Journal of
Marine Science and Engineering

MDPI

Article

Assessing Cyber Challenges of Maritime Navigation

Andrej Androjna [1,*], Tanja Brcko [1], Ivica Pavic [2] and Harm Greidanus [3]

[1] Faculty of Maritime Studies and Transport, University of Ljubljana, 6320 Portorož, Slovenia; tanja.brcko@fpp.uni-lj.si
[2] Faculty of Maritime Studies, University of Split, 21000 Split, Croatia; ipavic71@pfst.hr
[3] European Commission, Joint Research Centre (JRC), 21027 Ispra, Italy; harm.greidanus@ec.europa.eu
* Correspondence: andrej.androjna@fpp.uni-lj.si

Received: 15 September 2020; Accepted: 1 October 2020; Published: 3 October 2020

Abstract: This paper provides a close investigation into the landscape of both cyber threats and actual incidents in the maritime sector, identifying the cyber trends and challenges as they relate to safe navigation and marine shipping. As an important subset of cyber threats that impact many maritime systems, the vulnerabilities of satellite navigation systems, in particular the Global Positioning System (GPS), receive special attention. For this article, a systematic literature review was conducted, complemented by the research and analysis of a specific spoofing event. Analyzing available resources, we might summarize that a shift in mind-set is essential to direct more attention and resources toward cybersecurity as well as the necessity for manufacturers to improve the cybersecurity of their products, as shipping systems currently remain vulnerable to cybercriminals. There is a need for multiple positioning, navigation, and timing (PNT) systems onboard maritime vessels to complement GPS-only navigation. The use of multiple satellite navigation constellations, public as well as private, in combination with the terrestrial components of an enhanced LOng-RAnge Navigation (eLoran) system and ports' laser-based aid system for berthing and docking should provide the shipping industry with the direly needed increased protection from cyber-attackers for the foreseeable future.

Keywords: maritime cyber; cybersecurity; the safety of navigation; shipboard systems; GPS jamming and spoofing

1. Introduction

Today's global maritime sector depends increasingly on digitalization, integration of operations, and automation. New opportunities arise—and cyber threats emerge. Cyber technologies have become essential, even critical, not just to the operation and management of numerous systems and processes onboard ships and in ports, but also for the safety, security, and protection of the ship, the crew, the cargo, and the marine environment. These technologies have integrated IT (Information Technology) and OT (Operational Technology) onboard ships through networking and connectivity to the internet [1–6]. In the World Economic Forum's Global Risks Report 2020, cyberattacks on critical infrastructure with a reference to shipping are rated the fifth top risk in 2020 [1]. According to Rizika [2]: "Cyber–attacks on the maritime industry's OT systems have increased by 900% over the last three years. There were 50 significant OT hacks reported in 2017, rising to 120 in 2018 and more than 300 in the previous year. This year will probably end with more than 500 major cybersecurity breaches, with substantially more going unreported". When deliberate disruptions are discovered, there are many incentives to keep that information quiet, mainly because of the maritime industry not being eager to reveal the weaknesses and vulnerabilities of their products or services.

Safety has always been a critical driver in regulations of maritime operations; and now that navigation systems have been increasingly reliant on cyber technologies to improve the effectiveness

and safety of navigation, a need for safeguarding shipping from cyber threats has arisen [3–21]. Therefore, the International Maritime Organization (IMO) has already taken action and given ship owners and executives until 2021 to include cyber risk management into ship safety protocols. Owners run the risk of having ships detained if they have not included cybersecurity in the International Safety Management Code (ISM Code) on safety management onboard ships by 1 January 2021 [22,23].

The IT security system is known as cybersecurity. In contrast, the security system of the OT system is known as cyber safety, although both form part of the concept of cybersecurity [22]. Cybersecurity can be defined in brief as the "preservation of confidentiality, integrity and availability of information in the Cyberspace" [24]. However, the longer definition by the International Telecommunication Union (ITU) better reflects the wide scope: "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment" [25]. Indeed, "cybersecurity combines a multiplicity of disciplines from the technical to behavioural and cultural" [26].

Within this definition, 'cyber environment' comprises the interconnected networks of both IT and cyber-physical systems utilizing electronic, computer-based, and wireless systems, including the information, services, social, and business functions that exist only in cyberspace. On a ship, the computer-based systems will comprise a range of information technology components (for example, personal computers (PCs), laptops, tablet devices, servers, and networking components such as routers and switches) and operational technology (for example, control systems, sensors, actuators, radar) [27–29]. Current shipboard control systems contain significant levels of automation to perform complex functions such as navigation and propulsion control. The purpose of employing automated systems has been to reduce cost and improve performance. While automation offers excellent benefits, it also introduces a set of corresponding cybersecurity-related risks [22,30,31].

The global maritime industry systems depend on satellite navigation, especially GPS. Of particular concern is the relative ease [32] by which these systems can be jammed (through denial of reception by a competing signal) or spoofed (through deliberate introduction of a false signal). Satellite navigation is a vital part of a wide variety of the shipboard, port, and even oil rig systems [22,32–39], including the Automatic Identification System (AIS) that is vital for navigation safety [40].

This article is a close investigation of the landscape of both cyber threats and actual incidents in the maritime sector. Furthermore, it discusses the risks, the motives and likely entities behind the threats, and the impacts of an attack that can range far beyond the company being attacked. Finally, it recommends how cybersecurity could be improved in the maritime sector over time, and hopefully it might inspire further research work.

The paper is organized as follows: Section 2 describes the methodology, Section 3 presents an analysis of the cybersecurity landscape in the maritime sector and practical research into an AIS spoofing event. Section 4 discusses significant findings and provides some recommendation, and Section 5 contains a summary and conclusions.

2. Methodology

A systematic literature review was conducted, based on and structured according to documented guidelines [41–43] through which a comprehensive, explicit, reproducible, and implicit idiosyncratic method of data collection is followed. This method consists of ten steps that can be grouped into three main phases:

(1) Planning the review: The planning phase focused on defining a review question to guide the search: "What are the effects of cyberattacks and cybersecurity in the maritime domain?"

(2) Conducting a review: In the search phase, the relevant research databases, the keywords to be used during these searches, and the proper timeframe for the resulting documents to be included

were identified. Data for the study were available in the databases such as Scopus, Web of Science, Google Scholar, and open sources. The search keywords were determined from a knowledge domain analysis around the concept of "maritime cyber". The two main knowledge domains to be scanned were identified as "maritime cyber" and "cybersecurity". After the broad initial literature search, explicit inclusion and exclusion criteria—i.e., refined selection (e.g., document type, themes, research area) to identify relevant documents for this analysis—were applied. The documents were analyzed and synthesized according to contexts, methodological approaches, and outcomes. Our final list consisted of 171 documents (76 articles, 52 peer-reviewed journal papers, and 43 reports by specialized agencies) that covered the area of "maritime cyber", ranging from 2016 to 2020. While the results of this article are novel, a few earlier studies on this topic were also taken into account as references.

(3) Reporting and dissemination: In the next section, we report on our findings from the literature review.

The specific aspect of AIS/GPS spoofing is reinforced by an analysis in Chapter 3 by the Faculty of Maritime Studies and Transport, the University of Ljubljana, research and analysis [44] regarding a particular AIS spoofing event at Elba Island at the end of 2019.

3. Findings

This chapter demonstrates the unique challenges of maritime cybersecurity that include the issues with securing vessels at sea and the shore-based infrastructure supporting this industry. It presents findings of some of the possible cyberattack trajectories on maritime-related systems for navigation, propulsion, and cargo. Despite recent headlines in the media regarding the effects of cyberattacks in the maritime domain, there still seems to be a lack of understanding of cyber incidents on marine navigation systems [6]. To understand the current research being done, it is essential to apprehend its background, the working of the internet, its liabilities, and the methods which can be used to initiate attacks on the system [45]. Until 2010, the majority of cyberattacks were driven by an attempt to obtain personal or financial data. The nature of cyber is changing, and today, the maritime sector is experiencing highly sophisticated and complex attacks seeking to take the reins of its industrial control systems that are designed to be closed to the outer world [46].

3.1. Regulatory Framework—Global

The maritime cybersecurity legal issues are complex [40]. In 2017, the International Maritime Organization (IMO) adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management System (SMS) [47]. The resolution stated that an approved SMS should take into account cyber risk management following the objectives and functional requirements of the International Safety Management Code (ISM Code) [48]. It further encourages administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021. IMO also developed guidelines on maritime cyber risk management that provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities. These guidelines highlighted that effective cyber risk management should start at the senior management level [49]. Aligned with both IMO documents, the Guidelines on Cyber Security Onboard Ships were made to provide practical recommendations on maritime cyber risk management covering both cybersecurity and cyber safety [50]. In addition, IMO is preparing, in collaboration with the International Electrotechnical Commission (IEC), a new standard for maritime navigation and radio-communication equipment and systems: IEC 63,154 "Cybersecurity—General Requirements, Methods of Testing and Required Test Results" [3,51].

3.2. Regulatory Framework and Policy Priorities—EU

The 2013 EU cyber strategy aims to safeguard the EU's core values in cyberspace in light of the rapidly increasing growth of cyberspace and the threats to it. A safe cyberspace is essential to the digital single market that the EU sees as a vehicle for increased prosperity. Goals of the 2013 cyber strategy are increased resilience, decimated cybercrime, development of cyber defense policies and capabilities, increased EU autonomy in industrial resources for cybersecurity, and the fostering of a coherent international policy [52]. An EU Directive of 2013 seeks to legally criminalize cyberattacks and cybercrime [53].

