







Review

Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends

Mohamed Amine Ben Farah ¹, Elochukwu Ukwandu ², Hanan Hindy ³, David Brosset ⁴, Miroslav Bures ⁵, Ivan Andonovic ⁶ and Xavier Bellekens ^{7,8,*}

- ¹ Department of Networks and Cyber Security, Birmingham City University, Birmingham B4 7XG, UK; mohamed.benfarah@bcu.ac.uk
- ² Department of Computer Science, Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff CF5 2YB, UK; eaukwandu@cardiffmet.ac.uk
- ³ Computer Science Department, Faculty of Computer and Information Sciences, Ain Shams University, Cairo 11566, Egypt; hanan.hindy@cis.asu.edu.eg
- ⁴ Naval Academy Research Institute, Arts et Métiers Institute of Technology, BCRM Brest, École Navale, CC 600, CEDEX 9, 29240 Brest, France; david.brosset@ecole-navale.fr
- ⁵ Department of Computer Science, FEE, Czech Technical University in Prague, Karlovo Nam. 13, 121 35 Prague, Czech Republic; buresm3@fel.cvut.cz
- ⁶ Department of Electronic and Electrical Engineering, Royal College Building, University of Strathclyde, 204 George St., Glasgow G1 1XW, UK; i.andonovic@strath.ac.uk
- ⁷ Lupovis Limited, Glasgow G1 1XW, UK
- ⁸ The Scowcroft Center for Strategy and Security at the Atlantic Council, Washington, DC 20005, USA
- * Correspondence: xavier@lupovis.io

Abstract: The paper presents a classification of cyber attacks within the context of the state of the art in the maritime industry. A systematic categorization of vessel components has been conducted, complemented by an analysis of key services delivered within ports. The vulnerabilities of the Global Navigation Satellite System (GNSS) have been given particular consideration since it is a critical subcategory of many maritime infrastructures and, consequently, a target for cyber attacks. Recent research confirms that the dramatic proliferation of cyber crimes is fueled by increased levels of integration of new enabling technologies, such as IoT and Big Data. The trend to greater systems integration is, however, compelling, yielding significant business value by facilitating the operation of autonomous vessels, greater exploitation of smart ports, a reduction in the level of manpower and a marked improvement in fuel consumption and efficiency of services. Finally, practical challenges and future research trends have been highlighted.

Keywords: maritime industry; cyber-attack; autonomous vessel; port



Citation: Ben Farah, M.A.; Ukwandu, E.; Hindy, H.; Brosset, D.; Bures, M.; Andonovic, I.; Bellekens, X. Cyber-Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. *Information* **2022**, *13*, 22. <https://doi.org/10.3390/info13010022>

Academic Editor: Sokratis Katsikas

Received: 12 November 2021

Accepted: 22 December 2021

Published: 6 January 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/>).

1. Introduction

Maritime transportation is central to the economic sustainability of many regions throughout the world. The growth in global population, improvements in living standards and investment and elimination of trade barriers all contribute to driving an ever-increasing reliance on the industry. In geographies with navigable rivers or comprising a cluster of islands, maritime transportation is the spine to both domestic and international trading. Moreover, in markets that demand sustainable development, low cost, efficiency and, recently of growing importance, ecofriendly operations, the maritime sector is responsible for 90% of the transportation of all goods [1,2]. Recent developments in the Internet of Things (IoT), Big Data and Artificial Intelligence have enabled the migration to more digitalised maritime infrastructures and, consequently, have necessitated a renewed assessment of the cyber-security provision [3]. Furthermore, connectivity and reliance on intelligent devices play a pivotal role in motivating cyber criminality such as social engineering, identity theft and spam emails. The protection of the integrity of next generation maritime infrastructures is a pressing need [4–7].

