity practices of the maritime industry by interviewing maritime professionals. With the support of this combined approach, various recommendations in scientific papers were verified by industry practices. Moreover, several industry practices are included in the literature. Therefore, this study contributes to closing the gap between the literature and industry practices.

This study also supports various maritime stakeholders. It helps researchers recognize industry practices that have not yet been scientifically validated by offering opportunities for future studies to evaluate their effectiveness. Likewise, it enables manufacturers to assess the practicality of proposed scientific solutions and potentially convert them into viable products. The maritime industry may also use the insights to improve cybersecurity plans within their SMS and equip vessels with recommended technical measures. Furthermore, member states can consider the findings to submit cybersecurity proposals to the IMO aimed at strengthening global maritime cybersecurity efforts.

Cybersecurity is not only substantial for protecting ship systems but also significantly supports sustainable development. Maritime cybersecurity efforts impact the environment and society. That is why they are linked to specific Sustainable Development Goals (SDGs) [143]. For instance, technical and operational measures for improving the cybersecurity of ships and maritime infrastructures directly support *SDG 9: Industry, Innovation and Infrastructure*. Training initiatives for enhancing cybersecurity awareness of maritime professionals align with *SDG 4: Quality Education*. The INS system directly supports the safe navigation of ships. Given that it assists navigators in collision avoidance, cybersecurity of the INS is relevant to *SDG 14: Life Below Water*.

Coordinated endeavors from all stakeholders are required to achieve these objectives and enhance maritime cyber resilience. As a global regulatory body, the IMO plays a critical function in the maritime sector. Consequently, the cyber resilience of the maritime sector can be substantially improved through the implementation of comprehensive cybersecurity proposals submitted by member states. Nevertheless, the adaptation of such proposals

is frequently delayed because of the decision-making process in the IMO. To illustrate, the Republic of Korea submitted a proposal in 2021 to include cybersecurity training in the Standards of Training Certification and Watchkeeping (STCW) Convention [144]. Nevertheless, the IMO has not yet issued this proposal as a regulation.

As we discussed in our study before [142], formal courses for maritime cybersecurity are limited in the world. Maritime education and training (MET) institutions bear an essential responsibility to prepare cadets against cyber threats, as they will obtain operational responsibility onboard ships after graduation. However, to the best of our knowledge, only the Estonian Maritime Academy of the Tallinn University of Technology offers a maritime cybersecurity course to their cadets at the BSc level [145]. Institutions should urgently incorporate maritime cybersecurity courses into their educational curricula.

Communication between the scientists and professionals should be strengthened. According to our observations, the interaction between these two communities is quite weak. Scientists often share their findings with other scientists. The professionals obtain recommendations from the industry, such as classification societies or consultancy companies. As a result, the opportunity for knowledge transfer between communities is missed. To bridge this gap, MET institutes and maritime associations should organize events to bring researchers and professionals together. Such events can also be organized in hybrid or fully online formats because of the limited number of scientists in the maritime cybersecurity field.

Currently, several initiatives list maritime cyber incidents based on open sources [8,146]. However, many incidents are not publicly disclosed. Therefore, a collaborative threat intelligence database for sharing the details of incidents and potential mitigation measures could be established by the renowned maritime stakeholders, such as marine insurance companies, classification societies, and flag states. However, it is essential to identify access criteria for this database. Otherwise, the database could be exploited by threat actors for malicious purposes.

The gap should be addressed between scientific innovation and commercial application. As aforementioned, scientists propose technological solutions to prevent ship systems from cyber attacks. However, these solutions rarely evolve into a cybersecurity product. Cybersecurity companies are typically hesitant to invest in product development based on these solutions because of concerns about insufficient market demand. These products could also be deployed on warships where cybersecurity is critically important. By funding the product development process, states can support cybersecurity companies. Therefore, they can develop such products without financial concerns and then strive to sell the products to ship operators for merchant ships.

In conclusion, this study contributes to addressing the gap between scientific research and industry practices by comparing both perspectives associated with the INS. Nevertheless, several critical questions remain unanswered. Future research could investigate whether there is a correlation between the economic value of shipowners' fleets and their approach to cybersecurity. Additionally, a comprehensive study is required to identify cyber risks and mitigation measures for systems in the engine room. Addressing these questions would improve our understanding of the maritime cyber landscape.

Author Contributions: A.O. conducted the literature review. A.O. conducted interviews. A.O. performed formal analysis and investigation. A.O. created visualisations. A.O., G.K., and S.K. wrote the original draft. V.G. and S.K. provided supervision. V.G. reviewed and made modifications. V.G. and S.K. secured funding acquisition. All authors have read and agreed to the published version of the manuscript.

Funding: This paper received funding from the Research Council of Norway through the Maritime Cyber Resilience (MarCy, project number 295077) project and the SFI Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS, project number 310105). The content reflects only the authors' views, and neither the Research Council of Norway nor the project partners are responsible for any use that may be made of the information it contains.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author(s).