The 2016 NIS directive [54,55] requires that EU Member States are adequately equipped to deal with cyber incidents—e.g., by Computer Security Incident Response Teams (CSIRT)—and that businesses in vital and ICT-dependent sectors that provide essential services take appropriate security measures. Information exchange and operational cooperation are required. The directive specifies operators of essential services for the maritime sector: passenger and freight water transport; ports and their facilities and operating entities; and vessel traffic services.

The EU has set up specialized entities such as the European Union Agency for Cybersecurity (ENISA), the European Cyber Crime Centre (EC3) at Europol, and the Computer Emergency Response Team (CERT-EU) [56], as well as launching initiatives to increase cybersecurity in various critical sectors. In particular, the Information Sharing and Analysis Centres (ISAC) are intended to be trusted entities to foster information sharing and good practices about physical and cyber threats and their mitigation [57]. The US also uses ISACs, as well as Information Sharing and Analysis Organizations (ISAO), based on US government regulations, to share cyber threat information between various stakeholders [58], while the maritime sector has three (MPS-ISAO, Maritime ISAC, maritime transportation system (MTS)-ISAC). However, in Europe the maritime sector lags behind in creating ISACs [57]. The European Cyber Security Organisation (ECSO) represents the counterpart to the European Commission for the Implementation of the Cyber Security Contractual Public–Private Partnership (cPPP). Their recent report on the transportation sector [59] aims to take a holistic approach of the implications of cybersecurity on the transport sector as a whole, but also treats the maritime sector separately. It notes that information sharing in the maritime sector falls dramatically short, and recommends the creation of a safe, confidential, and anonymous reporting center for the maritime sector.

The 2017 Joint Communication on Resilience, Deterrence and Defence [60] proposes, among other things, greater resilience, strategic autonomy, more skills, and a security by design approach.

The 2019 EU Cybersecurity Act [61] sets new objectives and tasks for ENISA as a prime tool to implement cybersecurity in the EU, and provides a framework for the establishment of European cybersecurity certification schemes for digital products, services, and processes.

Specifically for maritime, the 2014 European Union Maritime Security Strategy [62] recognizes cyber as one of the risks in the maritime domain. Its 2014 Action Plan [63] contains five actions on cyber, and its 2018 revised Action Plan [64] contains six. Progress reports [65–67] provide details on the implementation of these actions in the EU maritime sector, including work on risk assessments, response capacity, exercises, workshops, and working groups. ENISA has published studies dedicated to the maritime sector [68,69].

Most recently, the EU Security Union Strategy for 2020–2025 [70] notes that cyberattacks and cybercrime continue to rise. It calls for a whole-of-society approach to security, with sector-specific initiatives to tackle the specific risks faced by critical infrastructures such as in transport and maritime. The latest conclusions of the Council of the EU [71] underline that cybersecurity remains a shared responsibility of all players, and continue to call for improved cyber resilience, more effective responses to cyberattacks, further development of cybersecurity standards and ICT certification schemes, more cybersecurity research, and innovation capabilities to autonomously secure the EU economy and critical infrastructures.

The development of 5G is expected to boost connectivity, with significant impacts on the maritime sector. The cybersecurity of 5G will be essential, and the recent communication "Secure 5G deployment in the EU—Implementing the EU toolbox" [72] offers references and guidelines.

3.3. Cyber Trends and Challenges

This chapter presents findings of some of the possible cyberattack trajectories on maritime-related systems for navigation, propulsion, and cargo, as well as shore-based systems. It has identified some areas where a special targeted effort is required to ensure cyber and information security [73].

3.3.1. Types of Cyberattack

There may be nothing new about the need for ships to deliver cargo or patrol their country's coasts. However, the threats they are increasingly likely to encounter, invisible to any telescope, might place the maritime sector in uncharted waters [74]. According to Jones et al. [75], current threat implications of maritime-based cyberattacks include business disruption, financial loss, damage to reputation, damage to goods and environment, incident response cost, and fines or legal issues. For example, attackers could manipulate passenger lists, perform illegal activities (transports), breach sensitive cargo transports, cause engines failures, shut down vessels, or otherwise manipulate onboard control systems [74,76]. Bansal et al. [45] categorized the risks associated with an attack into three dependent factors: threats (who is attacking), vulnerabilities (the weaknesses they are attacking), and impacts (what the attack does).

There is a variety of methods that exist for those who seek to target the shipping industry [74,77]:

- Extortion/ransomware for allowing the vessel/port to restore operations;
- Digital piracy by shutting down the vessel/port;
- Espionage for gaining sensitive information that can be used by the competition;
- Defamation/litigation by causing ISPS Code noncompliance/delaying the vessel/causing disruption;
- Subversion of the supply chain;
- Terrorism;
- (H)Activism for conveying a message.

In the Danish Cyber and Information Security Strategy for the maritime sector, 2019–2022 [73], it is assessed that the general cyber threat is directed against maritime commercial businesses and does not currently pose a direct threat to maritime operations. The strategy on one side considers that the threat from cyber espionage and cybercriminals against the maritime sector is very high. In contrast, on the other side, it evaluates the threat from destructive cyberattacks, cyber activism, and cyber terrorism as low.

In the maritime domain, a rise in spear-phishing of vessels at sea has been noted. The BIMCO survey [78] presented several incidents where malicious software was introduced to ship systems unintentionally, often by third parties, to check or even update specific bridge equipment. Although the malware significantly degraded functionality of the onboard computer system, no essential vessel control system had been impacted [79]. Consequently, BIMCO's survey [78] shows that maritime companies are increasingly not only assessing their own systems and work practices in a bid to limit the likelihood of an attack but are also assessing the risk introduced across their supply chain. Respondents have also noted that a company's staff was its greatest cyber vulnerability; therefore, many cybersecurity measures remain firmly focused on reducing human error.

3.3.2. Ships Suffer Cyberattack

Ship onboard systems are susceptible to a cyberattack. There are reports [6,32,33,44,46,75,77,79–93] in which significant weaknesses of these systems have been identified. Modern technologies have integrated IT (Information Technology) and OT (Operational Technology) onboard ships through

networking and connectivity to the internet [2,22,27,94–96]. However, there is no real segregation between the IT and OT networks. Any person can come in on the OT side and penetrate the IT side. We are seeing this now. Our analysis showed that there were many reports issued regarding anonymous hackers trying to disrupt ships' electronics/computers or to steal sensitive information. The impact of these kinds of attacks could be enormous. It has been noted that successful IT network hacks have their origins in the initial penetration of the OT system [2,22]. To gain remote access to the IT or OT systems, the satellite, 4G, or Wi-Fi connections of the vessel have to be breached [22,27,32].

Concerning security, time is a complicating factor. Technological vulnerability and its exposure change significantly during the lifetime of a vessel. The IT and OT will need dedicated technical improvements over time. The maintenance on IT and OT systems must be aligned with their dock-time, of course, or appropriate remote access management should be in place to ensure that only the vendor is able to perform updates [14].

According to the analysis in [73], there are three prevalent cyber and information security risks related to the maritime sector in general:

- Lack of timely response to technical vulnerabilities: A technology gap is identified between the IT and on ships and land-based systems. Land-based systems are usually better updated than the equivalent ship-based systems [97], which are, therefore, more susceptible to cyberattacks.
- No process in place for upgrades: There is a risk if the upgrading process of OT equipment does not match the standards associated with IT technologies.
- Securing critical systems: The potential consequences of a targeted attack to databases and registers based on older technology are lack of data integrity, loss of reputation, and a potential financial loss.

Two different experiments conducted by Svilicic et al. [98] and Hareide [6] demonstrated that cyberattacks against integrated navigational systems (INS), usually considered as an offline system, are relatively easily achievable. Disconnection from the internet prevents outside threats; however, the vulnerabilities arising from the unmaintained operating system could also be triggered by inside actors (the ship's crew), either unintentionally or maliciously. With the INS connection to the internet, the cyber threats would rise to a critical level, demanding instant action [3].

According to the BIMCO survey [93], the most vulnerable systems onboard ships are positioning systems (GPS, AIS, Radar), ECDIS, engine control, and monitoring. Like AIS, GPS for civilian use is not encrypted or authenticated, and each has been identified as potentially vulnerable to attack.

ECDIS can be compromised in order to modify files and insert malicious content [6,99]. An ECDIS compromise can take over the whole INS or display the vessel in a false position. A cyberattack can mislead a ship as, for example, in 2016 when two naval ships were misdirected in the Persian Gulf [100]. Another example happened in February 2017. Cybercriminals reportedly took control of the navigation systems of a German-owned 8250 TEU container vessel. The crew attempted to regain control and had to bring IT experts on board to solve the situation. The case serves as a "pre-warning" about hackers' abilities to gain control over the vessels to carry out, for instance, kidnap and ransom [101,102].

Another potential cyberspace vulnerability is the Voyage Data Recorder (VDR), from its connection to other ship systems that links to online services through satellite communications. However, the risks related to VDR weaknesses is, according to Kala [86], marginal, since VDRs do not directly control the movement of a vessel.