Connectivity through navigation systems such as Automatic Identification System (AIS, see Abbreviations), Global Navigation Satellite System (GNSS) and Radio Detection and Ranging (RADAR) impacts negatively on the security level of infrastructures. Moreover, shipping companies have been subjected to highly complex and new classes of cyber attacks targeting in-port information systems and inflicting damage on on-vessel core equipment [8,9]. The reliance on the Internet, operating with unprotected computers, and the fact that crews do not receive appropriate security training increase further the probability of a successful cyber breach. There is clear evidence that the absence of structured security awareness training for employees across the supply chain is a major source of vulnerabilities; as a result, hackers can use classical approaches such as spam emails or Denial-of-Service (DoS) attacks to achieve successful breaches [10,11]. A security plan providing recommendations to protect the maritime supply chain and a co-coordinated strategy with international marine organizations is a near-term necessity [12]. The update of software through removable media increases the risk of stealing identities and in-port data and the sharing of information in real time using new technologies—such as IoT—exacerbates the risk due to insecure network services or weak authentication.

The paper presents a comprehensive review of cyber-security frameworks and provides a classification of cyber-attacks within the maritime industry. A description of on-vessel equipment/functionalities and in-port services provides the reference against which a classification of the vulnerabilities in both operational environments is carried out, in turn informing on the optimum strategies to enhance existing cyber security protection. The remainder of the paper is organised as follows. Section 2 details the methodology applied to execute a review of the state of the art; Section 3 presents a summary of literature review of cyber security in the maritime industry. Section 4 provides a rigorous assessment of the vulnerabilities within on-vessel systems and in-port services while Section 5 classifies the spectrum of cyber-attacks. Section 6 focuses on the role and impact of the deployment of new technologies both on-ship and in-port. Section 7 elaborates on the evolution towards an extensively digitised maritime industry and the impact on cyber security provision. Conclusions are drawn in Section 8.

2. Methodology

The methodology by which the review has been executed is founded in reference to published literature enabling a mapping of the state-of-the-art methods and analysis, interpretation and implications of cyber security within the maritime industry.

2.1. Papers Selection

The review of the literature followed the guidance presented in [13–15] comprising the following phases:

1. Review: The principal question underpinning the literature review was “what is the impact of cyber-crimes on maritime infrastructures”;
2. Search: The search is based on journal papers, conference papers, official websites and published reports (Figure 1a). Table 1 shows a summary of significant recent survey papers on the maritime industry.

Documents were selected depending on the number of citations and/or relevance, and the sources are the following scientific databases: Science Direct, Springer and IEEE. The keywords used in the search were as follows:

- “Maritime”;
- “Cyber-attack” + “Maritime”;
- “Cyber-attack” + “Port.”

Figure 2 illustrates the growth in the number of published papers whilst Figure 1b shows that the bulk of the papers that met the selection criteria were published between 2015 and 2020. A classification of cyber-attacks reported on maritime infrastructures is presented in the next section to ease the evaluation of their impact(s).

3. The report on key findings is segmented as follows:

- Classification of on-vessel core equipment/systems;
- In-port architectures and services;
- Classification of cyber attacks;
- The impact of new technologies.

Table 1. Summary of significant recent survey papers on vessels/maritime industry.

Index	Title	Year	Comments	Ref.
1.	Collision-avoidance navigation systems for Maritime Autonomous Surface Ships: A state-of-the-art survey	2021	Overview of existing and future collision-avoidance navigation technologies.	[16]
2.	The impact of COVID-19 pandemic: A review on maritime sectors in Malaysia	2021	This paper reviews the impact of COVID-19 pandemic on maritime sectors, specifically shipping, fisheries, maritime tourism and oil and gas sector.	[17]
3.	C-Ports: A proposal for a comprehensive standardization and implementation plan of digital services offered by the “Port of the Future”	2022	A classification of C-Port services is proposed in the domains of vessel navigation, e-freight, mobility and sustainable growth strategies.	[18]
4.	Ports’ technical and operational measures to reduce greenhouse gas emission and improve energy efficiency: A review	2020	Review of port technical and operational measures to reduce GHG emissions.	[19]
5.	Decarbonisation of seaports: A review and directions for future research	2021	The paper provides a critical review of existing technologies and concepts that promote and contribute to the decarbonisation of seaports, including Smart Grids and Virtual Power Plants.	[20]
6.	Evaluating cybersecurity risks in the maritime industry: a literature review	2019	This research paper identifies three maritime cyber threats, including the lack of training and experts, the use of outdated system and the risk of being hacker’s target.	[21]
7.	Cybersecurity in ports: A conceptual approach	2017	The study is a conceptual analysis built upon a comprehensive literature review. The results show that regardless of the growing awareness of the issue, much work needs to be performed in order to mitigate cyberthreats in ports.	[22]
8.	Industry 4.0 in the port and maritime industry: A literature review	2020	The article reviews the state of the art on new emerging technologies, summarizing how ports and terminals are deploying specific projects in the new era of smart ports and Ports 4.0.	[23]
9.	Cybersecurity in logistics and supply chain management: An overview and future research directions	2021	This paper reviews studies on measures that enhance cybersecurity in logistics and supply chain management.	[24]
10.	Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review	2021	This paper aims to present an approach to investigate cyber risk perception with use of recognized psychological models and to provide an overview of state-of-the-art research within the field of cyber risk perception in general and in the context of the maritime domain.	[25]
11.	The CAN Bus in the Maritime Environment—Technical Overview and Cybersecurity Vulnerabilities	2021	This paper is a technical overview describing CAN bus standards and operations, with particular attention to its use with the NMEA 2000 maritime communications standard.	[26]