Acknowledgments: We would like to express our sincere gratitude to experts for their comments towards improving our study.

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

Appendix A

In Table A1, the details of reviewed publications are given with title, publication, year, and type. In the column of "Type", C denotes conference papers. J refers to journal articles, and B depicts a part of a book.

Table A1. The details of reviewed publications.

ID	Ref	Year	Publisher	Type	Component
1	[4]	2014	ACM	C	AIS
2	[48]	2015	IEEE	J	GNSS (GPS)
3	[49]	2016	DGLR	C	GNSS
4	[5]	2017	ION	J	GNSS (GPS)
5	[78]	2017	HRČAK	J	AIS
6	[40]	2017	Cambridge	J	GNSS
7	[77]	2017	ACM	C	AIS
8	[94]	2017	IEEE	C	GNSS (GPS)
9	[81]	2018	TransNav	J	GNSS
10	[6]	2018	Sjøkrigsskolen	J	INS (MFD)
11	[95]	2019	TransNav	J	GNSS
12	[147]	2019	Springer Link	J	GNSS
13	[91]	2019	Springer Link	J	AIS
14	[43]	2019	TransNav	J	ECDIS
15	[52]	2019	Springer Link	J	ECDIS
16	[35]	2019	Cambridge	J	ECDIS
17	[39]	2019	HRČAK	J	ECDIS
18	[38]	2019	MDPI	J	INS (MFD)
19	[109]	2019	IEEE	C	Network
20	[111]	2019	ScienceDirect	J	Network
21	[46]	2020	IEEE	C	AIS
22	[75]	2020	TransNav	J	AIS
23	[67]	2020	ScienceDirect	J	AIS
24	[60]	2020	IEEE	C	AIS
25	[90]	2020	TransNav	J	AIS
26	[45]	2020	ACM	C	GNSS
27	[37]	2020	Springer Link	J	ECDIS
28	[36]	2020	Cambridge	J	RADAR
29	[41]	2021	IEEE	C	GNSS (GPS)
30	[61]	2021	TransNav	J	Network
31	[44]	2021	Az-Buki	J	Network
32	[87]	2021	IAMU	C	AIS
33	[110]	2021	IEEE	C	Network
34	[33]	2021	MDPI	J	ECDIS, RADAR
35	[92]	2021	Cambridge	J	AIS

Table A1. *Cont.*

ID	Ref	Year	Publisher	Type	Component
36	[53]	2022	MDPI	J	Network
37	[70]	2022	IEEE	C	Network
38	[96]	2022	IEEE	J	GNSS
39	[66]	2022	IEEE	C	AIS
40	[42]	2022	Springer Link	C	AIS
41	[65]	2022	MDPI	J	AIS
42	[62]	2022	IEEE	C	RADAR
43	[101]	2022	MDPI	J	GNSS
44	[69]	2023	IEEE	J	RADAR
45	[58]	2023	IEEE	C	RADAR
46	[98]	2023	MDPI	J	GNSS
47	[102]	2023	IEEE	C	GNSS
48	[100]	2024	Springer Link	B	GNSS
49	[55]	2024	IEEE	J	Network
50	[88]	2024	IEEE	C	Network
51	[51]	2024	IEEE	C	GNSS
52	[89]	2024	IEEE	C	MFD
53	[103]	2024	IEEE	C	RADAR
54	[76]	2024	IEEE	C	AIS
55	[79]	2024	Springer	B	ECDIS
56	[104]	2024	Springer	C	RADAR
57	[93]	2024	AIRCC	C	AIS

References

1. UNCTAD. *Review of Maritime Transport*; UNCTAD: Geneva, Switzerland, 2021.
2. IMO. *Resolution MSC.252(83) Adoption of the Revised Performance Standards for Integrated Navigation Systems (INS), Introduction, Contents, Module A-B*; IMO: London, UK, 2018.
3. 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]
4. Balduzzi, M.; Pasta, A.; Wilhoit, K. A security evaluation of AIS Automated Identification System. In Proceedings of the ACSAC'14: Proceedings of the 30th Annual Computer Security Applications Conference, New Orleans, LA, USA, 8–12 December 2014; Payne, C.N., Hahn, A., Butler, K., Sherr, M., Eds.; Association for Computing Machinery: New York, NY, USA, 2014; pp. 436–445. [CrossRef]
5. Bhatti, J.; Humphreys, T.E. Hostile control of ships via false GPS signals: Demonstration and detection. *J. Inst. Navig.* **2017**, *64*, 51–66. [CrossRef]
6. Lund, M.S.; Hareide, O.S.; Jøsok, Ø. An attack on an Integrated Navigation System. *Necesse* **2018**, *3*, 149–163. [CrossRef]
7. M-CAD. Info. Available online: https://maritimecybersecurity.nl/info (accessed on 21 April 2025).
8. France Cyber Maritime. ADMIRAL Dataset. 2025. Available online: https://www.m-cert.fr/admiral/index.html (accessed on 21 April 2025).
9. France Cyber Maritime. About. Available online: https://www.france-cyber-maritime.eu/en/about/ (accessed on 21 April 2025).
10. France Cyber Maritime. Maritime Cybersecurity Statistics—Global Scale. Available online: https://www.m-cert.fr/admiral/statistics.html (accessed on 21 April 2025).
11. France Cyber Maritime. Detailed Maritime Cybersecurity Statistics by Threat. Available online: https://www.m-cert.fr/admiral/threats.html (accessed on 21 April 2025).
12. Blake, T. Hackers Took 'Full Control' of Container Ship's Navigation Systems for 10 Hours-IHS Fairplay. 2017. Available online: https://rntfnd.org/2017/11/25/hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-ihs-fairplay/ (accessed on 21 April 2025).
13. 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]
14. Androjna, A.; Brcko, T.; Pavic, I.; Greidanus, H. Assessing cyber challenges of maritime navigation. *J. Mar. Sci. Eng.* **2020**, *8*, 776. [CrossRef]

