

2022-03-07

# Cybersecurity Challenges in the Maritime Sector

Akpan, F

<http://hdl.handle.net/10026.1/18991>

---

10.3390/network2010009

Network




MDPI AG

---

*All content in PEARL is protected by copyright law. Author manuscripts are made available in accordance with publisher policies. Please cite only the published version using the details provided on the item record or document. In the absence of an open licence (e.g. Creative Commons), permissions for further reuse of content should be sought from the publisher or author.*

Review

# Cybersecurity Challenges in the Maritime Sector

Frank Akpan <sup>1</sup>, Gueltoum Bendiab <sup>2</sup>, Stavros Shiaeles <sup>1,3,\*</sup>, Stavros Karamperidis <sup>4</sup>  
and Michalis Michaloliakos <sup>5</sup>

<sup>1</sup> Cyber Security Research Group, University of Portsmouth, Portsmouth PO1 2UP, UK; Frank.Akpan1@myport.ac.uk

<sup>2</sup> Department of Electronic, Faculty of Sciences of Technology, University of Freres Mentouri, Constantine 25000, Algeria; bendiab.kelthoum@umc.edu.dz

<sup>3</sup> Faculty of Pure & Applied Sciences, Open University of Cyprus, Nicosia 2220, Cyprus

<sup>4</sup> Department of International Shipping, Plymouth Business School, University of Plymouth, Logistics and Operations, Cookworthy Building, Drake Circus, Room 321, Plymouth PL4 8AA, UK; stavros.karamperidis@plymouth.ac.uk

<sup>5</sup> TMS Cardiff Gas, Marousi, 151 24 Athens, Greece; mmichaloliakos@tms-management.org

\* Correspondence: stavros.shiaeles@port.ac.uk

**Abstract:** Cyberattacks have been rapidly increasing over the years, resulting to big financial losses to businesses for recovery, regulatory sanctions, as well as collateral damages, such as reputation and trust. In this respect, the maritime sector, which until now was considered safe due to the lack of Internet connectivity and the isolated nature of ships in the sea, is showing a 900% increase in cybersecurity breaches on operational technology as it enters the digital era. Although some research is being conducted in this area, maritime cybersecurity has not been deeply investigated. Hence, this paper provides a close investigation of the landscape of cybersecurity in the maritime sector with the aim of highlighting security problems and challenges. First, it explores the systems available on ships that could be targeted by attackers, their possible vulnerabilities that an attacker could exploit, the consequences if the system is accessed, and actual incidents. Then, it describes and analyses possible mitigation actions that can be utilised in advance to prevent such attacks. Finally, several challenges and open problems are discussed for future research.



**Citation:** Akpan, F.; Bendiab, G.; Shiaeles, S.; Karamperidis, S.; Michaloliakos, M. Cybersecurity Challenges in the Maritime Sector. *Network* **2022**, *2*, 123–138. <https://doi.org/10.3390/network2010009>

Academic Editor: Alberto Gotta

Received: 30 November 2021

Accepted: 28 February 2022

Published: 7 March 2022

**Publisher's Note:** MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



**Copyright:** © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

**Keywords:** maritime; ships; cybersecurity; vulnerabilities; cybercriminals

## 1. Introduction

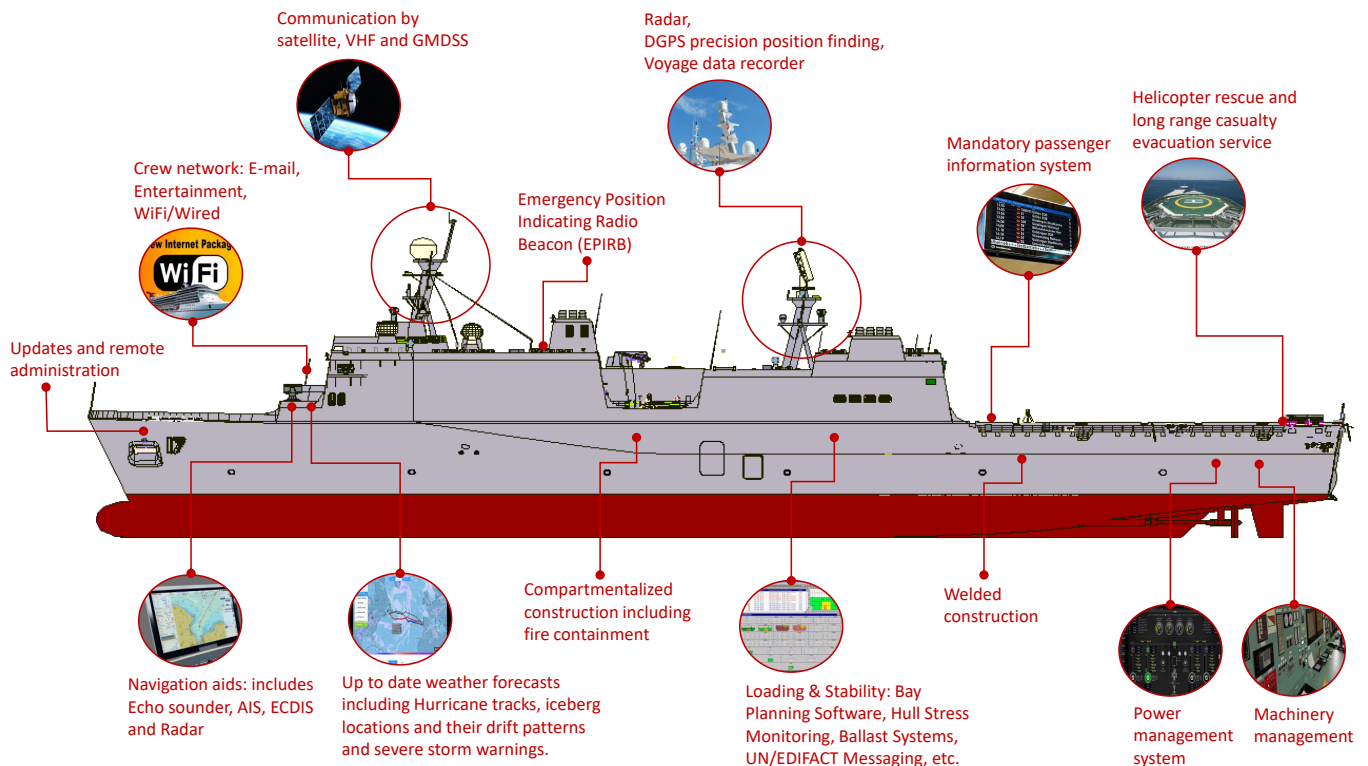
Today's global maritime sector is increasingly reliant on digitalisation, operational integration, and automation [1,2]. Leading shipbuilders and operators seek to innovate by utilizing cutting-edge technologies and systems that go beyond traditional designs to create ships with advanced remote control, communication, and connectivity capabilities [3]. Those capabilities are tested through various autonomous vessel projects. Mayflower was the first fully autonomous vessel that attempted to cross the Atlantic Ocean by using Artificial Intelligence (AI) technology and the energy from the Sun [4]. The vessel failed in its first attempt to cross the Atlantic, but it will try to sail across the Atlantic again this year. The Nippon Foundation will also test the first fully autonomous long-range commercial sail by February 2022 [5]. Autonomous vessels and modern ships contain a fleet of sensors (e.g., radar, LiDAR, high-definition cameras, thermal imaging, sonar, etc.) and many Operational Technology (OT) systems, which are interconnected with each other to give the ship's AI a precise combined image of the surrounding environment [6,7]. Their levels of automation can progress from fully manned ships to partially operated, remotely operated, partially autonomous, and fully autonomous unmanned ships [6,8]. The adoption of Information and Communications Technology (ICT) in the shipping industry is certainly accompanied by an explosion of cyber risks, with existing risks being increased and new risks being introduced [9]. Therefore, ensuring the safety and security of an autonomous ship cannot be ensured, and it is not possible to rely on previous system knowledge [2,3,6]. Instead, it

necessitates a novel security approach, which considers all of the various systems onboard and onshore, as well as how they interact [2,3,9,10].