Table 1. *Cont.*

Index	Title	Year	Comments	Ref.
12.	COVID-19 digitization in maritime: understanding cyber risks	2021	This paper reviews current events and introduces an exercise where participants at a NATO Centre of Excellency were shown scenarios involving maritime cyber incidents and evaluated cyber risk perception.	[27]
13.	Big data and artificial intelligence in the maritime industry: a bibliometric review and future research directions	2020	This study provides a bibliometric review of 279 studies on the applications of Big data and artificial intelligence (AI) in the maritime industry.	[28]
14.	Autonomous technologies in short sea shipping: trends, feasibility and implications	2019	This paper is a comprehensive literature review on the issues faced by the short sea shipping (SSS) industry. A model is developed to explore potential savings of removing crew and use of autonomous technologies.	[29]
15.	Innovation and maritime transport: A systematic review	2020	This paper performs a systematic review aiming to understand recent innovation studies in the maritime sector.	[29]
16.	A Conceptual Review of Cyber-Operations for the Royal Navy	2018	This paper discusses the nature of the threats faced by national-security institutions and the doctrinal factors that policy makers must consider.	[30]
17.	Internet of Ships: A Survey on Architectures, Emerging Applications, and Challenges	2020	A comprehensive survey of the IoS paradigm, its architecture, its key elements and its main characteristics. Furthermore, a review of the state of the art for its emerging applications is presented.	[31]
18.	Marine Vision-Based Situational Awareness Using Discriminative Deep Learning: A Survey	2021	The paper summarizes the progress made in four aspects of current research: full scene parsing of an image, target vessel re-identification, target vessel tracking and multimodal data fusion with data from visual sensors.	[32]
19.	Maritime 4.0-Opportunities in Digitalization and Advanced Manufacturing for Vessel Development	2020	The paper introduces a descriptive approach for understanding Maritime 4.0.	[33]
20.	Cybersecurity and Safety Co-Engineering of Cyberphysical Systems-A Comprehensive Survey	2020	The paper provides a comprehensive survey of safety and cyber security co-engineering methods.	[34]

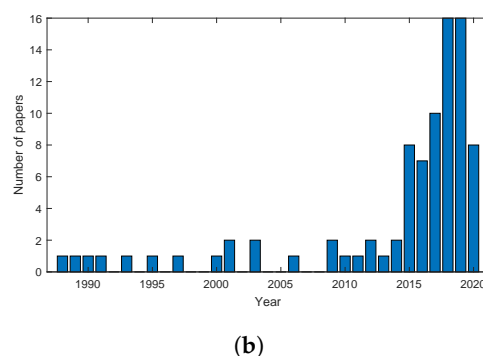
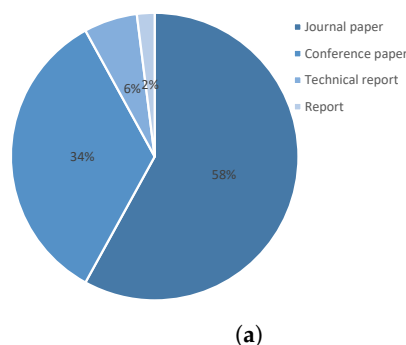


Figure 1. Classification of the reviewed papers.