3.3.3. Offices Onshore

After the devastating cyber incident in June 2017 when the NotPetya malware attack, originating in Ukraine, infected the IT systems of the shipping giant Maersk and forced the company to shut down all devices and handle all operations manually, shipping offices onshore have realized that the shipping industry is not immune to cybercrime. Maersk was not explicitly targeted, and thus it was

rather collateral damage. The attack resulted in significant interruptions to Maersk's operations and terminals worldwide, costing them up to USD 300 million [6,77,79,103].

Another wake-up call for the maritime industry were two major cyber incidents reported in 2018. The first happened in July 2018 when COSCO Shipping Lines fell victim to a cyberattack. The company's internet connection was disrupted within its offices in the Americas. After activation of COSCO's contingency plans, operations were back to normal after five days. Being aware of what happened to Maersk, they had taken proactive steps to minimize their risk of a cyberattack. The second incident occurred in October 2018 when the Australia-based ferry and defense shipbuilder Austal was hit by a cyberattack that penetrated their data management systems. The attackers managed to steal internal data and offered some of it for sale on the dark web in an apparent extortion attempt [103].

Carnival Corporation was the latest to fall victim to a ransomware attack on its IT systems in August 2020. The cybercriminals managed to download certain data files related to guests and employees' personal data, which could result in potential claims from guests, employees, shareholders, or regulatory agencies [104].

According to Hannemann [103], there are three key takeaways from these three cyberattacks. The first is related to IT hygiene, which is key to fighting cybercrime—a need to shift people's mind-set towards IT security. Second, every shipping manager needs to approach cybersecurity as an integral part of overall safety management. Response and recovery plans should be in place, updated, and tested frequently. Third, there is no zero cyber risk environment today, since new cyber threats and vulnerabilities are constantly emerging. Despite all precautions, vulnerabilities remain in the systems and networks, and attackers are constantly trying to find new tools to break through cyber defenses.

3.3.4. Ports, Terminals, and Supply Chains

Ports are an integral node of maritime transportation and the land transport chain. They rely on information from both shipping lines and land-side logistics companies. The lack of clear standards and requirements addressing critical maritime infrastructure demonstrates a compelling need for standardized policies for assessing, containing, and mitigating cyber risks. Legacy IT systems and an expanding Internet of Things (IoT) contribute to making ports vulnerable [105]. Roughly half, only, of the world's shipping ports understand or are aware of their problems and vulnerabilities concerning cybersecurity [59]. As valves in global economic arteries, the port infrastructures' protection against cyber risks is an absolute imperative [97].

As for this infrastructure, critical systems (ship's cargo handling, container tracking) may be penetrated, as occurred in the port of Antwerp where hackers gained access to the port's terminal operating system and trafficked drugs [77]. Hackers working with drug-smuggling criminals infiltrated the computerized cargo tracking system to identify the shipping containers in which consignments of drugs had been hidden. The gang then drove the containers from the port, retrieved the drugs, and covered their tracks. The criminal activity continued for two years from June 2011, until it was stopped by investigative authorities [46,75].

Another example is the hacking into the Port of San Francisco when their Electronic Information System "moved" the port in cyberspace twenty miles north, which became problematic in the foggy weather [106].

The analysis showed that successful cyber penetration into the port infrastructure information system allows attackers movement or the theft of illicit cargo. This system is vulnerable and it is easy to see how it can be exploited by cybercriminals that will continue to do the unexpected [7,107]. We can be certain that the nature of attacks of this sort will evolve [46,73].

Aids to Navigation (AtoN) are an integral and critical part of marine infrastructure. Traditionally AtoNs have been physical objects such as lighthouses, buoys, and beacons. The introduction of virtual AtoNs that appear on AIS INS displays via the AIS communication system is an achievement of the modern digital era. Though still under development, virtual AtoNs play a vital role in enhancing

navigational safety. The AIS system is not as secure as it should be and can, therefore, be disrupted by malignant action.

3.3.5. Jamming and Spoofing

This chapter presents the vulnerability of the Global Navigation Satellite System (GNSS) to jamming and spoofing activities of state and non-state actors that can cause significant damage to major economies and everyday consumers alike. GNSS refers to a space-based system such as the US Global Positioning System (GPS/NAVSTAR—a military capability which civilian use), Russia's Global Navigation Satellite System (GLONASS), the European Union's Galileo System (a civil project intended for civil government and commercial use), and China's Beidou Navigation Satellite System. In addition, there are regional systems such as India's Navigation Indian Constellation (NavIC) and Japan's Quazi-Zenith Satellite System (QZSS).

GNSS Jamming is the deliberate transmission of signals on frequencies used by GNSS in an effort to prevent receivers from locking-on to authentic GNSS Signals. GNSS jamming requires relatively little technical knowledge and can be conducted by merely drowning out genuine signals with random or disruptive noise. *GNSS Spoofing* refers to the transmission of simulated false GNSS satellite ephemeris and timing information which coerces the victim receiver into calculating incorrect positioning and, in some cases, timing information [108–110]. GNSS spoofing is quite different from GNSS jamming. While navigation systems sound alarms when they recognize jammers, spoofing systems create false signals that confuse even state-of-the-art GNSS systems, leading to more severe consequences. To mitigate most of the vulnerabilities of one navigational system, it is recommended to use more of them [3].

The threat of GNSS spoofing has been known to the maritime industry for years. In 2017, the incident at Gelendzhik Airport received attention in international media. At least 20 vessels in the vicinity of the Black Sea Novorossiysk Commercial Sea Port reported that their AIS traces erroneously showed their position as Gelendzhik Airport, around 32 km inland. There were a large number of vessels involved, and all of the ships' tracking systems placed them in the same nonsensical location. That led to informed speculation that the incident could be attributed to one of the space superpower states' testing of satellite navigation spoofing technology. Whether it was as part of its electronic warfare arsenal or they were simply using it as an anti-drone measure for very VIP protection, it is somewhat suggestive that it was GNSS spoofing of defense development inflicted on a civilian scenario.

In his research, Bergman [87] has found ships in various parts of the world reporting locations thousands of miles away and circling at precisely 20 knots. It is unclear if these errors were the result of the ships' AIS system or some fault or influence on GPS receivers, a real mystery of some form of GPS interference.

In another event, in July 2019, a British oil tanker, the Stena Impero, was seized by Iranian forces after being spoofed to cause the vessel to shift its course into Iranian waters. As a consequence, the vessel, cargo, and the crew had become more than pawns in a geopolitical war [111]. Many of the shipping companies operating ships in the region have also instructed their vessels to transit Hormuz only at high speed and during the daylight hours. Nevertheless, we should not forget that one-third of the world's seaborne oil—some 17 million barrels per day—passes through the strait, making it one of the most important oil trading routes in the world.

AIS is a critical safety system designed to provide a ship's position and course to neighboring ships to prevent collision [3]. The manipulation of the AIS system that was observed not long ago, on 3 December 2019, as illustrated in Figure 1, might have been spoofing.

An Italian AIS base station experienced a ship-spoofing situation near Elba Island that was visible in the European Maritime Safety Agency (EMSA) Maritime Application, SSN Ecosystem GUI [89]. The first investigation provided by the Italian Coast Guard indicated 870 different vessels were created at two different moments (13:13 and 13:28) with a duration of 3 min in the first transmission and 2 min in the second. All the tracks appeared in an area of 28 × 21 nautical miles between Elba Island and

Corsica with different routes and speeds, rendering the monitoring of the maritime traffic in the area impossible and impacting real vessel transmissions.

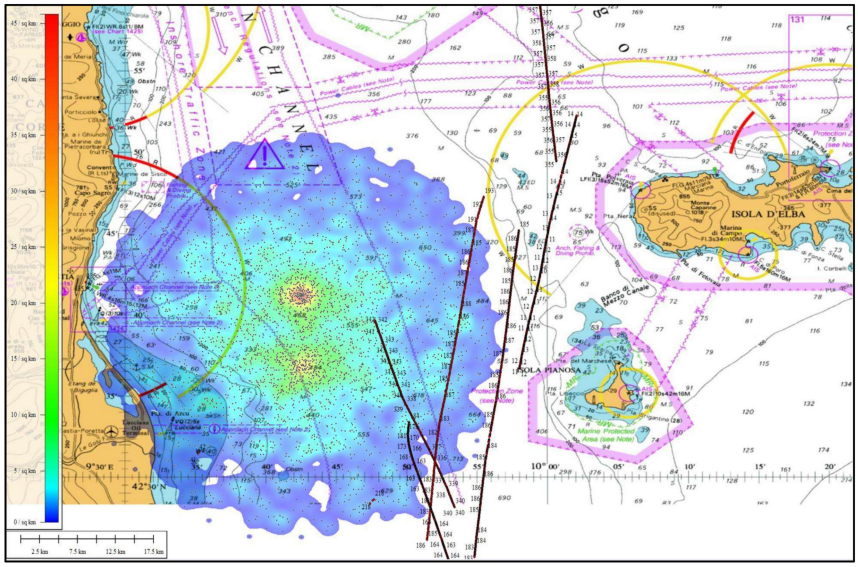

Figure 1. Automatic Identification System (AIS) spoofing analysis near Elba Island.