15. Paganini, P. A Sophisticated Cyberattack Hit the International Maritime Organization (IMO). 2020. Available online: https://securityaffairs.com/109154/hacking/international-maritime-organization-imo-cyberattack.html (accessed on 21 April 2025).
16. Bateman, T. HMS Defender: AIS Spoofing Is Opening up a New Front in the War on Reality. 2021. Available online: https://www.euronews.com/next/2021/06/28/hms-defender-ais-spoofing-is-opening-up-a-new-front-in-the-war-on-reality (accessed on 21 April 2025).
17. Smith, A. Anonymous Trolls Vladimir Putin by Renaming His Yacht 'FCKPTN' and Sending It to 'Hell' by Hacking Maritime Data. 2022. Available online: https://www.independent.co.uk/tech/anonymous-vladimir-putin-yacht-fckptn-b2024780.html (accessed on 21 April 2025).
18. Oruc, A. Second Cyber Incident at IMO: Data Leakage. 2024. Available online: https://cyberonboard.com/second-cyber-incident-at-imo-data-leakage/ (accessed on 21 April 2025).
19. Kessler, G.C.; Craiger, J.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. [CrossRef]
20. ProWritingAid. Features. Available online: https://prowritingaid.com/features (accessed on 21 April 2025).
21. Grammarly. Our Features. Available online: https://www.grammarly.com/features (accessed on 21 April 2025).
22. 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]
23. 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]
24. 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]
25. 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. [CrossRef]
26. Dimakopoulou, A.; Rantos, K. Comprehensive analysis of maritime cybersecurity landscape based on the NIST CSF v2.0. *J. Mar. Sci. Eng.* **2024**, *12*, 919. [CrossRef]
27. DNV. Maritime Cyber Priority 2024/25. Available online: https://www.dnv.com/cyber/insights/publications/maritime-cyber-priority-2024/ (accessed on 21 April 2025).
28. M-CERT. Maritime Cyber Threat Overview 2023. Available online: https://www.france-cyber-maritime.eu/wp-content/uploads/2024/11/Rapport_menace_2023_NUMERIQUE_BD.pdf (accessed on 21 April 2025).
29. NORMA Cyber. Annual Threat Assessment 2025. Available online: https://www.normacyber.no/news/annual-threat-assessment-2024-46a4p (accessed on 21 April 2025).
30. Dresch, A.; Lacerda, D.P.; Antunes, J.A.V. Systematic Literature Review. In *Design Science Research*; Dresch, A., Lacerda, D.P., Antunes, J.A.V., Jr., Eds.; Springer International Publishing: Cham, Switzerland, 2015; pp. 129–158. [CrossRef]
31. Okoli, C.; Schabram, K. A Guide to Conducting a Systematic Literature Review of Information Systems Research. 2015. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1954824 (accessed on 25. May 2025). [CrossRef]
32. Okoli, C. A guide to conducting a standalone systematic literature review. *Commun. Assoc. Inf. Syst.* **2015**, *37*. [CrossRef]
33. 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]
34. Lumivero. Citavi Tour: Organize. Available online: https://lumivero.com/products/citavi/citavi-product-tour/ (accessed on 21 April 2025).
35. Svilicic, B.; Kamahara, J.; Rooks, M.; Yano, Y. Maritime cyber risk management: An experimental ship assessment. *J. Navig.* **2019**, *72*, 1108–1120. [CrossRef]
36. Svilicic, B.; Rudan, I.; Frančić, V.; Mohović, D. Towards a cyber secure shipboard radar. *J. Navig.* **2020**, *73*, 547–558. [CrossRef]
37. Svilicic, B.; Kristić, M.; Žuškin, S.; Brčić, D. Paperless ship navigation: Cyber security weaknesses. *J. Transp. Secur.* **2020**, *13*, 203–214. [CrossRef]
38. 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]
39. Svilicic, B.; Rudan, I.; Frančić, V.; Doričić, M. Shipboard ECDIS cyber security: Third-party component threats. *Sci. J. Marit. Res.* **2019**, *33*, 176–180. [CrossRef]
40. Glomsvoll, O.; Bonenberg, L.K. GNSS jamming resilience for close to shore navigation in the Northern Sea. *J. Navig.* **2017**, *70*, 33–48. [CrossRef]
41. Boudehenn, C.; Jacq, O.; Lannuzel, M.; Cexus, J.C.; Boudraa, A. Navigation anomaly detection: An added value for Maritime Cyber Situational Awareness. In Proceedings of the 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, Ireland, 14–18 June 2021; pp. 1–4. [CrossRef]