According to the European Directive “EU 2016-679”, cyber-enabled ships are among the most critical infrastructures that already rely heavily on digital services, while malicious disruption of their operations can lead to financial and environmental damage or even endanger human safety [7]. Although some research is being conducted in this area [2,3,6,9,11], maritime cybersecurity has not been deeply investigated. In this paper, we first identify security issues and threats that the modern shipping industry is facing, especially those targeting the systems available on ships. Then, we describe possible mitigation actions that can be utilised in advance to prevent such attacks, and finally, we discuss several challenges and open problems for future research. The remainder of this article is structured as follows: the next section (Section 2) provides the background of the main systems available on modern and autonomous ships that could be targeted by attackers, while Section 3 presents the possible vulnerabilities and major security threats of these systems. Section 4 presents and discusses actual reported incidents in the last few years. Available security countermeasures and possible mitigation actions are discussed in Section 5, and finally, Section 6 concludes the paper and outlines directions for future research.

## 2. Background on Ship Automation Systems

Modern and autonomous ships are equipped with a variety of complex automated systems that have made the sea a much safer place than before [3]. However, some of these systems are often insecure and vulnerable to attack because they are considered less critical to security and performance [11]. As shown in Figure 1, these systems include navigation systems, radio detection and ranging (radar), Automatic Identification Systems (AISs), communications systems, and control systems for the wide range of electromechanical systems on board ships, such as the main engine, generators, converter drives, etc. [3,12].



**Figure 1.** Automation systems for modern and autonomous ships [13].

Navigation systems include the Electronic Chart Display and Information System (ECDIS), the Global Positioning System (GPS), and the Global Navigation Satellite Sys-

tem (GNSS). GPS and GNSS are crucial enablers for modern and autonomous shipping worldwide [14]. Satellite positioning can be used in conjunction with other situational awareness systems that provide relative positioning information for decision-making [11]. The Automatic Identification System (AIS) is a radio broadcasting system that operates on both ships and shores. It is used for vessel traffic monitoring and assistance and to notify port and maritime authorities of the ship's location. It is also very useful for accident investigation, search and rescue operations, and weather forecasting [11,15]. In fact, the ability to rely on transmitted data is crucial to maintain situational awareness and avoid collisions at sea. ECDIS is an integrated electronic navigation system that combines the data obtained from a number of electronic navigation sensors, such as GPS, radar, and AIS, and displays it in the form of a graphic image [12]. The International Maritime Organization (IMO) requires all commercial vessels to have ECDIS, which is typically installed on the bridge [11]. Radio detection and ranging (radar) is also a crucial system for modern ships because it provides valuable information about the ship's surroundings and also detects physical objects using radio waves, e.g., microwaves in the electromagnetic spectrum [16].

In order to ensure high-speed data transmission rates throughout naval operations, most modern ships and vessels are equipped with the Maritime Very Small Aperture Terminal (VSAT), which acts as a ground station for the satellite to transmit and receive data from the antenna. The transceiver is mounted above the deck to align with the satellite view, and the control unit is located beneath the deck and serves as the computer's interface [17]. VSAT offers a variety of communication and security services such as ECDIS, AIS, telephone, Internet, cargo handling, wireless integration, crew welfare, and weather forecasting. The modern shipping industry is also seeing an increase in demand for automated intelligent video surveillance systems to monitor transport operations, especially in large storage areas, generators, and large vessels carrying valuable cargo [12].

In addition, shipping and maritime industries are heavily dependent on Shipboard Industrial Control Systems (ICSs) and IT network systems [3,12]. ICSs help to quickly collect and aggregate security and operational data from the entire ship's control and automation systems. It monitors temperature, pressure, level, viscosity, flow control, speed, torque, voltage, current, and machinery and equipment status on board in order to maintain safety and operational reliability and to keep up with an evolving threat landscape [18,19].

The Global Maritime Distress System (GMDSS) [20], propulsion control system [21], Integrated Bridge Systems (IBSs), machinery management [22], and power control systems [23] are other key features of the automation systems on board a ship that play an increasingly important role in facilitating the smooth, safe, and efficient operation of the ship. As the complexity, digitalisation, and automation of systems in the maritime industry increase, modern ships and vessels are confronted with an increasing number of new challenges related to the security and data protection of IT systems on board ships [3,6,24]. Recently, several cybercrime cases have been reported in the maritime industry, while others remain unknown as shipowners are not willing to report them for potential reputational damage [24]. Potential threats to the security and privacy of shipboard IT systems are discussed in the next section, along with actual incidents of cyberattacks against these systems.

Table 1 presents a summary of the main automation systems in modern and autonomous ships and their uses. All these systems represent attack surfaces that malicious actors can exploit in order to get unauthorized access to the Ship, which is the topic discussed in the next section.

**Table 1.** A summary of the main automation systems in modern and autonomous ships.

Systems	USE
Automatic Identification System (AIS)	<ul style="list-style-type: none"> <li>- Vessel traffic monitoring and assistance</li> <li>- Avoid a collision</li> <li>- Notify ports and maritime authorities of the ship's location</li> <li>- Calculate the distance between the ship and the other ships</li> <li>- Ensure sea safety by monitoring traffic</li> <li>- Accident investigation and search and rescue operations</li> </ul>
Electronic Chart Display Information System (ECDIS)	<ul style="list-style-type: none"> <li>- Collect and combine data from electronic navigation sensors</li> <li>- Shows the position of the ship in real time</li> </ul>
GPS and GNSS	<ul style="list-style-type: none"> <li>- Displays the position of the ship</li> <li>- Displays the speed</li> <li>- Displays the route and time</li> </ul>
Radar	<ul style="list-style-type: none"> <li>- Provides information about the ship's surroundings</li> <li>- Detection of the position and speed of objects</li> </ul>
Global Maritime Distress System (GMDSS)	<ul style="list-style-type: none"> <li>- Broadcast the distress messages related to safety issues</li> <li>- Sending and receiving critical safety alerts</li> </ul>
Global Industrial Control Systems (ICSs)	<ul style="list-style-type: none"> <li>- Assist in reducing human errors</li> <li>- Increase resource productivity</li> <li>- Extend the life of the equipment</li> <li>- Control and monitor parameters on board a ship</li> </ul>
Very Small Aperture Terminal (VSAT)	<ul style="list-style-type: none"> <li>- Uses a satellite network to send and receive data</li> <li>- Offer a variety of communication and security services</li> </ul>
Propulsion and machinery management and power control systems	<ul style="list-style-type: none"> <li>- Monitor and regulate onboard machinery</li> <li>- Monitor and regulate propulsion</li> <li>- Monitor and regulate steering</li> </ul>
Video Surveillance System	<ul style="list-style-type: none"> <li>- Monitor transport operations in large storage areas</li> <li>- Monitor transport operations in large vessels</li> </ul>
IT Network Systems	<ul style="list-style-type: none"> <li>- Used for internal/external processes to send, receive, and store data</li> <li>- Used for crew welfare</li> <li>- Used for crew personal devices (BYOD)</li> </ul>

### 3. Cyberattacks on the Ship Automation Systems

The extensive utilisation of automation and IT systems in modern ships provides new opportunities for hackers and malicious actors to implement different cyberattacks that could lead to catastrophic incidents and cause major safety losses [3,6,24]. Extensive research efforts have been made by the research community to identify vulnerabilities in the modern maritime industry [3,6,24–27], and many successful cybercrime cases have been reported in the last few years [24,25]. According to [24], the main common motivations for these attacks are to gain remote control over ships and vessels, to steal important and confidential information that can be used for launching further attacks, or to disrupt the ship's operations by corrupting important components and making the automated systems unavailable. In fact, most of the IT systems in modern ships are insecure and vulnerable to attack because they are considered less critical to security and performance [6]. In this section, we investigate cyberattacks on modern and autonomous ships based on the already hacked automation systems and actual incidents.