At the Faculty of Maritime Studies and Transport, University of Ljubljana, we have thoroughly investigated the situation to support EMSA's analysis and found 3742 fake ships (861 false tracks with MMSI 24480XXXX) that generated together 5133 reports, as illustrated in Figure 1. By using the European Marine Observation and Data Network (EMODnet) method [112], a traffic density map (TDM) is created by using ship positioning data collected from Terrestrial and Satellite AIS data sources, the maritime infrastructure, and the SafeSeaNet Ecosystem Graphical Interface (SEG) application. It showed, according to Perkovič [44], shipping density of up to 45 ships/km^2. The analyses pointed out that the AIS spoofing generator was located in the Elba Island area and that spoofing was conducted by a transmitter tuned onto AIS channel A, occupying around 54% of the available slots. Data were further processed to see whether it affected traffic safety. Only one vessel can be seen to have deviated slightly, although it cannot be proven that the change in course was due to the spoofing.

As evident through such examples, deliberate disruptions have affected shipping in international waters and engaged in innocent passage through territorial waters. Disorders to GNSS-enabled positioning and navigation have therefore become a global phenomenon, and to tackle a global problem, the GNSS community requires a global solution [35].

Another concern of the satnav community is related to the risks of being covertly tracked and of being exposed to malware through a satellite communication channel. The two-way communication that some GNSS systems now offer opens up that possibility. These risks have in particular been discussed in connection with the now officially operational BeiDou system [90,91].

3.3.6. Autonomous Ship

Remotely piloted and even more so autonomous marine vessels are going to revolutionize maritime operations and will be undoubtedly more vulnerable to cyberattacks [66,67]. Navigation issues and cyber risks should be taken into serious consideration by IMO when creating rules for autonomous shipping. It is expected that the maritime attack surface will continue to expand and autonomous ships will form a prominent piece of the future maritime landscape, underscoring the growing reliance on interconnected information systems [74,113].

3.3.7. Cyber and Social Media

Analysis has shown that there is a need to consider the impact of social media on the crew's life at sea. The usage of social networking services can unintentionally cause many problems, such as the leakage of information on confidential shipping matters, diffusion of marine accident information, and the exposure of personal private information or photos [114]. Communication and socialization with the outside world, particularly with friends and family has become commonplace for the modern seafarer. From the perspective of the human element, cyber wellness is a critical component of their overall health and personal well-being. However, with that privilege also comes the responsibility to protect oneself and ensure that the ship's safety and security are not compromised. These shared objectives are achieved by employing good personal cybersecurity practices [115].

3.3.8. Hybrid Threats

In recent years, the West and the world's democratic societies have become increasingly exposed to hybrid threats. Hybrid threats are multi-faceted subversive or coercive activities that aim to undermine a state, frustrate its decision making processes, erode the trust in its institutions, stay below a threshold of detectability, and remain difficult to attribute. A threat is hybrid if it is part of a concerted set of mutually reinforcing actions. Hybrid threat campaigns are long-term and of varying intensity over time [70,116]. As a critical domain for economy, resources, trade, transport, security, and defense, the maritime domain, including ports, finds itself a target of hybrid threats [105]. The fact that much of the (maritime) critical infrastructure is privately owned complicates the construction of a strong and coordinated response to hybrid threats [117,118].

Cyberattacks are one of the main vectors of hybrid threats [117,119], and GNSS spoofing would also seem to be an attractive attack vector [118]. Foreign direct investments to gain ownership of critical infrastructure or technology (e.g., ports, hardware and software companies that supply the maritime industry) are part of the arsenal [119,120].

Since 2016, the EU and NATO have been cooperating on hybrid threats and cybersecurity [121], with these two topics prominently figuring in a common set of proposals [122,123]. In relation to that cooperation, the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) was set up in April 2017 in Helsinki to encourage strategic dialogue and carry out research and analysis on hybrid threats [124]. To this end, common exercises and workshops are carried out [125]. Following a closer look at hybrid threats versus sea lines of communication, the Hybrid CoE recently published a Handbook on Maritime Hybrid Threats [126].

Due to their low-level and dispersed nature, hybrid threats can only be fully recognized by bringing together the information about occurrences of disruptions that individually may seem minor but are part of a larger whole, thereby creating situational awareness [70]. The sharing of information on disruptions is therefore crucial, just like it is the case for cyberattacks outside the hybrid context. For adequate business continuity, operators should develop a resilience against hybrid attacks. The EU plans to identify sectoral hybrid resilience baselines [70]—one sector would be the maritime. Sectorial approaches, including maritime, are proposed in several other EU policies [127,128]. Risk analysis and enhancing of the overall resilience of EU critical maritime infrastructure with regard to cyber and hybrid threats, among others, are slated for action in the updated EU Maritime Security Strategy Action Plan [64]. A proper defense against hybrid threats requires all-of-society awareness and resilience [118,129,130].

3.3.9. Environmental Pollution

According to research, the side effects of disasters caused by a hacked port system or deluded onboard ship system could include environmental threats. The key to the security of the waterways is agility and constant paradigm-shifting to out-manoeuvre those who want to damage or disrupt the maritime transportation system (MTS) [69,131]. One might expect that cybercriminals, terrorists,

and rogue states will, at some point, begin holding the environment to ransom—cyber-induced environmental pollution [2]. It is a possible scenario that hackers would over-ride ship systems in ports, open valves and initiate leaks, or dump hazardous materials, ballast water, fuel, or oil.

4. Discussion

Analyzing available resources, we may summarize that there are severe consequences posed by cybersecurity risks, ranging from ship accidents caused by hacking e-Navigation to massive operational and economic disruption, to a port or shipping companies' activities and business. Cybercrime is a growing threat to the shipping industry that may have severe repercussions, as the Maersk, COSCO, Austal, Carnival, and other incidents have demonstrated. The present security situation in regard to hybrid threats further exposes the risk. As per BIMCO [78], it is not a question of whether an organization will be affected by a cybersecurity incident, but of when. Perhaps the organization has already been affected without knowing it. It is the connectedness of multiple and diverse systems that exacerbates the cyber risks, and connectivity will only continue to increase—e.g., with the introduction of the Internet of Things (IoT) and 5G in the maritime domain [59,67,132]. Therefore, maintaining the operational safety of these systems is of paramount importance. There continue to be numerous advancements in the field of hardware and software network security with which cyber administrators need to keep up. Though with the increased demand of the internet, it is only going to become more difficult; therefore, IT managers of maritime specialty may become necessities.

The maritime sector has always focused on safety and security issues, such as aspects of seafarer safety, transport, and cargo security. Now, the essence of navigational safety and maritime security include building a significant security culture which needs to be developed even further to include the cyber and information security domain, *maritime cybersecurity*. Maritime cybersecurity includes people, technologies, and processes capable of preventing cyber and information security breaches [73]. Hareide et al. [6] and Fitton et al. [133] note that maritime cybersecurity can be understood as a part of maritime security concerned with the protection from cyber threats of all aspects of maritime cyber systems that should include *technology*, *information*, and the *human* factor to understand and mitigate cyberattacks. Hasratyan et al. [59] mention the new concept of 'cyber seaworthiness' recently introduced in the shipping insurance industry.

Following the BIMCO 2020 survey [78], we found that there is room for improvement in regard to the *human* factor in maritime cybersecurity training that is seen by many as the first line of defense against the most common cyber incidents. The survey is quite encouraging, as 88% of respondents indicated that their company offers some sort of cybersecurity training; however, improvement is necessary, as only 22% of respondents received high-quality training. A 2020 ECSO report estimates that the maritime industry lacks 50,000 to 100,000 trained people in the cyber field [59]. It is a fact that cybersecurity training and awareness are paramount to the maritime industry. People need to be aware of the threats they encounter, not only on work IT systems but to their private devices as well. Training courses, refreshers, and adequate software protection should be offered and modified to fit the crews' needs. The crew on the ships might rotate quite often, meaning that seafarers potentially often use systems they are unfamiliar with, which might increase the potential for human error.

It was noted, concerning *technology* and *information*, that a shift in mind-set is essential to direct more attention and resources toward cybersecurity [134–136]. In the event of the worst scenario, appropriate contingency plans should be in place. Such plans should also include the use of alternative modes to ensure safe and reliable operations in the cyber non-secure environment [75,137]. Manufacturers should also improve the cybersecurity of their products, not leaving critical shipping systems vulnerable to cybercriminals [60].

National defense forces are already in the hunt for alternate position, navigating, and timing (PNT) systems (to GPS) within two years. Even though military commanders would prefer equipment that does not need to rely on GPS because their current systems are increasingly being jammed or spoofed, the costly GPS III program is going to be developed in the USA. It will be designed to include

improved anti-jam features, including the higher-fidelity M-Code signal for military users only [81]. In the meantime, the US Air Force is looking for solutions that could provide alternative signal sources that might even be from a non-US GNSS system. Lockheed U-2 high altitude reconnaissance jet pilots wear GPS-enabled smartwatches (Garmin D2 Charlie) for navigation backup in case their GNSS signal becomes unavailable [80]. Watches are capable of receiving multiple navigation signals including GPS, GLONASS, and BeiDou. Indeed, the combination of multiple GNSS systems in a smart receiver makes spoofing much more difficult, and now that Galileo is available worldwide, it is already used in over a billion smartphones [138]. The questions we might be asking here are

- Is it not a bit unusual that a superpower state does not have its alternative navigation system for their own defense forces in order not to rely on the signal sources of their rivals?
- Would it not be wise to develop and put into practice GPS-enabled smartwatches for mariners in case their GPS signal onboard becomes unavailable?
- Is there any viable non-GNSS alternative or backup system for vulnerable GPS navigation?