42. Amro, A.; Gkioulos, V. From Click to sink: Utilizing AIS for Command and Control in maritime cyber attacks. In *Proceedings of the Computer Security—ESORICS 2022*; Atluri, V., Di Pietro, R., Jensen, C.D., Meng, W., Eds.; Springer: Cham, Switzerland, 2022; pp. 535–553.
43. Svilicic, B.; Brčic, D.; ŽuŁkin, S.; Kalebic, D. Raising awareness on cyber security of ECDIS. *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2019**, *13*, 231–236. [CrossRef]
44. Stoynov, S.; Nikolov, B. Approach to ship's IT and OT systems cybersecurity improvement. *Pedagogika-Pedagogy* **2021**, *93*, 185–196. [CrossRef]
45. Oligeri, G.; Sciancalepore, S.; Di Pietro, R. GNSS spoofing detection via opportunistic IRIDIUM signals. In Proceedings of the WiSec'20: Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Linz, Austria, 8–10 July 2020; Mayrhofer, R., Roland, M., Eds.; Association for Computing Machinery: New York, NY, USA, 2020; pp. 42–52. [CrossRef]
46. Aziz, A.; Tedeschi, P.; Sciancalepore, S.; Di Pietro, R. SecureAIS—Securing pairwise vessels communications. In Proceedings of the 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 29 June 2020–1 July 2020; pp. 1–9. [CrossRef]
47. ADI. ADALM-PLUTO Software-Defined Radio Active Learning Module. Available online: https://www.analog.com/en/design-center/evaluation-hardware-and-software/evaluation-boards-kits/adalm-pluto.html#eb-overview (accessed on 21 April 2025).
48. Fan, Y.; Zhang, Z.; Trinkle, M.; Dimitrovski, A.D.; Song, J.B.; Li, H. A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids. *IEEE Trans. Smart Grid* **2015**, *6*, 2659–2668. [CrossRef]
49. Iliopoulos, A.; Fohlmeister, F.; Appel, M.; Pérez Marcos, E.; Sgammini, M.; Caizzone, S.; Cuntz, M.; Antreich, F. Testing of a multi-antenna GNSS receiver in DLR's maritime jamming testbed. In Proceedings of the Deutscher Luft- und Raumfahrtkongress, DGLR, Braunschweig, Germany, 13–15 September 2016.
50. Tenable. Nessus Professional. Available online: https://www.tenable.com/products/nessus/nessus-professional (accessed on 21 April 2025).
51. Chinnarong, T.; Pomsathit, A.; Yongsiriwit, K. Analysis of cybersecurity vulnerabilities in maritime GNSS systems. In Proceedings of the 2024 8th International Conference on Information Technology (InCIT), Chonburi, Thailand, 14–15 November 2024; pp. 325–330. [CrossRef]
52. Svilicic, B.; Kamahara, J.; Celic, J.; Bolmsten, J. Assessing ship cyber risks: A framework and case study of ECDIS security. *WMU J. Marit. Aff.* **2019**, *18*, 509–520. [CrossRef]
53. Amro, A.; Oruc, A.; Gkioulos, V.; Katsikas, S. Navigation data anomaly analysis and detection. *Information* **2022**, *13*, 104. [CrossRef]
54. Kali. hping3. Available online: https://www.kali.org/tools/hping3/ (accessed on 21 April 2025).
55. Vu, L.; Nguyen, T.L.; Abdelrahman, M.S.; Vu, T.; Mohammed, O.A. A Cyber-HIL for investigating control systems in ship cyber physical systems under communication issues and cyber attacks. *IEEE Trans. Ind. Appl.* **2024**, *60*, 2142–2152. [CrossRef]
56. Scapy. About Scapy. Available online: https://scapy.readthedocs.io/en/latest/introduction.html#about-scapy (accessed on 21 April 2025).
57. Fedora. Fedora Linux. Available online: https://fedoraproject.org/ (accessed on 21 April 2025).
58. Longo, G.; Merlo, A.; Armando, A.; Russo, E. Electronic Attacks as a Cyber False Flag against Maritime Radars Systems. In Proceedings of the 2023 IEEE 48th Conference on Local Computer Networks (LCN), Daytona Beach, FL, USA, 2–5 October 2023; pp. 1–6. [CrossRef]
59. Trend Micro. Trend Micro Safe Lock. Available online: https://docs.trendmicro.com/all/ent/tmsl/v2.0_SP1/en-us/_tmsl_server_olh_2.0sp1/about_tmsl.html (accessed on 21 April 2025).
60. Jakovlev, S.; Daranda, A.; Voznak, M.; Lektauers, A.; Eglynas, T.; Jusis, M. Analysis of the possibility to detect fake vessels in the Automatic Identification System. In Proceedings of the 2020 61st International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), Riga, Latvia, 15–16 October 2020. [CrossRef]
61. 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]
62. Wolsing, K.; Saillard, A.; Bauer, J.; Wagner, E.; van Sloun, C.; Fink, I.B.; Schmidt, M.; Wehrle, K.; Henze, M. Network attacks against marine RADAR systems: A taxonomy, simulation environment, and dataset. In Proceedings of the 2022 IEEE 47th Conference on Local Computer Networks (LCN), Edmonton, AB, Canada, 26–29 September 2022; pp. 114–122. [CrossRef]
63. Trend Micro. Toolkit for Research Purposes in AIS. 2014. Available online: https://github.com/trendmicro/ais (accessed on 21 April 2025).
64. Maritec Solutions. AIS VDM/VDO Decoder. Available online: https://www.maritec.co.za/tools/aisvdmvdodecoding/ (accessed on 21 April 2025).
65. Goudosis, A.; Katsikas, S. Secure Automatic Identification System (SecAIS): Proof-of-concept implementation. *J. Mar. Sci. Eng.* **2022**, *10*, 805. [CrossRef]