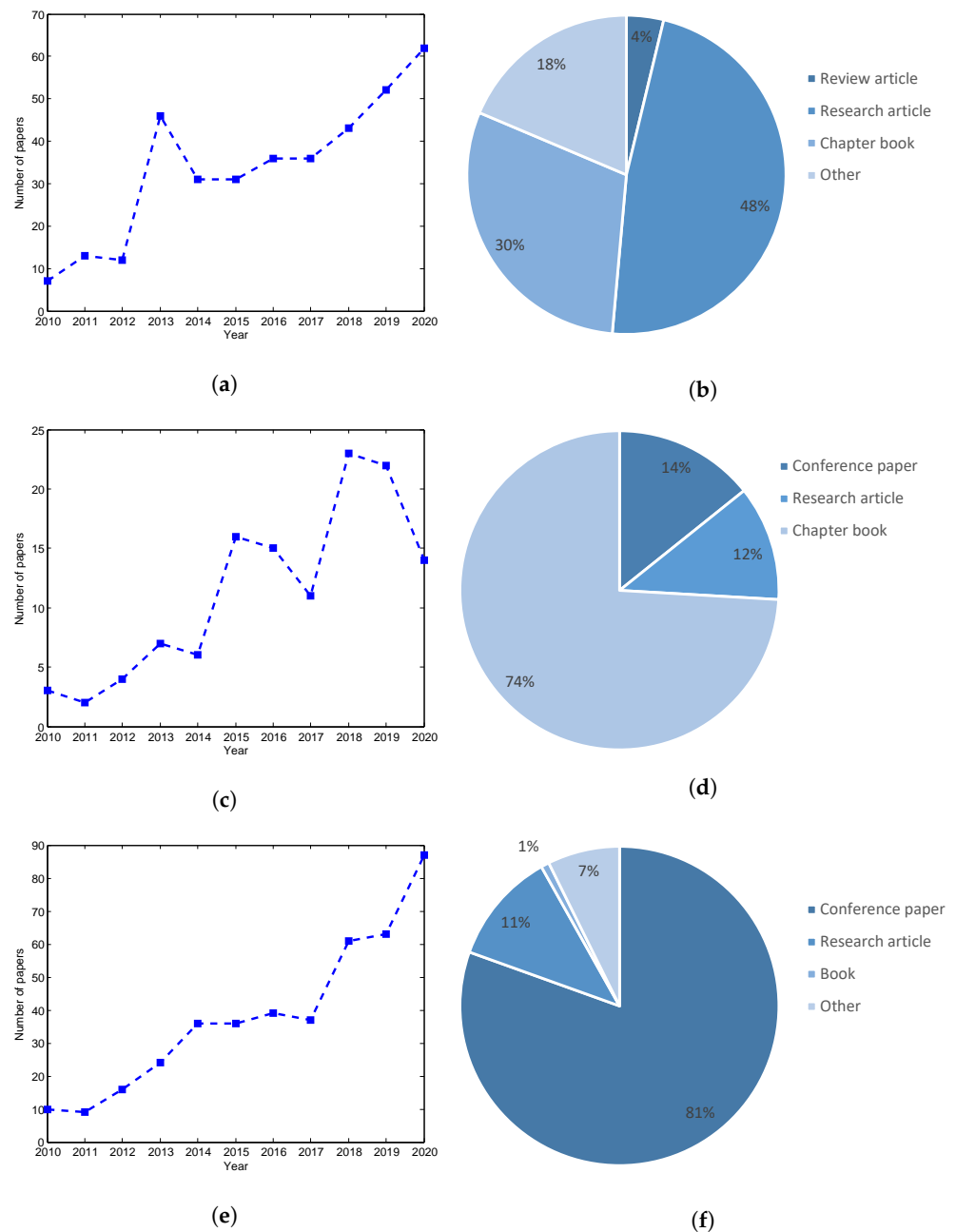


Figure 2. Evolution and classification of published papers: (a,d) ScienceDirect, (b,e) Springer and (c,f) IEEE.