At this stage, we might find an answer only to the third question. IMO recognizes the need for multiple PNT systems onboard maritime vessels. However, there has been no widely available substitute system for GPS navigation, although, now Galileo is becoming a viable alternative. IMO has developed the e-Navigation concept to increase maritime safety and security via means of electronic navigation, based on (at least) two different independent sources of the PNT system to make it robust and fail-safe. The most viable terrestrial system providing PNT services that meets IMO's requirements an enhancement of LOng-RAnge Navigation (LORAN)—eLoran. Not precisely as accurate as GPS, it can provide sub-5 m (in the Netherlands) to sub-10 m (in the United Kingdom) horizontal positioning accuracy. It meets the availability, integrity, and continuity performance requirements for maritime harbor entrance and approach manoeuvres, aviation non-precision instrument approaches, land-mobile vehicle navigation, and location-based services [83–85].

Galileo offers the Public Regulated Service (PRS) which is encrypted to protect against spoofing [139]. However, that is only available for use by authorities. However, in the near future, it will offer (free) Open Service Navigation Message Authentication (OS NMA) that will provide a low level of protection against spoofing, and a (paid) Commercial Authentication Service (CAS) that is encrypted like PRS—but for commercial use—while also providing higher accuracy [140].

Perkovic et al. [37–39] presented an impressive laser-based aid system for berthing and docking that is providing accuracy within 2 cm even when the GNSS satellite signal is obstructed by Ship to Shore (STS) cranes, or redirected. This system could be one of the core subsystems required for collision avoidance [141,142] of autonomous surface vessels, which still require solutions for a variety of technical problems [113].

The answer to the third question could eventually come about by a public–private partnership. Humphreys [143] predicts that companies such as Elon Musk's SpaceX and Amazon's Project Kuiper, maintaining networks with hundreds of low-Earth-orbit satellites, will eventually become a vital component of the GNSS ecosystem. The new GNSS will pick up the slack in the event of malfunctions or attacks.

5. Conclusions

To summarize, the importance of cybersecurity has been recognized, and there will be a series of new cybersecurity openings in the future through which hackers can attack if systems are not adequately protected. It is expected that cybersecurity challenges will expand as autonomous ships will form a prominent piece of the future maritime landscape, underscoring the growing reliance on interconnected information systems [74]. New, unexpected circumstances may lead to increased cyber risks, as the year 2020 is now seeing with COVID-19, with reports of 400 percent increase in attempted hacks since February 2020 [144]. Moreover, the global security landscape that gives rise to hybrid threats is not expected to improve soon.

The maritime industry has shown that it is neither immune to cyberattacks nor completely prepared to combat the risks involved in using some obsolete or modern digital systems. Maintaining seaworthiness given the impact of digital technologies requires robust cybersecurity policy/strategies, cyber-secure maritime technology, a shift in mind-set, and new insurance offers that specifically cover maritime cyber risks. A modest beginning is to have the right people on board and have established trust between maritime stakeholders. A company under attack must have the confidence to share the information with others in the sector, allowing them to bolster their defenses.

GNSS signals are indispensable to safe and efficient navigation and are an integral component of maritime operations. To interfere with them jeopardizes maritime safety and security at sea. This paper demonstrates the GNSS vulnerabilities that impact many maritime systems. The use of multiple GNSS constellations (public and private), intelligent processing on the receiver side, and encrypted signals will in the near future provide increased robust defense against jamming and spoofing. The paper also recommends that the maritime community implement an eLoran system as a terrestrial augmentation to space-based GNSS capabilities. Terrestrial signals could be coded and authenticated, further increasing security and, subsequently, safeguarding GNSS satellites by making them less attractive targets. Locally, the positioning systems can be complemented by the harbor's laser-based aid system for berthing and docking, so that the regional shipping industry can be better protected from cyberattacks for the foreseeable future. As presented, building resilience against cybercriminals is a never-ending battle.

Author Contributions: Conceptualization, A.A. and I.P.; methodology, A.A. and T.B.; data collection, A.A., T.B., and I.P.; EU aspects, H.G.; validation, A.A., T.B., and I.P.; formal analysis, A.A. and I.P.; data curation, A.A., T.B., and I.P.; writing—original draft preparation, A.A.; internal review, H.G. All authors have read and agreed to the published version of the manuscript.

Funding: The authors acknowledge the financial support of the Slovenian Research Agency (research core funding No. P2-0394, Modelling and Simulations in Traffic and Maritime Engineering).

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

List of Acronyms

AtoN	Aids to Navigation
AIS	Automatic Identification System
BeiDou	China's BeiDou Navigation Satellite System
CERT-EU	Computer Emergency Response Team
cPPP	contractual Public-Private Partnership
CSIRT	Computer Security Incident Response Teams
ECDIS	Electronic Chart Display and Information System
EC3	European Cyber Crime Centre at Europol
eLORAN	Enhanced LOng-RAnge Navigation
EMODnet	European Marine Observation and Data Network
EMSA	European Maritime Safety Agency
ENISA	European Union Agency for Cybersecurity
ECSO	European Cyber Security Organisation
Galileo	European Union's GNSS
GLONASS	Russia's Global Navigation Satellite System
GNC	Guidance, Navigation and Control
GNSS	Global Navigation Satellite System
GPS, GPS/NAVSTAR	Global Positioning System (USA's GNSS)
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats
IEC	International Electrotechnical Commission
IMO	International Maritime Organization
INS	Integrated Navigational System
IoT	Internet of Things
ISAC	Information Sharing and Analysis Centres

ISAO	Information Sharing and Analysis Organizations
ISM Code	International Safety Management Code
IT	Information Technology
ITU	International Telecommunication Union
LORAN	LOng-RAnge Navigation
MSC	Maritime Safety Committee
MTS	Maritime Transportation System
NavIC	India's Navigation Indian Constellation
OT	Operational Technology
PC	Personal Computer
PNT	Positioning, Navigation and Timing
QZSS	Japan's Quazi-Zenith Satellite System
SCADA	Supervisory Control And Data Acquisition
SEG	SafeSeaNet Ecosystem Graphical Interface
SMS	Safety Management System
SOLAS	Safety Of Life At Sea
SSN Ecosystem GUI	The SafeSeaNet Ecosystem Graphical User Interface (GUI)
STS	Ship to Shore
TDM	Traffic Density Mapping
TEU	Twenty-foot equivalent unit
VDR	Voyage Data Recorder
VIP	Very Important Persons

References

1. World Economic Forum. Wild Wide Web—Consequences of Digital Fragmentation. *The Global Risks Report 2020*, 15th Ed. ed. January 2020. Available online: https://www.weforum.org/reports/the-global-risks-report-2020 (accessed on 20 June 2020).
2. Maritime Cyber-Attacks Increase by 900% in Three Years. Available online: https://www.marineinsight.com/shipping-news/maritime-cyber-attacks-increase-by-900-in-three-years/# (accessed on 20 July 2020).
3. Middleton, A. Hide and Seek: Managing Automatic Identification System Vulnerabilities: Proceedings of the Marine Safety and Security Council, Coast Guard. *J. Saf. Secur. Sea* **2014**, *71*, 48–50.
4. Chybowski, L.; Gawdzinska, K.; Laskowski, R. Assessing the Unreliability of Systems during the Early Operation Period of a Ship—A Case Study. *J. Mar. Sci. Eng.* **2019**, *7*, 213. [CrossRef]
5. Dobryakova, L.A.; Lemieszewski, L.S.; Ochin, E.F. GNSS spoofing detection using static or rotating single-antenna of a static or moving victim. *IEEE Access* **2018**, *6*, 79074–79081. [CrossRef]
6. Hareide, O.S.; Jøsok, Ø.; Lund, M.S.; Ostnes, R.; Helkala, K. Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *J. Navig.* **2018**, *71*, 1025–1039. [CrossRef]
7. Kaleem Awan, M.S.; Al Ghamdi, M.A. Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS). *J. Mar. Sci. Eng.* **2019**, *7*, 350. [CrossRef]
8. Lee, E.; Mokashi, A.J.; Moon, S.Y.; Kim, G. The Maturity of Automatic Identification Systems (AIS) and Its Implications for Innovation. *J. Mar. Sci. Eng.* **2019**, *7*, 287. [CrossRef]
9. Polatidis, N.; Pavlidis, M.; Mouratidis, H. Cyber-attack path discovery in a dynamic supply chain maritime risk management system. *Comput. Stand. Interfaces* **2018**, *56*, 74–82. [CrossRef]
10. Kalogeraki, E.; Apostolou, D.; Polemi, N.; Papastergiou, S. Knowledge management methodology for identifying threats in maritime/ logistics supply chains. *Knowl. Manag. Res. Pract.* **2018**, *16*, 508–524. [CrossRef]
11. Kessler, G.C.; Craiger, J.P.; Haass, J.C. A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System. *Trans. Nav. Int. J. Mar. Navig. Safety Sea Trans.* **2018**, *12*, 429–437. [CrossRef]
12. Lee, Y.C.; Park, S.K.; Lee, W.K.; Kang, J. Improving cybersecurity awareness in maritime transport: A way forward. *J. Korean Soc. Mar. Eng.* **2017**, *41*, 738–745.
13. Lewis, S.; Maynard, L.; Chow, C.E.; Akos, D. Secure GPS Data for Critical Infrastructure and Key Resources: Cross-Layered Integrity Processing and Alerting Service. *Navig. J. Inst. Navig.* **2018**, *65*, 389–403. [CrossRef]