#### 3.1. Automatic Identification System

The AIS transponders communicate over the air without any authentication or integrity checks, which allows hackers to use it to spread fake messages [24]. As stated in [11], software-defined radio is used by attackers to instigate fake "man-in-the-water" signals, making the ship unnoticed, and transmitting fake weather reports. Trusting in possibly inaccurate data can lead to poor choices and disastrous results. AIS data are also freely accessible to the public through websites such as Vessel Finder Limited

(<https://www.vesselfinder.com/>) and Marine Traffic [28]. In this context, the IMO criticised the disclosure of information about ships and their itineraries because this information can be very useful in the event of a targeted attack.

### 3.2. Global Position System

GPS and navigational technologies, which are actively used in the maritime sector, are specific goals of various cyberattack that aim to exploit design flaws to destabilise services that depend on these technologies [29]. Such attacks pose medium to high risks because, in addition to data and service protocol violations, there is the possibility of physical damage. Several attacks have been reported that attempted to exploit this set of technologies [30–32]. For instance, spoofed GPS signals enabled attackers to reroute a vessel without triggering an alarm or alert from system handling [30]. In a similar incident, GPS signal jamming in South Korea affected the signal reception of more than 1000 aircraft and 700 ships for more than a week. Such cyberattacks can be classified as medium to high difficulty and are the result of the designs and standards of GPS and navigation systems. According to [33], Satellite Communication Systems (SATCOMs), including those connecting vessels via the Internet with each other and with the mainland, contain a large number of vulnerabilities and critical security holes such as devices using unsecured or even undocumented protocols, factory-set-up accounts, the ability to exploit the password reset function, and backdoors.

### 3.3. Global Navigation Satellite System

One of the most interconnected systems is the Global Navigation Satellite System (GNSS). As a result, autonomous vessels that rely on improved satellite communications to transmit operational commands and sensor data may be at risk of cyberattacks [34], such as denial-of-service attacks, package changes, and man-in-the-middle attacks. Furthermore, low-power satellite signals have a significant technical disadvantage due to simple congestion. As a result, spoofing and jamming are considerable flaws that may represent high-cost and low-effort attacks [35,36]. Additionally, because many ship systems rely heavily on satellite position, GNSS failure can lead to the breakdown of other ship systems (e.g., AIS). Autonomous transportation systems must be capable of communicating with operational crews from ground crews, allowing cyberattacks to take full control of critical transport operations, allowing for a broader range of attacks and incentives for intruders [10,15].

### 3.4. Electronic Chart Display Information System

Security issues related to ECDIS have been deeply investigated in many studies [9,37–40]. In fact, there is a long list of flaws in ECDIS software implementations. The system is frequently run on old computers, which have no security updates available. The maps are downloaded from the Internet or manually uploaded via USB to the system, which may cause a compromise of the system while trying to update the maps. This update medium can open much room for attack [38]. The authors in [40] investigated ECDIS software and discovered several security flaws that could allow an attacker to delete or reinstall system files, as well as inject malicious content. As a result, altered sensor data can be sent to ECDIS to affect navigation judgements, thereby causing collisions [38,39].

### 3.5. Very Small Aperture Terminal

With the widespread use of VSAT in the modern maritime industry, some aspects of the VSAT network, such as the transparent transmission and the openness, need to be improved to counter security threats, especially unauthorised access and interception attacks [41]. In 2014, IOActive [42] tested several VSATs from different vendors and concluded that because they used plain text transmission with no authentication, encryption, security, or verification of personal information, all the tested devices were vulnerable at the implementation levels. As a result of the weak protection, attackers can send false signals or malicious code to the device to disable it or compromise the system, preventing the vessel from safely navigating. As reported in [41,42], AIS aggregators typically provide

ship location data. The real risk is that VSAT network interfaces can be found on the Internet using tools such as the Shodan Ship Tracker. This can reveal valuable and sensitive information such as brand names, product codes, and other data that could be used in cyberattacks. Standard information is typically available on vendors' websites, and many terminals continue to use the same factory settings, including the username and server password. An attacker can alter the GPS coordinates and settings, as well as download malicious software if he/she finds an open VSAT interface, and this enables further network hacking and provides access to critical management systems [43].

### 3.6. Radio Detection and Ranging

Although radar signals are more difficult to interrupt than satellites, they are still susceptible to interference and DDoS attacks from cyberattacks. In the event of a cyberattack, radar can provide false information about nearby objects due to false echoes caused by external radar waves. This incorrect information can cause ship collision accidents.

This incorrect information can cause the ship to collide with an object. It is important to note that while radar and other frequencies in the electromagnetic spectrum are susceptible to noise-based interference or more advanced spoofing attacks, the mechanisms to achieve the same effect vary significantly between systems [44].

### 3.7. Video Surveillance Systems

Video Surveillance Systems (VSSs) play a crucial role in the security and safety of vessels, cargo, and crew in all types of modern ships [45]. These systems are mainly used for monitoring and tracking the ship's critical operations and for protecting against attacks by terrorists and pirates [45,46]. However, VSSs have been recently found vulnerable to several cyberattacks, and a number of security issues have arisen [24,46]. For instance, researchers from Bitdefender found that two models of CCTV cameras, used in modern ships, are vulnerable to buffer overflow flaws. By exploiting this vulnerability, the researchers were able to track the activities of the hacked camera and overwrite passwords [46]. Moreover, this vulnerability can cause a VSS system crash or, worse, create an entry point for other cyberattacks [46].

### 3.8. Industrial Control Systems

Most industrial control systems have been designed and programmed in a manner that is independent of the security requirements, and data are transmitted in plain text [3,12]. Component security should be shared by vendors who maintain secure development structures and operators who configure components in accordance with industry standards and best practices. Either way, it often assumes the opponent's fault and takes no action, exposing many critical flaws for attackers to exploit [47]. Designers and operators of ICSs must understand the system's limitations, as well as the weaknesses of their components and protocols, as these are critical for the vessel's safety. The ship's distributed information technology network allows these control systems to communicate with one another. Continuous communication between the IT network and the website enables remote monitoring, troubleshooting, and debugging, while also lowering field travel costs and simplifying data collection and evaluation. One of the major concerns is that operators and engineers frequently disregard safety for the sake of convenience and efficiency, which can have far-reaching consequences throughout the whole shipping industry [48]. This conduct is caused by commercial pressure to save time and circumvent security policies [24,39,48].

### 3.9. IT Network Systems

Several types of networks are used in the maritime industry for the transmission of the data gathered and processed by networked information systems. Examples of these technologies include SHIPNET, SAFENET, C3I system, RICE 10, SHIP system 2000, Smart Ship, and TSCE [24]. These technologies have many security vulnerabilities because the design and configuration of communication links between IT networks pay little attention to authentication and encryption methods, resulting in potentially vulnerable and outdated

systems being available on the Internet. Actually, shipboard information technology systems are frequently linked to onshore facilities, increasing the risk of systematic and continual threats [49]. Financial pressures, legal requirements, and remote monitoring and management requirements increase the need for IT systems and network connectivity in the modern shipping industry; however, these systems will increase the size of the attack surface that security teams must defend [3,12,46] and create additional points of access that hackers could use to enter the ship's system. Therefore, vulnerabilities in these automated systems should be investigated carefully. Further, critical control networks must be isolated from the ship's IT and Internet networks in a secure area.

Moreover, the human factor becomes even more challenging with the complex interconnected ecosystem in the maritime sector. Therefore, a lack of a cybersecurity culture may be beneficial to any attacker that wants to gain access to a vessel and its systems, steal actual information, or disrupt the vessel's operations. Table 2 summarises the main vulnerabilities of modern and autonomous ship systems and their consequences.