66. Shyshkin, O. Cybersecurity providing for maritime Automatic Identification System. In Proceedings of the 2022 IEEE 41st International Conference on Electronics and Nanotechnology (ELNANO), Kyiv, Ukraine, 10–14 October 2022; pp. 736–740. [CrossRef]
67. Iphar, C.; Napoli, A.; Ray, C. An expert-based method for the risk assessment of anomalous maritime transportation data. *Appl. Ocean Res.* **2020**, *104*, 102337. [CrossRef]
68. Bridge Command. Home. Available online: https://www.bridgecommand.co.uk/ (accessed on 21 April 2025).
69. 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]
70. Ruhland, L.; Schmidt, M.; Bauer, J.; Padilla, E. Keeping the baddies out and the bridge calm: Embedded authentication for maritime networks. In Proceedings of the 2022 International Symposium on Networks, Computers and Communications (ISNCC), Shenzhen, China, 19–22 July 2022; pp. 1–6. [CrossRef]
71. Wireshark. About Wireshark. Available online: https://www.wireshark.org/ (accessed on 21 April 2025).
72. Amazon. Cinematic RADAR Simulator 2.0. Available online: https://www.amazon.com/CINEMATIC-RADAR-SIMULATOR-2-0-Download/dp/B075R1PLP9 (accessed on 21 April 2025).
73. VMware. What Is ESXI. Available online: https://www.vmware.com/products/cloud-infrastructure/esxi-and-esx (accessed on 21 April 2025).
74. OPAL-RT Technologies. OPAL-RT, Real-Time Simulation Solutions. Available online: https://www.opal-rt.com/ (accessed on 21 April 2025).
75. Goudosis, A.; Katsikas, S. Secure AIS with identity-based authentication and encryption. *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2020**, *14*, 287–298. [CrossRef]
76. Klör, F.; Bauer, J.; Paulus, S.; Rademacher, M. Dude, Where's that ship? Stealthy radio attacks against AIS broadcasts. In Proceedings of the 2024 IEEE 49th Conference on Local Computer Networks (LCN), Normandy, France, 8–10 October 2024; pp. 1–7. [CrossRef]
77. Su, P.; Sun, N.; Zhu, L.; Li, Y.; Bi, R.; Li, M.; Zhang, Z. A privacy-preserving and vessel authentication scheme using Automatic Identification System. In Proceedings of the SCC'17: Proceedings of the Fifth ACM International Workshop on Security in Cloud Computing, Abu Dhabi, United Arab Emirates, 2 April 2017; Wang, C., Kantarcioglu, M., Eds.; Association for Computing Machinery: New York, NY, USA, 2017; pp. 83–90. [CrossRef]
78. Botunac, I.; Gržan, M. Analysis of software threats to the Automatic Identification System. *Brodogradnja* **2017**, *68*, 97–105. [CrossRef]
79. Jones, K.D.; Tam, K. High impact malware targeting maritime infrastructure. In *The Practice of Formal Methods: Essays in Honour of Cliff Jones, Part I*; Cavalcanti, A., Baxter, J., Eds.; Springer: Cham, Switzerland, 2024; pp. 236–250. [CrossRef]
80. Deng, Z.L.; Liu, H.D.; Huang, J.M.; Zou, D.J. A novel anti-jam navigation system based on A-GNSS. In Proceedings of the 2009 Joint Conferences on Pervasive Computing (JCPC), Tamsui, Taiwan, 3–5 December 2009; pp. 279–284. [CrossRef]
81. Filic, M. Foundations of GNSS spoofing detection and mitigation with Distributed GNSS SDR receiver. *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2018**, *12*, 649–656. [CrossRef]
82. Świerczyński, S.; Zwolan, P.; Rutkowska, I. Jamming as a threat to navigation. *Annu. Navig.* **2016**, *23*, 219–233. [CrossRef]
83. Liu, Y.; Li, S.; Fu, Q.; Liu, Z. Impact assessment of GNSS spoofing attacks on INS/GNSS Integrated Navigation System. *Sensors* **2018**, *18*, 1433. [CrossRef]
84. Jan, S.S.; Tao, A.L. Comprehensive comparisons of satellite data, signals, and measurements between the BeiDou Navigation Satellite System and the Global Positioning System. *Sensors* **2016**, *16*, 689. [CrossRef]
85. Lund, M.S.; Gulland, J.E.; Hareide, O.S.; Jøsok, Ø.; Weum, K.O.C. Integrity of Integrated Navigation Systems. In Proceedings of the 2018 IEEE Conference on Communications and Network Security (CNS), Beijing, China, 30 May–1 June 2018. [CrossRef]
86. Summers, W.C.; Bosworth, E. Password policy: The good, the bad, and the ugly. In Proceedings of the Winter International Synposium on Information and Communication Technologies, Cancun, Mexico, 5–8 January 2004.
87. Dimitrov, N.; Alexandrov, C.; Todorov, M. Cyber security analysis of maritime surveillance systems. In Proceedings of the 21st Annual General Assembly Proceedings of the International Association of Maritime Universities (IAMU) Conference, Alexandria, Egypt, 26–28 October 2021.
88. Rivas, L.; Stevens, S.; Zitter, A.; Khandelwal, V.; Vardhan, A.; Lohani, C.; Rouff, C.; Watkins, L. Assuring safe navigation and network operations of autonomous ships. In Proceedings of the 2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 8–10 January 2024; pp. 0138–0143. [CrossRef]
89. Visky, G.; Rohl, A.; Vaarandi, R.; Katsikas, S.; Maennel, O.M. Hacking on the high seas: How automated reverse-engineering can assist vulnerability discovery of a proprietary communication protocol. In Proceedings of the 2024 IEEE 49th Conference on Local Computer Networks (LCN), Normandy, France, 8–10 October 2024; pp. 1–7. [CrossRef]
90. Kessler, G.C. Protected AIS: A demonstration of capability scheme to provide authentication and message integrity. *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2020**, *14*, 279–286. [CrossRef]