14. Shapiro, L.R.; Maras, M.-H.; Velotti, L.; Pickman, S.; Wei, H.-L.; Till, R. Trojan horse risks in the maritime transportation systems sector. *J. Trans. Secur.* **2018**, *8*, 1–19. [CrossRef]
15. Svilicic, B.; Brčić, D.; Žuškin, S.; Kalebić, D. Raising Awareness on Cyber Security of ECDIS. *TransNav Int. J. Mar. Navig. Saf. Sea Trans.* **2019**, *13*, 231–236. [CrossRef]
16. Svilicic, B.; Kamahara, J.; Celic, J.; Bolmsten, J. Assessing Ship Cyber Risks: A Framework and Case Study of ECDIS Security. *WMU J. Mar. Aff.* **2019**, *18*, 509–520. [CrossRef]
17. Svilicic, B.; Kamahara, J.; Rooks, M.; Yano, Y. Maritime Cyber Risk Management: An Experimental Ship Assessment. *J. Navig.* **2019**, *72*, 1108–1120. [CrossRef]
18. Svilicic, B.; Rudan, I.; Frančić, V.; Mohović, Đ. Towards a Cyber Secure Shipboard Radar. *J. Navig.* **2019**, *73*. [CrossRef]
19. Tam, K.; Jones, K. MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU J. Mar. Aff.* **2019**, *18*, 129–163. [CrossRef]
20. Tsimplis, M.; Papadas, S. Information Technology in Navigation: Problems in Legal Implementation and Liability. *J. Navig.* **2019**, *72*, 833–849. [CrossRef]
21. Zăgan, R.; Raicu, G.; Pazara, R.H.; Enache, S. Realities in Maritime Domain Regarding Cyber Security Concept. *Adv. Eng. Forum* **2018**, *27*, 221–228. [CrossRef]
22. Assessing the Cyber Risks of Maritime Navigation. Available online: https://www.kennedyslaw.com/media/3288/kennedys_assessingthecyberrisksofmaritimenavigation.pdf (accessed on 20 May 2020).
23. Lessons Learned from Maritime License to Operate at Risk? Available online: https://www.kongsberg.com/digital/resources/stories/2019/10/maritime-license-to-operate-at-risk/ (accessed on 4 July 2020).
24. ISO. Information Technology—Security Techniques—Guidelines for Cybersecurity. ISO/IEC 27032:2012, 07/2012. Available online: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en (accessed on 24 August 2020).
25. International Telecommunication Union. Overview cybersecurity. In *ITU-T X.1205 Recommendation*; International Telecommunication Union: Geneva, Switzerland, 2008; p. 2.
26. European Commission. *Cybersecur. Eur. Digit. Single Mark.* **2017**, *2*, 13. [CrossRef]
27. Maritime-License-to-Operate-at-Risk-KPMG-and-KONGSBERG.Pdf. Available online: https://assets.kpmg/content/dam/kpmg/no/pdf/2019/09/Maritime-license-to-operate-at-risk-KPMG-and-KONGSBERG.pdf (accessed on 2 August 2020).
28. Jensen, L. Challenges in Maritime Cyber-Resilience. *Technol. Innov. Manag. Rev.* **2015**, *5*, 35–39. [CrossRef]
29. Code of Practice - Cyber Security for Ships. Available online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf (accessed on 22 June 2020).
30. Babineau, G.; Jones, R.; Horowitz, B. A System-Aware Cyber Security Method for Shipboard Control Systems with a Method Described to Evaluate Cyber Security Solutions. In Proceedings of the 2012 IEEE Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 13–15 November 2012; pp. 99–104. [CrossRef]
31. Masala, C.; Tsetsos, K.A. Cyber risks and threats: Demanding challenge for the maritime industry. In *Look Out 2016 Maritime Domain Cyber: Risks, Threats & Future Perspectives*; Lampe & Schwartze KG: Bremen, Germany, 2015; pp. 11–26.
32. Glomsvoll, O.; Bonenberg, L. GNSS Jamming Resilience for Close to Shore Navigation in the Northern Sea. *J. Navig.* **2017**, *70*, 33–48. [CrossRef]
33. Direnzo, J.; Goward, D.A.; Roberts, F.S. The Little-Known Challenge of Maritime Cyber Security. In Proceedings of the 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA), Corfu, Greece, 6–8 July 2015; pp. 1–5. [CrossRef]
34. Ziebold, R.; Romanovas, M.; Gewies, S. Experimental Evaluation of the Impact of Jamming on Maritime Navigation. In Proceedings of the 29th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2016), Portland, OR, USA, 12–16 September 2016; pp. 3461–3480. [CrossRef]
35. Thombre, S.; Bhuiyan, M.Z.H.; Eliardsson, P.; Gabrielsson, B.; Pattinson, M.; Dumville, M.; Fryganiotis, D.; Hill, S.; Manikundalam, V.; Pölöskey, M.; et al. GNSS threat monitoring and reporting: Past, present, and a proposed future. *J. Navig.* **2018**, *71*, 513–529. [CrossRef]
36. Elsobeiey, M.E. Accuracy Assessment of Satellite-Based Correction Service and Virtual GNSS Reference Station for Hydrographic Surveying. *J. Mar. Sci. Eng.* **2020**, *8*, 542. [CrossRef]

37. Perkovic, M.; Gucma, M.; Luin, B.; Gucma, L.; Brcko, T. Accommodating larger container vessels using an integrated laser system for approach and berthing. *Microprocess. Microsyst.* **2017**, *52*, 106–116. [CrossRef]
38. Perkovič, M.; Gucma, L.; Bilewski, M.; Muczynski, B.; Dimc, F.; Luin, B.; Vidmar, P.; Lorenčič, V.; Batista, M. Laser-Based Aid Systems for Berthing and Docking. *J. Mar. Sci. Eng.* **2020**, *8*, 346. [CrossRef]
39. Gucma, L.; Bak, A.; Jankowski, S.; Zalewski, P.; Perkovic, M. Laser docking system integrated with Pilot Navigation Support System, a background to high precision, fast and reliable vessel docking. In Proceedings of the 17th Saint Petersburg International Conference on Integrated Navigation Systems, St. Petersburg, Russia, 31 May–2 June 2010.
40. Mileski, J.; Clott, C.; Galvao, C.B. Cyberattacks on Ships: A Wicked Problem Approach. *Marit. Bus. Rev.* **2018**, *3*, 414–430. [CrossRef]
41. Tranfield, D.; Denyer, D.; Smart, P. Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review* Introduction: The Need for an Evidence-Informed Approach. *Br. J. Manag.* **2003**, *14*, 207–222. [CrossRef]
42. Grant, M.J.; Booth, A. A Typology of Reviews: An Analysis of 14 Review Types and Associated Methodologies. *Health Inf. Libr. J.* **2009**, *26*, 91–108. [CrossRef]
43. Milner, K.A. Systematic Reviews. *Oncol. Nurs. Forum* **2015**, *42*, 89–93. [CrossRef]
44. Perkovič, M. *AIS Spoofing Near Elba Island Analysis and Research Data*; University of Ljubljana, Faculty of Maritime Studies and Transport: Ljubljana, Slovenia, 2020.
45. Bansal, M.; Kaur, J.; Kaur, A.; Raina, C.K. Cyber Security: Impact and Preventions. *IJSRCSEIT* **2017**, *2*, 1096–1100.
46. The Risk of Cyber-Attack to the Maritime Sector. Glob. Mar. Pract. Available online: https://www.marsh.com/uk/insights/research/the-risk-of-cyber-attack-to-the-maritime-sector.html (accessed on 26 June 2020).
47. IMO Resolution MSC.428 (98). 2017. Available online: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf (accessed on 20 May 2020).
48. ISM. *International Safety Management Code*; IMO Publishing: London, UK, 2018.
49. Guidelines on Cyber Risk Management. Maritime Safety Committee: 2017, MSC-FAL (1/Circ.3). pp. 1–6. Available online: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf (accessed on 16 July 2020).
50. The Guidelines of Cyber Security Onboard Ships (2018). Available online: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships (accessed on 15 May 2020).
51. International Electrotechnical Commission. *Maritime Navigation and Radiocommunication Equipment and Systems-Cybersecurity-General Requirements, Methods of Testing and Required Test. Results*; IEC 63154 ED1; IEC: Geneva, Switzerland, 2019.
52. European Commission; High Representative. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN(2013) 1 final, Brussels. 7 February 2013. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013JC0001 (accessed on 15 July 2020).
53. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA. Available online: https://eur-lex.europa.eu/legl-content/EN/ALL/?uri=CELEX:32013L0040 (accessed on 15 July 2020).
54. Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union (NIS Directive). Available online: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (accessed on 15 July 2020).
55. European Commission. Communication Making the Most of NIS—towards the Effective Implementation of Directive (EU) 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union. COM(2017) 476 final/2, Brussels. 4 October 2017. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:476:FIN (accessed on 15 July 2020).
56. European Commission. Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry. COM(2016) 410 final, Brussels. 5 July 2016. Available online: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2016:0410:FIN (accessed on 15 July 2020).
57. ENISA. Information Sharing and Analysis Centres (ISACs)—Cooperative Models. Available online: https://doi.org/10.2824/549292 (accessed on 17 July 2020).