**Table 2.** A summary of the main vulnerabilities of modern ship systems and their consequences.

Systems	Vulnerabilities	Consequences
Automatic Identification System (AIS)	<ul style="list-style-type: none"> <li>- Signal interference</li> <li>- False information sharing</li> <li>- Malware</li> <li>- Spoofing</li> <li>- No encryption</li> <li>- Signal jamming</li> </ul>	<ul style="list-style-type: none"> <li>- Ship hijacking</li> <li>- Destruction of data</li> <li>- Theft of valuable data</li> </ul>
Electronic Chart Display Information System (ECDIS)	<ul style="list-style-type: none"> <li>- Obsolete OSs</li> <li>- Insecure update mediums</li> </ul>	<ul style="list-style-type: none"> <li>- Loss of communication with the NS</li> <li>- Hijacking of a ship</li> <li>- Sensitive data theft</li> <li>- Compromising computers and OSs</li> </ul>
GNSS and GPS	<ul style="list-style-type: none"> <li>- Jamming attacks</li> <li>- Weak signal strength</li> <li>- Interference</li> <li>- Spoofing attacks</li> <li>- DoS/DDoS attacks</li> <li>- Packet modification</li> </ul>	<ul style="list-style-type: none"> <li>- Ship hijacking</li> <li>- Problems with the NS</li> <li>- GPS signal false information</li> <li>- Disrupt vessel operation</li> <li>- Delays in services</li> </ul>
Radar	<ul style="list-style-type: none"> <li>- Jamming attacks</li> <li>- Spoofing attacks</li> <li>- DoS/DDoS attacks</li> </ul>	<ul style="list-style-type: none"> <li>- Loss of communication with the NS</li> <li>- Loss of lives and cargo</li> <li>- Delays in cargo management</li> </ul>
Global Maritime Distress System (GMDSS)	<ul style="list-style-type: none"> <li>- Malware</li> <li>- Spoofing attacks</li> <li>- DoS/DDoS attacks</li> </ul>	<ul style="list-style-type: none"> <li>- Wrong position of the ship</li> <li>- Further attacks on ECDIS</li> </ul>
Industrial Control Systems (ICSs)	<ul style="list-style-type: none"> <li>- Inadequate ACM</li> <li>- No support for integrity check</li> <li>- Information exposure</li> <li>- Poor patch management</li> <li>- Hardware failures</li> <li>- Improper security configuration</li> <li>- Lack of network segmentation</li> <li>- Weak password policies</li> <li>- Lack of firewalls</li> <li>- Lack of encryption</li> <li>- Weak remote access policies</li> <li>- Weak USB policy</li> <li>- Lack of training for SOS</li> </ul>	<ul style="list-style-type: none"> <li>- Ship hijacking</li> <li>- Unavailability of the ICS</li> <li>- Data leakage</li> <li>- Physical damage to facilities</li> <li>- Interference with safety systems</li> <li>- Unplanned shutdowns</li> <li>- Damage to equipment</li> </ul>



Table 2. Cont.

Systems	Vulnerabilities	Consequences
Propulsion and machinery management and power control systems	<ul style="list-style-type: none"> <li>- Malware attack</li> <li>- DoS/DDoS attacks</li> <li>- Smuggling</li> <li>- Stealing</li> <li>- Manipulation attacks</li> </ul>	<ul style="list-style-type: none"> <li>- Ship hijacking</li> <li>- Diversion of the ship</li> <li>- PS could be interrupted</li> <li>- Ship damage</li> <li>- Financial damage</li> <li>- Disclosure of sensitive data</li> </ul>
Very Small Aperture Terminal (VSAT)	<ul style="list-style-type: none"> <li>- Fake signals</li> <li>- Malware attack</li> <li>- Stealing</li> </ul>	<ul style="list-style-type: none"> <li>- Theft of sensitive data</li> <li>- Upload of malware</li> <li>- Change of GPS coordinates</li> </ul>
IT network systems	<ul style="list-style-type: none"> <li>- Poor access control</li> <li>- DoS/DDoS attacks</li> <li>- Weak password policies</li> <li>- Malware attacks</li> <li>- Poor patch management</li> <li>- Improper security configuration</li> <li>- Poor security documentation</li> <li>- Lack of network segmentation</li> <li>- Lack of firewalls</li> <li>- Lack of encryption</li> <li>- Weak remote access policies</li> <li>- Weak USB policy</li> <li>- Lack of training for SOS</li> </ul>	<ul style="list-style-type: none"> <li>- Upload malware</li> <li>- Unauthorised physical access</li> <li>- Unauthorised logical access</li> <li>- Loss of confidential documents</li> <li>- Financial damage</li> <li>- Theft of sensitive data</li> <li>- Reputation damage</li> </ul>

OS: Operating System. NS: Navigational System. ACM: Access Control Management. SOS: Secure Operations of the System. PS: Propulsion System.

#### 4. Cyberattack Cases from the Maritime Transport Sector

Increased automation and artificial intelligence appear to be opening up new avenues for cyberattacks against the shipping industry, which has experienced serious cybersecurity incidents in recent years [24,49,50]. The technology needed to “spoof” a vessel is not expensive and is becoming easier to find and download online. Spoofing incidents have already been reported in the Black Sea, where a number of ships reported anomalies with their GPS-derived position and found themselves apparently located at an airport [51]. In the same area as the incident above, a ship was also exposed to GPS spoofing. The ship was at sea, but the geolocation system onboard claimed that the ship was on land [33]. Moreover, ship collisions and sea accidents due to the malfunction of navigation systems have been observed many times [52–54]. In May 2017, a spoofing attack led to a collision between a U.S. Navy ship and a South Korean fishing boat [53]. In February 2017, an 8250 Twenty-Foot Equivalent Unit (TEU) vessel was completely hacked in route from Cyprus to Djibouti [54]. For about 10 h, the attacker took over the ship’s navigation system and the captain was helpless to do anything to put the ship back into operation. In a previous GPS jamming attack, more than 280 vessels were reported by South Korea to have experienced navigational system issues; the GPS signal was jammed by hackers, causing some GPS signals to die and others to receive incorrect data [55]. When GPS fails to function properly, there is a very high risk of a disaster with catastrophic consequences for the crew, the ship, and the environment.

In a recent incident [56], the onboard control system network of a U.S. vessel was infected with malware. This network is usually used to update electronic charts, manage cargo data, and communicate with shore-side facilities. The FBI reported that the lack of security strategies on the vessel was the main reason for such an attack, which caused critical credential mining of the vessel’s control systems. In another similar incident, hackers remotely compromised the onboard computers of a U.S. Navy contractor, stealing massive amounts of highly sensitive data (614 GB) [57]. In recent years, the shipping industry has become an attractive target for ransomware attacks due to a perceived lack of investment in cybersecurity and the potential for significant operational disruptions [33]. In 2020,

two ships were infected by the ransomware Hermes 2.1 via the AZORult trojan. The infection came as a macro-enabled Word document attached to an email, and multiple workstations on the administrative networks were affected [33,58]. In 2021, multiple Greek shipping companies were hit by a ransomware attack that spread through the systems of an IT consulting firm [58]. This incident showed the reality of IT supply chain risk for shipowners, shipmanagers, and the shipping industry, where a large number of them were affected by the hack. A few days later, one vessel was hijacked and up to six others reported the loss of steering control in the Gulf of Oman. These incidents were considered as “cyberpiracy” [59]. In another cyber incident, a newly built dry bulk ship was delayed from sailing for several days because its ECDIS was infected by an unknown virus. The source and means of infection, in this case, remain unknown [60]. According to [60], the delay in sailing and costs in repairs totalled hundreds of thousands of dollars (USD).