91. Goudossis, A.; Katsikas, S.K. Towards a secure automatic identification system (AIS). *J. Mar. Sci. Technol.* **2019**, *24*, 410–423. [CrossRef]
92. 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.* **2021**, *75*, 333–345. [CrossRef]
93. Silonosov, A.; Henesey, L. Crypto-agility performance analysis for AIS data sharing confidentiality based on attribute-based encryption. In Proceedings of the 14th International Conference on Computer Science and Information Technology (CCSIT 2024), Copenhagen, Denmark, 21–22 September 2024; AIRCC Publishing Corporation: Tamil Nadu, India, 2024; Volume 14, pp. 193–212.
94. Hassani, V.; Crasta, N.; Pascoal, A.M. Cyber security issues in navigation systems of marine vessels from a control perspective. In Proceedings of the ASME 2017 36th International Conference on Ocean, Offshore and Arctic Engineering, Trondheim, Norway, 25–30 June 2017. [CrossRef]
95. Filic, M.; Dimc, F. Logistic Map-encrypted chaotic ranging code as a proposed alternative to GNSS PRN pseudorange code. *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2019**, *13*, 587–590. [CrossRef]
96. Ke, Y.; Lv, Z.; Zhang, C.; Deng, X.; Zhou, W.; Song, D. Tightly coupled GNSS/INS integration spoofing detection algorithm based on innovation rate optimization and robust estimation. *IEEE Access* **2022**, *10*, 72444–72457. [CrossRef]
97. Williams, P.; Basker, S.; Ward, N. e-Navigation and the case for eLoran. *J. Navig.* **2008**, *61*, 473–484. [CrossRef]
98. 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]
99. Ochin, E. Detection of spoofing using Differential GNSS. *Sci. J. Marit. Univ. Szczecin, Zesz. Nauk. Akad. Morska W Szczecinie* **2017**, *50*, 59–67. [CrossRef]
100. Raiyn, J. Maritime cyber-attacks detection based on a convolutional neural network. In *Computational Intelligence and Mathematics for Tackling Complex Problems 5*; Cornejo, M., Kóczy, L.T., Medina, J., Ramírez-Poussa, E., Eds.; Springer: Cham, Switzerland, 2024; pp. 115–122. [CrossRef]
101. Singh, S.; Singh, J.; Singh, S.; Goyal, S.B.; Raboaca, M.S.; Verma, C.; Suciu, G. Detection and mitigation of GNSS spoofing attacks in maritime environments using a genetic algorithm. *Mathematics* **2022**, *10*, 4097. [CrossRef]
102. Shyshkin, O.; Konovets, V. Detection of satellite navigation jamming in the maritime shipping. In Proceedings of the 2023 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), Kyiv, Ukraine, 13–18 November 2023; pp. 1–6. [CrossRef]
103. Basels, F.; Wolsing, K.; Padilla, E.; Bauer, J. Demo: Maritime Radar Systems under Attack. Help is on the Way! In Proceedings of the 2024 IEEE 49th Conference on Local Computer Networks (LCN), Normandy, France, 8–10 October 2024; pp. 1–4. [CrossRef]
104. Saillard, A.; Wolsing, K.; Wehrle, K.; Bauer, J. Exploring anomaly detection for marine RADAR systems. In *Proceedings of the European Symposium on Research in Computer Security*; Springer: Cham, Switzerland, 2024; pp. 361–381.
105. IMO. *MSC.1/Circ.1595 E-Navigation Strategy Implementation Plan—Update 1*; IMO: London, UK, 2018.
106. *IEC 61162-1*; Maritime Navigation and Radiocommunication Equipment and Systems: Part 1: Single Talker and Multiple Listeners. IEC: Geneva, Switzerland, 2016.
107. *IEC 61162-450*; Maritime Navigation and Radiocommunication Equipment and Systems—Digital Interfaces—Part 450: Multiple Talkers and Multiple Listeners—Ethernet Interconnection. IEC: Geneva, Switzerland, 2024.
108. *IEC 61162-460*; Maritime Navigation and Radiocommunication Equipment and Systems—Digital Interfaces—Part 460: Multiple Talkers and Multiple Listeners—Ethernet Interconnection—Safety and Security. IEC: Geneva, Switzerland, 2024.
109. Zhu, J.; Yan, L.; Guo, S. Research on ship network security based on game theory. In Proceedings of the 2019 2nd International Conference on Safety Produce Informatization (IICSPI), Chongqing, China, 28–30 November 2019; pp. 78–81. [CrossRef]
110. Hemminghaus, C.; Bauer, J.; Wolsing, K. SIGMAR: Ensuring integrity and authenticity of maritime systems using digital signatures. In Proceedings of the 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 31 October–2 November 2021; pp. 1–6. [CrossRef]
111. Sahay, R.; Meng, W.; Estay, D.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]
112. IMO. *Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems*; IMO: London, UK, 2017.
113. RWO Veolia. Bilge Water Management. Available online: https://ship.nridigital.com/ship_mar19/veolia_water_technologies (accessed on 21 April 2025).
114. Oruc, A. Tanker industry is more ready against cyber threats. In Proceedings of the International Conference on Marine Engineering and Technology Oman 2019 (ICMET Oman), Muscat, Oman, 5–7 November 2019. [CrossRef]
115. INTERTANKO. Social Media Guidance for Seafarers. Available online: https://cyberonboard.com/wp-content/uploads/Intertanko-Golden-Rules.pdf (accessed on 21 April 2025).
116. ICS; BIMCO; MPA. Cyber Security Onboard Ships. Available online: https://cyberonboard.com/wp-content/uploads/ICS-Cyber-Security-onboard-Ships.pdf (accessed on 21 April 2025).