58. What is an ISAC or ISAO? How These Cyber Threat Information Sharing Organizations Improve Security. Available online: https://www.csoonline.com/article/3406505/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html (accessed on 8 September 2020).
59. Hasratyan, N.; Olesen, N. Transportation Sector Report—Cyber Security for Road, Rail, Air, and Sea. European Cyber Security Organisation. Available online: https://www.ecs-org.eu/documents/publications/5e78cb9869953.pdf (accessed on 17 July 2020).
60. European Commission; High Representative. Joint Communication on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. JOIN(2017) 450 final, Brussels. 13 September 2017. Available online: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52017JC0450 (accessed on 17 July 2020).
61. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Available online: https://eur-lex.europa.eu/eli/reg/2019/881/oj (accessed on 17 July 2020).
62. Council of the EU. European Union Maritime Security Strategy. 11205/14, Brussels. 24 June 2014. Available online: http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2011205%202014%20INIT (accessed on 17 July 2020).
63. Council of the EU. European Union Maritime Security Strategy Action Plan. 17002/14, Brussels. 16 December 2014. Available online: https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf (accessed on 17 July 2020).
64. Council of the EU. Revised European Union Maritime Security Strategy (EUMSS) Action Plan. Annex to 10494/18, Brussels. 26 June 2018. Available online: https://data.consilium.europa.eu/doc/document/ST-10494-2018-INIT/en/pdf (accessed on 17 July 2020).
65. European Commission; High Representative. On the implementation of the EU Maritime Security Strategy Action Plan. Joint Staff Working Document SWD(2016)217 Final. Available online: https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/swd-2016-217_en.pdf (accessed on 17 July 2020).
66. European Commission; High Representative. Second report on the implementation of the EU Maritime Security Strategy Action Plan. Joint Staff Working Document SWD(2017)238 Final. Available online: https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/swd-2017-238_en.pdf (accessed on 17 July 2020).
67. European Commission; High Representative. Report on the implementation of the revised EU maritime security strategy action plan. In *Joint Staff Working Document*; European Commission: Brusselsl, Belgium, 2020; in draft.
68. European Union Agency for Cybersecurity. *Port Cybersecurity—Good Practices for Cybersecurity in the Maritime Sector*; ENISA: Athens, Greece, 2019. [CrossRef]
69. Cimpean, D.; Meire, J.; Bouckaert, V.; Stijn, V.C.; Pelle, A.; Hellebooge, L. *Analysis of Cyber Security Aspects in the Maritime Sector*; ENISA: Athens, Greece, 2011.
70. European Commission. Communication on the EU Security Union Strategy. COM(2020) 605 Final. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0605 (accessed on 17 July 2020).
71. Council of the EU. Shaping Europe's Digital Future—Council Conclusions. 8711/20, Brussels. 9 June 2020. Available online: https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/en/pdf (accessed on 18 July 2020).
72. European Commission. Secure 5G Deployment in the EU—Implementing the EU Toolbox. COM(2020) 50 Final. Available online: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:0050:FIN (accessed on 18 July 2020).
73. Cyber and Information Security Strategy for the Maritime Sector 2019–2022. Available online: https://www.dma.dk/Documents/Publikationer/Cyber%20and%20Information%20Security%20Strategy%20for%20the%20Maritime%20Sector.pdf (accessed on 27 July 2020).
74. Modernized Maritime Industry Transports Cyber threats to Sea. Available online: https://www.csoonline.com/article/3410236/modernized-maritime-industry-transports-cyberthreats-to-sea.html (accessed on 27 July 2020).
75. Jones, K.; Tam, K.; Papadaki, M. Threats and Impacts in Maritime Cyber Security. *Eng. Technol. Ref.* **2016**, *1*. [CrossRef]

76. Caponi, S.; Belmont, K. Maritime Cybersecurity: A Growing Threat Goes Unanswered. *Intellect. Prop. Technol. Law J.* **2015**, *27*, 16.
77. Lagouvardou, S. Maritime Cyber Security: Concepts, Problems and Models. Master' Thesis, Technical University of Denmark, Copenhagen, Denmark, 2018. Available online: https://pdfs.semanticscholar.org/3158/103669fe46911b52e55dc7afe82237994036.pdf (accessed on 3 August 2020).
78. Safety at Sea and BIMCO cybersecurity white paper—IHS Markit 2020 Cyber Security Survey. Available online: https://ihsmarkit.com/info/0819/cyber-security-survey.html?utm_medium=website&utmsource=sas-news-article-1&utm_campaign=cyber-security-whitepaper (accessed on 20 May 2020).
79. Maritime Meets Cyber Security. Available online: https://www.maritime-executive.com/blog/maritime-meets-cyber-security (accessed on 3 August 2020).
80. Why Are U-2 Jet Pilots Wearing Garmin Satellite Navigation Smartwatches? Available online: https://arstechnica.com/gadgets/2020/03/why-are-u-2-jet-pilots-wearing-garmin-satellite-navigation-smartwatches/ (accessed on 30 April 2020).
81. SASC Wants Alternative GPS by 2023. Available online: https://breakingdefense.com/2020/06/sasc-wants-alternative-gps-by-2023/ (accessed on 29 July 2020).
82. Silgado, D.M. Cyber-Attacks: A Digital Threat Reality Affecting the Maritime Industry. *World Marit. Univ. Diss.* **2018**, 9–26.
83. Bartlett, S.; Offermans, G.; Shue, C. Enhanced Loran. A Wide-Area Multi-Application PNT Resiliency Solution. *GPS World* **2015**, *26*, 58–64.
84. Johnson, G.; Swaszek, P.; Hartnett, R.; Shalaev, R.; Wiggins, M. An Evaluation of eLoran as a Backup to GPS. In Proceedings of the 2007 IEEE Conference on Technologies for Homeland Security, Woburn, MA, USA, 16–17 May 2007; pp. 95–100. [CrossRef]
85. E-Loran: The PNT Technology Which Is More Accurate and Less Vulnerable—Sea News Global Maritime News. Available online: https://seanews.co.uk/features/e-loran-the-pnt-technology-which-is-more-accurate-and-less-vulnerable/ (accessed on 2 August 2020).
86. Kala, N.; Balakrishnan, M. Cyber Preparedness in Maritime Industry. *Int. J. Sci. Technol. Adv.* **2019**, *5*, 19–28.
87. New GPS' circle Spoofing' Moves Ship Locations Thousands of Miles—GPS World/SkyTruth/RNTF. Available online: https://www.gpsworld.com/new-gps-circle-spoofing-moves-ship-locations-thousands-of-miles/ (accessed on 3 August 2020).
88. Drougkas, A.; Sarri, A.; Kyranoudi, P.; Zisi, A. European Union Agency for Cybersecurity. *Port. Cybersecur. Good Pract. Cybersecur. Marit. Sect.* **2019**, 12–46.
89. EMSA. AIS spoofing incident. In Proceedings of the 6th HLSG for Governance of the Digital Maritime System and Services, Brussels, Belgium, 20 January 2020. Available online: https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=18913 (accessed on 14 May 2020).
90. Now Operational, BeiDou Could Conceal Cybersecurity Threat—Inside GNSS. Available online: https://insidegnss.com/now-operational-beidou-could-conceal-cybersecurity-threat/ (accessed on 3 August 2020).
91. Wilson, J. *China's Alternative to GPS and Its Implications for the United States*; U.S. China Economic and Security Review Commission: Washington, DC, USA, 2017.
92. Ship Automation/Control System—KONGSBERG. Available online: http://www.shippipedia.com/ship-automation-control-system/ (accessed on 4 August 2020).
93. IHS-BIMCO-Survey-Findings—Story in Numbers. Available online: https://cybersail.org/wp-content/uploads/2017/02/IHS-BIMCO-Survey-Findings.pdf (accessed on 4 August 2020).
94. The importance of Cyber Security Risk Management in Shipping. Available online: https://www.shippingandfreightresource.com/cyber-security-risk-management-in-shipping/# (accessed on 4 July 2020).
95. The Future of Maritime Cybersecurity. Available online: https://www.maritimecyberadvisors.com/l/the-future-of-maritime-cybersecurity2/ (accessed on 3 July 2020).
96. Detect and Address Cyber Risk in the Maritime Industry. Available online: https://home.kpmg/no/nb/home/campaigns/2019/10/detect-and-address-cyber-risks-in-the-maritime-industry.html (accessed on 10 November 2019).
97. Trimble, D.; Monken, J.; Sand, A. A Framework for Cybersecurity Assessments of Critical Port Infrastructure. In Proceedings of the 2017 International Conference on Cyber Conflict (CyCon US), Washington, DC, USA, 7–8 November 2017; pp. 1–7.