The IT systems of ports have also had a burst of associated cyber incidents that affected the maritime infrastructure. The most frequent types of attacks are phishing, malware, social engineering, brute force, and denial of service. In March 2020, the port of Marseilles was hit with the “Mespinoza/Pysa” ransomware. In this incident, the maritime infrastructures were affected by the attack due to their interconnection with information systems in Aix-Marseille-Provence, which was the main target of the attack [61]. In another large-scale incident, the port system of Maersk fell victim to a major cyberattack caused by the “NotPetya” malware, which also affected many other shipping companies globally. Maersk’s ships are still at sea, and its 76 port terminals around the world have stopped [62]. This incident was followed in 2020 by a serious ransomware attack on the shipping company CMA CGM SA, which impacted some servers on its network and prevented customers from having external access to the company’s IT applications and booking systems [63]. This year, the Port of Houston was the target of an attack that involved a password management program that contained a formerly unknown vulnerability. The hackers exploited that to install malicious code that granted access to the networks, which they used to exfiltrate login credentials needed to control network access [64]. Luckily, the hack attempt was successfully defended, and “no system was impacted”. All these incidents confirm that modern cyberattacks go beyond manipulating navigation or tampering with cargo; they can disrupt local and global supply chains and even put the lives of the crew or passengers on board the ship at risk. Table 3 presents examples of recent cyber incidents in the maritime transport sector.

**Table 3.** Examples of recent cyber incidents in the maritime transport sector.

Year	Incident	Consequences
2016	GPS jamming attack in South Korea [54]	280 vessels were affected
2017	Cyberattack against the navigation system [54]	Hijack of the vessel for 10 h
2017	Cyberattack against the navigation system [53]	U.S. Navy ship collided with a boat
2018	GPS spoofing attack against ships in the Black Sea [51]	Deviation of 20 ships to an airport
2018	Remotely compromising onboard computers [57]	Stealing sensitive data
2018	GPS spoofing attack [33]	Manipulation of the ship position
2018	NotPetya malware attack [62]	Affected shipping infrastructures
2018	ECDIS was infected by a virus [60]	Delay in the ship sailing
2019	Malware attack targeted a U.S. vessel [56]	Critical credential mining
2020	Ransomware Hermes 2.1. attack on 2 ships [33]	Infection of the whole network
2020	Ransomware attack “Mespinoza/Pysa” [33,61]	Maritime infrastructures infected
2021	Ransomware attack on shipping companies [58]	All their files were encrypted
2022	Installation of malicious code [57]	Gain access to the port network

## 5. Security and Safety Countermeasures

Modern and autonomous ships have become ripe targets for high-profile cyberattacks due to the increasing usage of digital technologies. Therefore, several countermeasures and in-depth defence strategies should be adopted in order to build resilience to external and internal security threats [65,66]. The first is to create a continuous monitoring system that can

provide real-time situation awareness of the ship's security health status [65,67,68]. In this context, blockchain technology has been proposed to improve autonomous vessels' control security in many studies [65,69–71]. The main feature of blockchain technology, including traceability, transparency, auditability, immutability, and decentralisation, is proposed to enable secure communication and secure storage of the data exchanged between vessels and the shore control centre. The utilisation of this technology will eliminate some critical security threats for ship communication, such as losing data, data changing by malicious actors, or data hijacking [71]. According to [70], blockchain technology will play a major role in identification and certification, ensuring data integrity and information security in the future of the maritime industry and autonomous vessels.

Since all ship systems are interconnected, only one compromised system can allow attacks to access all other systems, from the water treatment system to the engine management system. Therefore, the design of the IT and OT systems themselves can be a valuable asset to defend from certain attacks as well [65]. According to [72], one mechanism that could increase navigational safety is the Navigation Message Authentication (NMA) system, which is designed to prevent spoofing and to provide increased safety. An NMA scheme would include authentication messages in the navigation message stream, authenticating the source, while also protecting the navigation data's cryptographic integrity [73]. The receiver can detect intruders trying to generate or modify navigation data. An attacker cannot simulate an authentication message because he/she does not have the key required to generate the authentication message. Considering the dangers of the ECDIS failure, the IMO outlined the need for backup arrangements on board vessels. Because these backups do not provide the full functionality of ECDIS, they should be used in conjunction with current paper charts. Many reputable shipping companies choose to install a second ECDIS on board to reduce the risk of ECDIS failure [74].

Given the vast amounts of data that ships tend to generate, efficient authentication and access control mechanisms would be preferable in most circumstances [65,67,68]. The shipping community must implement a Public Key Infrastructure (PKI) for the electronic trust system to function; this is because the PKI will allow users and systems to validate the legitimacy of certificate-holding entities, while also securely exchanging information among them. Many PKIs are already in operation, with the majority being established on a commercial basis by private entities. A shipping PKI with the IMO as the top trusted entity ("root Certificate Authority (CA0)") and flag states directly underneath can be set up [75]. Flag states have the authority to issue new keys and certificates to coastal state authorities, ships flying their flag, recognised organisations, ports, and others who require an internationally available public key certificate. Certificates can also be issued to ship owners or other organisations that play important roles in the international shipping community for secured communication and sharing of digital information [76]. The study in [77] indicated that based on spatial correlation, an antenna array structure is used to detect and mitigate spoofing signals. This method can detect interfering signals, and array calibration is not required or any array orientation information. This technique is capable of effectively distinguishing spoofing attacks that use a single transmit antenna. Furthermore, because all spoofing signals share the same propagation channel properties, their performance is unaffected by multipath propagation. Since it requires the use of multiple antenna branches, this procedure increases the hardware complication of the GPS receiver, because it must acquire and track both spoofing and authentic signals to distinguish spoofing PRNs; this method increases the computational density of the GPS receiver.

In addition, third-party access to systems, such as remote access solution providers, can be problematic because it is difficult to determine the security posture of these organisations and their networks are not typically included in security assessments. This should be performed in a manner that is confirmed by an entity actually present on the vessel. It is important to evaluate each of these factors to reduce the likelihood of a security vulnerability that could allow an attacker to access a ship's system or traverse the network without obstruction [33]. One of the first steps in mitigating a potential attack is to be aware of the vulnerabilities, which are essentially a niche in the network. However, integrating a

comprehensive security plan into the ship's network systems provides the most effective way to prepare for the worst and know how to get back. To achieve this, a comprehensive risk assessment should be carried out, and this will assist in the development of a robust cybersecurity risk strategy.

In the maritime security policies, the human factor plays a significant role within an organisation, as this can be the weakest link, but on the other hand, the first defence in the cyber chain [33,78,79]. Under this prism, the human factor becomes even more challenging with a complex interconnected ecosystem such as the one that exists in the maritime sector. Ships, ports, and third-parties are often operating with rotating crews with different levels of cybersecurity understanding, who may not be fully familiar with the safe operation of the related systems and established cyber hygiene practices. A lack of a cybersecurity culture may be beneficial to any attacker that wants to gain access to a vessel and its systems, steal actual information, or disrupt the vessel's operations. Hence, there is a critical need in the maritime industry to enhance the level of awareness and understanding related to the actual cyber risks. The most effective way to achieve this is with the promotion of a cybersecurity culture that, among others, includes cybersecurity awareness training, education, and certification for the relevant parts of the vessel's operation (crew, third-parties, ports, operators) [60].

Finally, collaborative defence systems that implicate multiple stakeholders are being explored [16,80]. These defence systems can participate in the identification and mitigation of potential cyberattacks at multiple levels. Detection and countermeasures taken for an attack on a single vessel can be communicated to other autonomous vessels in the fleet. Table 4 presents possible countermeasures and mitigation actions that can help to build resilience to external and internal security threats.

**Table 4.** A summary of possible mitigation actions.

Systems	Mitigation Actions
Automatic Identification System (AIS)	<ul style="list-style-type: none"> <li>- All AIS information should be verified</li> <li>- Encryption of the VHF signals</li> <li>- Integrity of broadcast information should be monitored to ensure that position and identity are correct.</li> <li>- Equipment that broadcasts AIS signals should be secured, and unauthorised access should not be possible</li> <li>- Local navigation warnings should be considered if false AIS signals are being broadcast</li> </ul>
Electronic Chart Display Information System (ECDIS)	<ul style="list-style-type: none"> <li>- ECDIS developers should look to adopt security development lifecycles</li> <li>- Regular documentation, monitoring, and patching of the ECDIS framework</li> <li>- ECDIS chart update should be monitored and registered, especially manual updates via CD or USB disc</li> <li>- All upgrade files should be scanned with antivirus software</li> <li>- The internal network to which ECDIS is linked should be examined to see whether the ECDIS system can be fully isolated or firewalled</li> <li>- Only approved staff should have physical access to ECDIS and its underlying components</li> </ul>
GNSS and GPS	<ul style="list-style-type: none"> <li>- Device identification and authentication</li> <li>- Cryptographic protection</li> <li>- Protection of information at rest</li> </ul>
Radar	<ul style="list-style-type: none"> <li>- Device identification and authentication</li> <li>- Cryptographic protection</li> <li>- Information system backup</li> </ul>
Global Maritime Distress System (GMDSS)	<ul style="list-style-type: none"> <li>- Cryptographic protection.</li> <li>- Device identification and authentication</li> <li>- Protection of information at rest</li> <li>- Physical access control</li> <li>- Contingency plan</li> </ul>

Table 4. Cont.