117. MarineLink. From Mines to AIS Spoofing, Assessing the Risks to Shipping in the Black Sea. 2022. Available online: https://www.marinelink.com/news/mines-ais-spoofing-assessing-risks-494729 (accessed on 21 April 2025).
118. OCIMF. *SIRE 2.0 Question Library: Part 1—Chapters 1 to 7*; OCIMF: London, UK, 2022. Available online: https://www.ocimf.org/document-libary/630-sire-2-0-question-library-part-1-chapters-1-to-7-version-1-0-january-2022/file (accessed on 21 April 2025).
119. Oruc, A. In September 2024, SIRE 2.0 Enforces Improved Cybersecurity Requirements. 2024. Available online: https://cyberonboard.com/in-september-2024-sire-2-0-enforces-improved-cybersecurity-requirements/ (accessed on 21 April 2025).
120. Leovy, J. Cyberattack Cost Maersk as Much as $300 Million and Disrupted Operations for 2 Weeks. 2017. Available online: https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html (accessed on 21 April 2025).
121. Oruc, A.; Amro, A.; Gkioulos, V. Assessing Cyber Risks of an INS Using the MITRE ATT&CK Framework. *Sensors* **2022**, *22*, 8745. [CrossRef]
122. IMO. *MSC.192(79) Adoption of the Revised Performance Standards for RADAR Equipment*; IMO: London, UK, 2004.
123. BIMCO; CSA; DCSA; ICS; INTERCARGO; InterManager; INTERTANKO; IUMI; OCIMF; WSC; et al. The Guidelines on Cyber Security Onboard Ships. Available online: https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf (accessed on 21 April 2025).
124. IACS. E26 Cyber Resilience of Ships. Available online: https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/02/04140503/UR-E26-Rev.1-Nov-2023-CR.pdf (accessed on 21 April 2025).
125. IACS. E27 Cyber Resilience of On-Board Systems and Equipment. Available online: https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2022/05/29103853/UR-E27-Rev.1-Sep-2023-CLN.pdf (accessed on 21 April 2025).
126. Blenkey, N. ABS Issues First Cyber Security-Ready Notation to HHI VLCC. 2018. Available online: https://www.marinelog.com/news/abs-issues-first-cyber-security-ready-notation-to-hhi-vlcc/ (accessed on 21 April 2025).
127. Safety4Sea. BV Awards Cyber Security Notation to LNG Carrier. 2020. Available online: https://safety4sea.com/bv-awards~-cyber-security-notation-to-lng-gas-carrier/ (accessed on 21 April 2025).
128. O'dwyer, R. NYK Line Oil Tanker Gets First ClassNK Cyber Notation. 2021. Available online: https://smartmaritimenetwork.com/2021/11/10/nyk-line-oil-tanker-gets-first-classnk-cyber-notation/ (accessed on 21 April 2025).
129. DNV. Stena Drilling and DNV GL Sign Contract for First Cyber Secure Class notation. 2019. Available online: https://www.dnv.com/news/stena-drilling-and-dnv-gl-sign-contract-for-first-cyber-secure-class-notation-149153 (accessed on 21 April 2025).
130. Digital Ship. KR Issues First Cybersecurity Class Notation to HHI for Very Large LPG Carriers. 2020. Available online: https://thedigitalship.com/news/maritime-satellite-communications/kr-issues-first-cybersecurity-class-notation-to-hhi-for-very-large-lpg-carriers/ (accessed on 21 April 2025).