98. Svilicic, B.; Rudan, I.; Jugovi, A. A Study on Cyber Security Threats in a Shipboard Integrated Navigational System. *J. Mar. Sci. Eng.* **2019**, *7*, 364. [CrossRef]
99. Preparing for Cyber Battleships–Electronic Chart Display and Information System Security. Available online: https://www.nccgroup.com/uk/our-research/preparing-for-cyber-battleships-electronic-chart-display-and-information-system-security/ (accessed on 27 May 2020).
100. The Story You Aren't Being Told About Iran Capturing Two American Vessels. Available online: https://www.mintpressnews.com/the-story-you-arent-being-told-about-iran-capturing-two-american-vessels/212937/ (accessed on 21 May 2020).
101. Hackers Took 'Full Control' of a Container Ship's Navigation Systems for 10 Hours. 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 January 2020).
102. Shipping Must Confront Onboard Systems' Cyber Vulnerabilities. Available online: https://safetyatsea.net/news/2017/shipping-must-confront-onboard-systems-cyber-vulnerabilities/ (accessed on 21 January 2020).
103. Key Takeaways from 3 Recent Cyber Attacks in Shipping. Available online: https://www.dualog.com/blog/key-takeaways-from-3-recent-cyber-attacks-in-shipping (accessed on 24 July 2020).
104. Carnival Hit by Cyber Attack: Hackers Steal Personal Information of Cruise Giant's Passengers and Staff. Available online: https://www.thisismoney.co.uk/money/markets/article-8640269/Carnival-hit-ransomware-attack-Hackers-steal-passenger-information.html (accessed on 17 August 2020).
105. Filitz, J. Maritime port systems cyber security vulnerability. *NMIO Tech. Bull.* **2019**, *13*, 22–27.
106. Kramek, J. The critical infrastructure gap: US port facilities and cyber vulnerabilities. In *Federal Executive Fellows Policy Papers 16*; Brookings: Washington, DC, USA, 2013; pp. 414–430. [CrossRef]
107. Newberry, M.E. Maritime Critical Infrastructure Cyber Risk: Threats, Vulnerabilities, and Consequences. Proceedings of the Marine Safety and Security Council, Coast. Guard. *J. Saf. Secur. Sea* **2014**, *71*, 42–45.
108. Gunther, C. Design of maritime cybersecurity systems. In *Look Out 2016 Maritime Domain Cyber: Risks, Threats & Future Perspectives*; Lampe & Schwartze KG: Bremen, Germany, 2015; pp. 27–46.
109. Above Us Only Stars—Exposing GPS Spoofing in Russia and Syria. Available online: https://www.c4reports.org/aboveusonlystars (accessed on 27 July 2020).
110. Jie, H.; Presti, L.; Motella, B.; Pini, M. GNSS Spoofing Detection: Theoretical Analysis and Performance of the Ratio Test Metric in Open Sky. *ICT Express* **2016**, *2*, 37–40. [CrossRef]
111. Seized UK Tanker Likely 'Spoofed' by Iran. Available online: https://lloydslist.maritimeintelligence.informa.com/LL1128820/Seized-UK-tanker-likely-spoofed-by-Iran (accessed on 20 July 2019).
112. Traffic Density Mapping Service—Methodology. EMS—Ref. Ares (2019)4005069—24/06/2019. Available online: http://www.emsa.europa.eu/related-projects/tdms.html (accessed on 26 June 2020).
113. Autonomous Shipping Concepts. Available online: https://www.norclub.no/blog/autonomous-shipping-concepts/ (accessed on 7 January 2020).
114. Cyber risk and Cybersecurity Countermeasures Supplement. P & I Loss Prevention Bulletin-Vol.48_Full.Pdf. Available online: https://www.piclub.or.jp/wp-content/uploads/2020/05/Loss-Prevention-Bulletin-Vol.48_Full.pdf (accessed on 24 July 2020).
115. Cyber Awareness. Available online: https://www.american-club.com/files/cyber_awareness_comic.pdf (accessed on 4 July 2020).
116. Giannopoulos, G.; Smith, H.; Theocharidou, M. *The Landscape of Hybrid Threats—A conceptual Model*; Joint Research Centre, Centre of Excellence for Countering Hybrid Threats: Helsinki, Finland, 2020.
117. Savolainen, J. Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure—Weapons of Mass Disturbance (WMDi)? Hybrid CoE Working Paper 4. Available online: https://www.hybridcoe.fi/publications/hybrid-threats-and-vulnerabilities-of-modern-critical-infrastructure-weapons-of-mass-disturbance-wmdi/ (accessed on 10 August 2020).
118. Kremidas-Courtney, C. Countering Hybrid Threats in the Maritime Environment. Center for International Maritime Security. Available online: http://cimsec.org/countering-hybrid-threats-in-the-maritime-environment/36553 (accessed on 12 June 2020).
119. European Commission; High Representative. Increasing resilience and bolstering capabilities to address hybrid threats. JOIN(2018) 16 Final. Available online: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2018:16:FIN (accessed on 15 June 2020).

120. Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 Establishing a Framework for the Screening of Foreign Direct Investments Into the Union. Available online: https://eur-lex.europa.eu/eli/reg/2019/452/oj (accessed on 15 June 2020).
121. Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. Warsaw. 8 July 2016. Available online: https://www.consilium.europa.eu/en/press/press-releases/2016/07/08/eu-nato-joint-declaration/ (accessed on 2 August 2020).
122. EU; NATO. Common Set of Proposals for the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization. Available online: https://data.consilium.europa.eu/doc/document/ST-15283-2016-INIT/en/pdf (accessed on 2 August 2020).
123. EU; NATO. Common Set of New Proposals on the Implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission and the Secretary General of the North Atlantic Treaty Organization. Available online: https://www.consilium.europa.eu/media/31947/st14802en17.pdf (accessed on 2 August 2020).
124. What is Hybrid CoE? The European Centre of Excellence for Countering Hybrid Threats. Available online: https://www.hybridcoe.fi/what-is-hybridcoe/ (accessed on 9 September 2020).
125. Hybrid Threats Against Harbours: Workshop at EDA. Available online: https://www.eda.europa.eu/info-hub/press-centre/latest-news/2018/05/30/hybrid-threats-against-harbours-workshop-at-eda (accessed on 9 September 2020).
126. Lohelia, T.; Schatz, V. Handbook On Maritime Hybrid Threats—10 Scenarios and Legal Scans. Hybrid CoE Working Paper. Available online: https://www.hybridcoe.fi/publications/handbook-on-maritime-hybrid-threats-10-scenarios-and-legal-scans/ (accessed on 9 September 2020).
127. European Commission; High Representative. On the Implementation of the Joint Framework on Countering Hybrid Threats—A European Union Response. JOIN(2017) 30 Final. Available online: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52017JC0030 (accessed on 9 September 2020).
128. European Commission; High Representative. Joint Framework on Countering Hybrid Threats—A European Union Response. JOIN(2016) 18 Final. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016JC0018 (accessed on 9 September 2020).
129. Braw, E. From Schools to Total Defence Exercises: Best Practices in Greyzone Deterrence. Available online: https://rusi.org/sites/default/files/20191115_newsbrief_vol39_no10_braw_web.pdf (accessed on 6 September 2020).
130. Council of the EU. Complementary Efforts to Enhance Resilience and Counter Hybrid Threats. Council Conclusions, 14972/19. Available online: https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf (accessed on 4 August 2020).
131. Radgowski, J.; Tiongson, K. Cyberspace—The Imminent Operational Domain. Proceedings of the Marine Safety and Security Council. *Coast. Guard J. Saf. Secur. Sea* **2014**, *71*, 18–22.
132. Jaskolka, J.; Villasenor, J. Securing cyber-dependent maritime systems and operations. *NMIO Tech. Bull.* **2017**, *12*, 4–6.
133. Fitton, O.; Prince, D.; Germond, B.; Lacy, M. *The Future of Maritime Cyber Security*; Lancaster University: Lancashire, UK, 2015.
134. Secretary of the Navy: Cybersecurity Readiness Review. Available online: https://www.navy.mil/strategic/CyberSecurityReview.pdf (accessed on 27 July 2020).
135. Tam, K.; Jones, K. Factors Affecting Cyber Risk in Maritime. In 2019 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA). *IEEE* **2019**, *3*, 1–8.
136. Navy Culture Must Be Adapted to Fit the Information Age. Available online: http://cimsec.org/navy-culture-must-be-adapted-to-fit-the-information-age/40594 (accessed on 27 July 2020).
137. Naval Dome—Maritime Cyber Defense Solution. Available online: https://navaldome.com/aapa-video-2020-07.html (accessed on 24 July 2020).
138. GSA Celebrates 1 Billion Galileo Smartphone Users. Available online: https://www.gsa.europa.eu/newsroom/news/gsa-celebrates-1-billion-galileo-smartphone-users (accessed on 8 September 2020).
139. PRS. Available online: https://www.gsa.europa.eu/security/prs (accessed on 8 September 2020).

140. How do We Ensure GNSS Security Against Spoofing? Available online: https://www.gpsworld.com/how-do-we-ensure-gnss-security-against-spoofing (accessed on 8 September 2020).
141. Van Cappelle, L.E.; Chen, L.; Negenborn, R.R. Survey on Short-Term Technology Developments and Readiness Levels for Autonomous Shipping. In *Computational Logistics*; Cerulli, R., Raiconi, A., Voß, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2018.
142. Spange, J. Autonomous Docking for Marine Vessels Using a Lidar and Proximity Sensors. Ph.D. Thesis, Norwegian University of Science and Technology, Trondheim, Norway, 2016.
143. How Vulnerable is, G.P.S.? Available online: https://www.newyorker.com/tech/annals-of-technology/how-vulnerable-is-gps (accessed on 6 August 2020).
144. Maritime Cyberattacks Up by 400 Percent. Available online: https://maritime-executive.com/article/report-maritime-cyberattacks-up-by-400-percent (accessed on 20 September 2020).