Systems	Mitigation Actions
Industrial Control Systems (ICSs)	<ul style="list-style-type: none"> <li>- Use cryptography or other protected methods to shield passwords from unauthorised interception</li> <li>- To keep control systems safe, implement configuration management and patch management controls</li> <li>- As far as possible, communications between security zones should be guarded</li> <li>- Ensure that all Internet-connected ICS devices are protected and that passwords are updated regularly</li> <li>- ICS network administrators should use network segmentation and firewall rules that block access to file-sharing ports</li> <li>- Protect password files adequately by making hashed passwords more difficult to obtain</li> <li>- System administrators should enforce strong passwords</li> <li>- Use concrete remote access policy</li> <li>- Audit remote access and related changes</li> <li>- Block unnecessary USB ports</li> <li>- Ensure cybersecurity awareness training has been conducted for all users</li> </ul>
Propulsion and machinery management and power control systems	<ul style="list-style-type: none"> <li>- Information system backup</li> <li>- Denial of service protection</li> <li>- Monitoring physical access</li> </ul>
Very Small Aperture Terminal (VSAT)	<ul style="list-style-type: none"> <li>- Encrypted communication systems should be considered</li> <li>- The service provider's cyber defence mechanisms should be carefully considered, but they should not be relied on solely to protect every shipboard device and data</li> <li>- Authentication and access control management should be strictly complied with</li> <li>- Protection of information at rest</li> </ul>
IT network systems	<ul style="list-style-type: none"> <li>- Information system backup</li> <li>- Authentication and access control</li> <li>- Segmentation of crew vs. business functions</li> <li>- Ensure threat protection mechanisms</li> <li>- Promote configuration/patch/update management system</li> <li>- Ensure BYOD policy is in place</li> <li>- Ensure cybersecurity awareness training has been conducted for all users</li> </ul>
Human factor	<ul style="list-style-type: none"> <li>- Promote a cybersecurity culture within the organisation</li> <li>- Create relationships with the members of the operation chain</li> <li>- Ensure cyber awareness training has been conducted</li> <li>- Evaluate training effectiveness with cybersecurity drills</li> <li>- Promote cyber hygiene within the operation parties</li> </ul>

## 6. Conclusions

Although the maritime industry faces broadly the same cybersecurity challenges as other sectors, it is becoming increasingly apparent that it fits the profile of critical infrastructure being targeted by cybercriminals, and it also faces risks that might be considered unique to the nature of this industry. For instance, a successful cyberattack could shut down a ship, disclose valuable information, disable the vessel's AIS, and/or create false or misleading AIS reports facilitating cyberpiracy and criminal, terrorist, or even state actors. This paper reviewed the current security threats and vulnerabilities in the modern shipping industry. In this context, various types of cyberattacks, these ships could face, were discussed along with real-world incidents. From the numerous reported cyber incidents and their consequences, there is clear evidence that every ship, vessel, or even port is at risk of cyberattacks if key information systems are not adequately protected. Therefore, IT and OT systems in modern ships should be prepared with enhanced security measures due to their great vulnerability to cyber threats. In this paper, we discussed some possible countermeasures that can mitigate potential cyberattacks and make the shipping industry a hard target, such as the implementation of a new security standard that reduces the number and scope of cyberattacks. However, many security challenges remain unresolved, especially with the increasing use of autonomous and semi-autonomous vessels.

**Author Contributions:** Conceptualisation, F.A., G.B. and S.S.; investigation, F.A., G.B., S.S., S.K. and M.M.; methodology, G.B., F.A. and S.S.; supervision, S.S.; writing—original draft, F.A. and S.S.; writing—review and editing, G.B., F.A., S.S., S.K. and M.M. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

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

### Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
AIS	Automatic Identification System
CE	Certificate Authority
ECDIS	Electronic Chart Display and Information System
GMDS	Global Maritime Distress System
GPS	Global Positioning System
IBS	Integrated Bridge System
ICS	Industrial Control System
ICT	Information and Communications Technology
IMO	International Maritime Organization
IT	Information Technology
NNSS	Global Navigation Satellite System
NMA	Navigation Message Authentication
OT	Operational Technology
PKI	Public Key Infrastructure
Radar	Radio Detection and Ranging
VSAT	Very Small Aperture Terminal
VSS	Video Surveillance System

### References

1. DiRenzo, J.; Goward, D.A.; Roberts, F.S. The little-known challenge of maritime cybersecurity. In Proceedings of the 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA), Corfu, Greece, 6–8 July 2015; pp. 1–5.
2. Jensen, L. Challenges in maritime cyber-resilience. *Technol. Innov. Manag. Rev.* **2015**, *5*, 35. [CrossRef]
3. Alcaide, J.I.; Llave, R.G. Critical infrastructures cybersecurity and the maritime sector. *Transp. Res. Procedia* **2020**, *45*, 547–554. [CrossRef]
4. Fell, J. Mayflower tribute set to sail unmanned [automated marine transport]. *Eng. Technol.* **2015**, *10*, 42–44. [CrossRef]
5. Foundation, N. Demonstration Test of World’s First Unmanned Operation of Small Tourism Boat Successfully Completed at Sarushima, Yokosuka. Available online: <https://www.nippon-foundation.or.jp/en/news/articles/2022/20220111-67000.html> (accessed on 14 January 2022).
6. Gu, Y.; Goetz, J.C.; Guajardo, M.; Wallace, S.W. Autonomous vessels: State of the art and potential opportunities in logistics. *Int. Transp. Oper. Res.* **2021**, *28*, 1706–1739. [CrossRef]
7. Gu, Y.; Wallace, S.W. Operational benefits of autonomous vessels in logistics—A case of autonomous water-taxis in Bergen. *Transp. Res. Part E Logist. Transp. Rev.* **2021**, *154*, 102456. [CrossRef]
8. Werle, D.; Boudreau, P.R.; Brooks, M.R.; Butler, M.J.; Charles, A.; Coffen-Smout, S.; Griffiths, D.; McAllister, I.; McConnell, M.L.; Porter, I.; et al. The Future of Ocean Governance and Capacity Development. In *The Future of Ocean Governance and Capacity Development*; Brill Nijhoff: Leiden, The Netherlands, 2019; pp. 1–4.
9. Kavallieratos, G.; Katsikas, S.; Gkioulos, V. Cyberattacks against the autonomous ship. In *Computer Security*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 20–36.
10. Tam, K.; Jones, K. Cyber-risk assessment for autonomous ships. In Proceedings of the 2018 International Conference on Cybersecurity and Protection of Digital Services (Cybersecurity), Scotland, UK, 11–12 June 2018; pp. 1–8.
11. Balduzzi, M.; Pasta, A.; Wilhoit, K. A security evaluation of AIS automated identification system. In Proceedings of the 30th Annual Computer Security Applications Conference, New Orleans, LA, USA, 8–12 December 2014; pp. 436–445.
12. LR. Cyber Enabled Systems. Available online: <https://unece.org/fileadmin/DAM/trans/doc/2018/sc3wp3/07.LR.pdf> (accessed on 31 January 2022).
13. CruisMapper. Cruise Ship Safety. Available online: <https://www.cruisemapper.com/wiki/751-cruise-ship-safety> (accessed on 3 February 2022).