131. Safety4Sea. Lloyd's Register Gives World's First Cyber SAFE Notation. 2017. Available online: https://safety4sea.com/lloyds-register-gives-worlds-first-cyber-safe-notation/ (accessed on 21 April 2025).
132. *ISO 14001*; Environmental Management Systems—Requirements with Guidance for Use. International Organization for Standardization: Geneva, Switzerland, 2015.
133. IMO. *MSC.112(73) Adoption of the Revised Performance Standards for Shipborne Global Positioning System (GPS) Receiver Equipment*; IMO: London, UK, 2000.
134. Howell, E. Russia Is Jamming GPS Satellite Signals in Ukraine, US Space Force Says. 2022. Available online: https://www.space.com/russia-jamming-gps-signals-ukraine (accessed on 21 April 2025).
135. Son, P.W.; Park, S.G.; Han, Y.; Seo, K. eLoran: Resilient positioning, navigation, and timing infrastructure in maritime areas. *IEEE Access* **2020**, *8*, 193708–193716. [CrossRef]
136. Luccio, M. eLoran: Part of the Solution to GNSS Vulnerability. 2021. Available online: https://www.gpsworld.com/eloran-part~-of-the-solution-to-gnss-vulnerability/ (accessed on 21 April 2025).
137. IMO. *MSC-FAL.1/Circ.3/Rev.3 Guidelines on Maritime Cyber Risk Management*; IMO: London, UK, 2025.
138. Salim, H.M. Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risks. Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, USA, 2014.
139. Ahn, W.; Chung, M.; Min, B.G.; Seo, J. Development of cyber-attack scenarios for nuclear power plants using scenario graphs. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 836258. [CrossRef]
140. Torres, D. Cyber security and cyber defense for Venezuela: An approach from the Soft Systems Methodology. *Complex Intell. Syst.* **2018**, *4*, 213–226. [CrossRef]
141. Omrani, M.; Shafiee, M.; Khorsandi, S. A model to measure cyber security maturity at the national level. In Proceedings of the 2023 31st International Conference on Electrical Engineering (ICEE), Tehran, Iran, 9–11 May 2023; pp. 110–116. [CrossRef]
142. Oruc, A.; Chowdhury, N.; Gkioulos, V. A modular cyber security training programme for the maritime domain. *Int. J. Inf. Secur.* **2024**, *23*, 1477–1512. [CrossRef]
143. United Nations. The 17 Goals. Available online: https://sdgs.un.org/goals (accessed on 21 April 2025).
144. IMO. *HTW 8/15/1 Any Other Business. Necessity of Developing Relevant Provisions Concerning Cybersecurity-Related Training for Seafarers*; IMO: London, UK, 2021.

145. TalTech. Introduction to Cyber Security. Available online: https://ois2.ttu.ee/uusois/subject/VLL1480 (accessed on 21 April 2025).
146. NHL Stenden University of Applied Sciences. MCAD Maritime Cyber Attack Database. 2025. Available online: https://maritimecybersecurity.nl/ (accessed on 21 April 2025).
147. Appel, M.; Iliopoulos, A.; Fohlmeister, F.; Pérez Marcos, E.; Cuntz, M.; Konovaltsev, A.; Antreich, F.; Meurer, M. Experimental validation of GNSS repeater detection based on antenna arrays for maritime applications. *CEAS Space J.* **2019**, *11*, 7–19. [CrossRef]