14. Yastrebova, A.; Höyhty, M.; Boumard, S.; Ometov, A. Comparative study on GNSS positioning systems for autonomous vessels in the arctic region. In Proceedings of the WiP Proceedings of the International Conference on Localization and GNSS (ICL-GNSS 2020), Tampere, Finland, 1–3 June 2020.
15. Kessler, G.C.; Craiger, J.P.; Haass, J.C. A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system. *Int. J. Mar. Navig. Saf. Sea Transp.* **2018**, *12*, 429. [CrossRef]
16. Bhutani, A.; Göttel, B.; Van, N.T.P.; Mukhopadhyay, S.; Demir, V. *Advances in Radar Technology*; Scientific Research Publishing: Wuhan, China, 2021; p. 245.
17. Kuzmichev, A.P.; Smirnov, V.G.; Zakhvatkina, N.Y.; Bychkova, I.A. Use of Satellite Communication Systems for Collecting and Transmitting Data on the State of the Arctic Sea Ice Cover. In Proceedings of the 2021 IEEE International Geoscience and Remote Sensing Symposium IGARSS, Brussels, Belgium, 11–16 July 2021; pp. 5732–5734.
18. FORSCOUT. Securing Ship Automation & Control Systems. Available online: <https://www.forescout.com/resources/securing-ship-automation-control-systems/> (accessed on 31 January 2022).
19. Stouffer, K.; Falco, J.; Scarfone, K. Guide to industrial control systems (ICS) security. *NIST Spec. Publ.* **2011**, *800*, 16.
20. Ilcev, M. New Aspects for Modernization Global Maritime Distress and Safety System (GMDSS). *Int. J. Mar. Navig. Saf. Sea Transp.* **2020**, *14*, 519–530. [CrossRef]
21. Sáiz, V.M.M.; López, A.P. Future trends in electric propulsion systems for commercial vessels. *J. Marit. Res.* **2007**, *4*, 81–100.
22. Scherer, T.; Cohen, J. The evolution of machinery control systems support at the naval ship systems engineering station. *Nav. Eng. J.* **2011**, *123*, 85–109. [CrossRef]
23. Kazak, N.; Frolova, S. Ship Automation and Control Systems. In Proceedings of the IX All-Russian Science-Practical Conference of Students, Postgraduates and Young Scientists, Kerch, Crimea, 6 May 2020; p. 46.
24. Ben Farah, M.A.; Ukwandu, E.; Hindy, H.; Brosset, D.; Bures, M.; Andonovic, I.; Bellekens, X. Cybersecurity in the maritime industry: A systematic survey of recent advances and future trends. *Information* **2022**, *13*, 22. [CrossRef]
25. Menhat, M.N.; Zaideen, I.M.M.; Yusuf, Y.; Salleh, N.H.M.; Zamri, M.A.; Jeevan, J. The impact of Covid-19 pandemic: A review on maritime sectors in Malaysia. *Ocean. Coast. Manag.* **2021**, 105638. [CrossRef] [PubMed]
26. Chang, C.; Wenming, S.; Wei, Z.; Changki, P.; Kontovas, C. Evaluating cybersecurity risks in the maritime industry: A literature review. In Proceedings of the International Association of Maritime Universities (IAMU) Conference, Tokyo, Japan, 30 October–1 November 2019.
27. Larsen, M.H.; Lund, M.S. A Maritime Perspective on Cyber Risk Perception: A Systematic Literature Review. *IEEE Access* **2021**, *9*, 144895–144905. [CrossRef]
28. Marine Traffic. Available online: <https://www.marinetraffic.com/en/ais/home/centerx:-12.0/centery:25.0/zoom:4> (accessed on 14 January 2022).
29. Androjna, A.; Brcko, T.; Pavic, I.; Greidanus, H. Assessing cyber challenges of maritime navigation. *J. Mar. Sci. Eng.* **2020**, *8*, 776. [CrossRef]
30. Lisa, V. \$80 Million Yacht Hijacked by Students Spoofing GPS Signals. 31 July, Naked Security (Sophos). Available online: <https://nakedsecurity.sophos.com/2013/07/31/80-million-yachthijacked-by-students-spoofing-gps-signals> (accessed on 31 January 2022).
31. GPS World. State Department Issues Notice on North Korean Jamming. 2016. Available online: <http://gpsworld.com/state-department-issues-notice-on-north-korean-jamming> (accessed on 31 January 2022).
32. John, R. GPS fLaw Could Let Terrorists Hijack Ships, Planes. Fox News Tech. Available online: <http://www.foxnews.com/tech/2013/07/26/exclusive-gps-flaw-could-let-terroristshijack-ships-planes.html> (accessed on 31 January 2022).
33. Meland, P.; Bernsmed, K.; Wille, E.; Rødseth, Ø.; Nesheim, D. A retrospective analysis of maritime cybersecurity incidents. *Int. J. Mar. Navig. Saf. Sea Transp.* **2021**, *15*, 4. [CrossRef]
34. Analytica, O. Global maritime security risks rise with GNSS use. In *Emerald Expert Briefings*; Oxford Analytica: Oxford, UK, 2019; Volume 1.
35. Coffed, J. *The Threat of GPS Jamming: The Risk to an Information Utility*; Report of EXELIS: Herndon, VA, USA, 2014; pp. 6–10.
36. Schmidt, D.; Radke, K.; Camtepe, S.; Foo, E.; Ren, M. A survey and analysis of the GNSS spoofing threat and countermeasures. *ACM Comput. Surv.* **2016**, *48*, 1–31. [CrossRef]
37. Svilicic, B.; Brčić, D.; Žuškin, S.; Kalebić, D. Raising awareness on cybersecurity of ECDIS. *Int. J. Mar. Navig. Saf. Sea Transp.* **2019**, *13*, 231–236.
38. 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]
39. Kavallieratos, G.; Diamantopoulou, V.; Katsikas, S.K. Shipping 4.0: Security requirements for the cyber-enabled ship. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6617–6625. [CrossRef]
40. Dyryavy, Y. *Preparing for Cyber Battleships—Electronic Chart Display and Information System Security*; NCC Group: Manchester, UK, 2014.
41. Wu, Z.; Pan, Q.; Yue, M.; Ma, S. An Approach of Security Protection for VSAT Network. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1511–1516.
42. Santamarta, R. Maritime Security: Hacking into a Voyage Data Recorder (VDR). 2015. Available online: <https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr/> (accessed on 10 January 2022).

43. Pavur, J.; Moser, D.; Strohmeier, M.; Lenders, V.; Martinovic, I. A tale of sea and sky on the security of maritime VSAT communications. In Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 18–21 May 2020. Available online: [https://ieeexplore.ieee.org/abstract/document/9152624?casa\\_token=WNlJxkEBkiMAAAAA:M7VuGUYSWSjs0C9DUqJuH9gJfI9IWUO9MvFuZoCpEwuAX3BmKg57M9w2ZSfDFKM.sTvYrwwgQ6P](https://ieeexplore.ieee.org/abstract/document/9152624?casa_token=WNlJxkEBkiMAAAAA:M7VuGUYSWSjs0C9DUqJuH9gJfI9IWUO9MvFuZoCpEwuAX3BmKg57M9w2ZSfDFKM.sTvYrwwgQ6P) (accessed on 10 January 2021).
44. Tam, K.; Jones, K. MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU J. Marit. Aff.* **2019**, *18*, 129–163. [[CrossRef](#)]
45. Heffner, C. Exploiting Surveillance Cameras Like a Hollywood Hacker. Available online: <https://privacy-pc.com/articles/exploiting-network-surveillance-cameras-like-a-hollywood-hacker.html> (accessed on 10 January 2021).
46. Bugeja, J.; Jönsson, D.; Jacobsson, A. An investigation of vulnerabilities in smart connected cameras. In Proceedings of the 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Athens, Greece, 19–23 March 2018; pp. 537–542.
47. Shoultz, D. Securely Connected Vessels: Vessel Communications and Maritime Cybersecurity. Technical Report. 2017. Available online: <https://www.maritimeprofessional.com/blogs/post/securely-connected-vessels-vessel-communicationsand-maritime-15176> (accessed on 9 July 2021).
48. Healey, J. *Beyond Data Breaches: Global Interconnections of Cyber Risk*; Atlantic Council: Washington, DC, USA, 2014.
49. Caprolu, M.; Di Pietro, R.; Raponi, S.; Sciancalepore, S.; Tedeschi, P. Vessels cybersecurity: Issues, challenges, and the road ahead. *IEEE Commun. Mag.* **2020**, *58*, 90–96. [[CrossRef](#)]
50. Al-Mhiqani, M.N.; Ahmad, R.; Yassin, W.; Hassan, A.; Abidin, Z.Z.; Ali, N.S.; Abdulkareem, K.H. Cyber-security incidents: A review cases in cyber-physical systems. *Int. J. Adv. Comput. Sci. Appl.* **2018**, *1*, 499–508.
51. Forscout. Spoofing in the Black Sea: What Really Happened? Available online: <https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/> (accessed on 31 January 2022).
52. Borger, J. Pentagon Orders Temporary Halt to US Navy Operations after Second Collision. Available online: <https://www.theguardian.com/us-news/2017/aug/21/us-destroyer-uss-john-s-mccain-damaged-after-collision-with-oil-tanker> (accessed on 31 January 2022).
53. Cohen, Z. US Navy Ship Collides with South Korean Fishing Boat. Available online: <https://edition.cnn.com/2017/05/09/politics/fishing-vessel-hits-us-navy-ship-south-korea/index.html> (accessed on 31 January 2022).
54. Roberts, F.S.; Egan, D.; Nelson, C.; Whytlaw, R. Combined cyber and physical attacks on the maritime transportation system. *NMIOTC Marit. Interdiction Oper. J.* **2019**, *18*, 22.
55. Oruc, A.; MIMarEST, M.S.M. Claims of State-Sponsored Cyberattack in the Maritime Industry. In Proceedings of the 15th International Naval Engineering Conference & Exhibition, Delft, The Netherlands, 6–8 October 2020.
56. Winder, D. U.S. Coast Guard Issues Alert after Ship Heading into Port of New York Hit By Cyberattack. Available online: <https://www.forbes.com/sites/daveywinder/2019/07/09/u-s-coast-guard-issues-alert-after-ship-heading-into-port-of-new-york-hit-by-cyberattack/?sh=61b920e741aa> (accessed on 31 January 2022).
57. Cooper, H. Chinese Hackers Steal Unclassified Data from Navy Contractor. 2018. Available online: <https://www.nytimes.com/2018/06/08/us/politics/china-hack-navy-contractor.html> (accessed on 31 January 2022).
58. Maritime-Executive. Cyberattack Hits Multiple Greek Shipping Firms. Available online: <https://www.maritime-executive.com/article/cyberattack-hits-multiple-greek-shipping-firms> (accessed on 3 February 2022).
59. Bebbington, T. Cyberattack or Coincidence? Available online: <https://www.seatrade-maritime.com/opinions-analysis/cyberattack-or-coincidence> (accessed on 3 February 2022).
60. The Guidelines on Cybersecurity Onboard Ships. Available online: <https://safety4sea.com/wp-content/uploads/2018/12/BIMCO-Guidelines-on-cyber-security-onboard-ships-2018.12.pdf> (accessed on 3 February 2022).
61. Nicaise, V. Cybermarétique: A Short History of Cyberattacks against Ports. Available online: <https://www.stormshield.com/news/cybermarétique-a-short-history-of-cyberattacks-against-ports/> (accessed on 3 February 2022).
62. Team, E. Maersk Line: Surviving from a Cyber Attack. Available online: <https://safety4sea.com/cm-maersk-line-surviving-from-a-cyberattack/> (accessed on 3 February 2022).
63. Rosehana Amin, R.D.; Jones, D. Part 1: A Very Modern Form of Piracy: Cybercrime against the Shipping Industry—Rapidly Developing Risks. Available online: <https://www.clydeco.com/en/insights/2021/03/a-very-modern-form-of-piracy-cybercrime-against-th> (accessed on 3 February 2022).
64. Elliott, L. Port of Houston Target of Suspected Nation-State Hack. Available online: <https://www.nbcnews.com/tech/security/port-houston-target-suspected-nation-state-hack-rcna2249> (accessed on 3 February 2022).
65. Silverajan, B.; Ocak, M.; Nagel, B. Cybersecurity attacks and defences for unmanned smart ships. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 15–20.
66. Bothur, D.; Zheng, G.; Valli, C. A critical analysis of security vulnerabilities and countermeasures in a smart ship system. In Proceedings of the 15th Australian Information Security Management Conference, Perth, Australia, 5–6 December 2017.
67. Zhou, X.; Liu, Z.; Wu, Z.; Wang, F. Quantitative processing of situation awareness for autonomous ships navigation. *Int. J. Mar. Navig. Saf. Sea Transp.* **2019**, *13*, 25–31. [[CrossRef](#)]



68. Reddy, G.N.; Reddy, G. A study of cybersecurity challenges and its emerging trends on latest technologies. *arXiv* **2014**, arXiv:1402.1842.
69. Petković, M.; Vujović, I. Blockchain security of autonomous maritime transport. *J. Appl. Eng. Sci.* **2019**, *17*, 333–337. [[CrossRef](#)]
70. Bechtsis, D.; Tsolakis, N.; Bizakis, A.; Vlachos, D. A blockchain framework for containerized food supply chains. In *Computer Aided Chemical Engineering*; Elsevier: Amsterdam, The Netherlands, 2019; Volume 46, pp. 1369–1374.
71. Ahmad, R.W.; Hasan, H.; Jayaraman, R.; Salah, K.; Omar, M. Blockchain applications and architectures for port operations and logistics management. *Res. Transp. Bus. Manag.* **2021**, *41*, 100620. [[CrossRef](#)]
72. Wullems, C.; Pozzobon, O.; Kubik, K. Signal authentication and integrity schemes for next generation global navigation satellite systems. *Eur. J. Navig.* **2005**, *3*, 4.
73. Caparra, G.; Sturaro, S.; Laurenti, N.; Wullems, C.; Ioannides, R.T. A novel navigation message authentication scheme for GNSS open service. 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. 2938–2947.
74. Brčić, D.; Kos, S.; Žuškin, S. Navigation with ECDIS: Choosing the proper secondary positioning source. *Int. J. Mar. Navig. Saf. Sea Transp.* **2015**, *9*, 317–329.
75. Bour, G.; Bernsmed, K.; Borgaonkar, R.; Meland, P.H. On the certificate revocation problem in the maritime sector. In Proceedings of the Nordic Conference on Secure IT Systems, Aalborg, Denmark, 29–30 November 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 142–157.
76. Rødseth, Ø.J.; Frøystad, C.; Meland, P.H.; Bernsmed, K.; Nesheim, D.A. The need for a public key infrastructure for automated and autonomous ships. In Proceedings of the IOP Conference Series: Materials Science and Engineering, Ulaanbaatar, Mongolia, 10–13 September 2020; Volume 929, p. 012017.
77. Seo, S.H.; Lee, B.H.; Im, S.H.; Jee, G.I.; Kim, K.S. Efficient spoofing identification using baseline vector information of multiple receivers. *GPS Solut.* **2018**, *22*, 1–14. [[CrossRef](#)]
78. Mraković, I.; Vojinović, R. Maritime cybersecurity analysis—How to reduce threats? *Trans. Marit. Sci.* **2019**, *8*, 132–139. [[CrossRef](#)]
79. Tam, K.; Jones, K.D. Maritime cybersecurity policy: The scope and impact of evolving technology on international shipping. *J. Cyber Policy* **2018**, *3*, 147–164. [[CrossRef](#)]
80. Jones, K.D.; Tam, K.; Papadaki, M. Threats and Impacts in Maritime Cybersecurity. Master's Thesis, University of Plymouth, Plymouth, UK, 2016.