2.2. Cyber-Attacks within the Maritime Industry

Reported cyber-attacks were collated and classified from published information and/or the declarations of stakeholders within the industry. Table 2 is a summary of cyber-attacks covering a period of ten years. Clearly evident is the increase in the number of cyber attacks and the lack of consistency in security practices across the sector. A statistical study—based on a system-of-system analysis between the period of October 2017 and February 2019—carried out by the Chatham House Cyber-Security Group [35] of the Royal Institute of International Affairs identified the essential systems both on-ship and in-port that require cyber-attack protection due to their respective vulnerabilities. The findings showed that the number of vulnerable components in-port is higher than on-ship.

Table 2. Summary of significant previous cyber-attacks on vessels/maritime industry.

Index	Type of Cyber-Attack	Year	Location and Description	Ref.
1.	Ransomware attack/ fishing attack	12 June 2021	South Korea's national flagship carrier HMM: Cyber attack resulting in limited access to the email outlook system.	[36]
2.	Ransomware attack	May 2020	Hormuz Port: The attempted cyber attack damaged some operating systems at the ports.	[37]
3.	Malware attack	10 April 2020	Mediterranean Shipping Company (MSC): For security issues servers of MSC were closed down to protect the data of the company, and, as a result, the website of the company was taken down. The attack disturbed only internal data processes.	[38]
4.	Malware attack	8 July 2019	The attack targeted a U.S. vessel, causing critical credential mining. The Coast Guard and the FBI reported that the lack of security strategies on the vessel was the main reason for such an attack. It has been noticed that all crew on the vessel shared the same login and password of the vessel's computer. Moreover, the use of external devices facilitated the task of the hacker. Another critical mistake is the lack of antivirus.	[39]
5.	Phishing attack	2019	Hackers obtained unauthorized access to the computer systems of James Fisher and Sons Pls (UK).	[40]
6.	Ransomware attack	2018	Chinese hackers had attacked US Navy contractors.	[41]
7.	Petya Ransomware	27 June 2017	The attack named Petya affected computer servers in Europe and India. The encrypted malware has been targeted at all services of the Maersk shipping company. As a result, 17 shipping container terminals had been affected and more than USD 200 million was lost. The attack severely destroyed the operating system of the computers by infecting its master boot record (MBR).	[42]
8.	GPS spoofing attack	25 August 2017	The attack is reported by U.S. maritime administration. The GPS of a ship in the Russian port of Novorossiysk indicated a wrong localization. The attack is probably a test of a new GPS spoofing system.	[43]
9.	Navigation Systems attack	June 2017	A collision between the USS Fitzgerald and a container ship, causing the death of 7 sailors. (the coast of Japan)	[44]
10.	Navigation Systems attack	June 2017	A collision between an oil tanker and the USS John S. McCain near the Malaysian coast: the death of 10 sailors.	[45]
11.	Navigation Systems attack	May 2017	A collision between USS Lake Champlain and South Korean fishing ship.	[46]
12.	GPS spoofing	2013	Experience realized by a research team at the University of Texas to spoof a Yacht.	[47]
13.	A computer virus inside the control systems	October 2012	Communication networks installed on the offshore oil and gas platform in the Persian Gulf	[48]
14.	Phishing attacks	2010–2013	The cyber criminals developed a backdoor entry which was called Fucobha: the Icefog (Japanese and South Korean)	[49]
15.	Ransomware attack	August 2011	The shipping lines IRISL (Islamic Republic of Iran Shipping lines)	[50]
16.	Phishing attack	June 2011–2013	Port of Antwerp in Belgium: An organised crime group used hackers based in Belgium to control the computer networks of companies operating in the port of Antwerp.	[51]

2.3. Aim and Objectives

The paper presents the consequences of cyber attacks within the maritime industry through a mapping of current cyber-security provisions on vessels and in ports. A classification of cyber attacks and a mapping of components and services with associated vulnerabilities both on vessel and in port are provided. The major contributions of the paper are as follows:

1. Mapping of on-vessel core equipment/systems and in-port services;
2. Evaluation of cyber attacks;
3. Definition of solutions that mitigate the impact of cyber attacks;
4. Future cyber-security trends.

3. Literature Review

The role of the maritime industry in the transportation sector is currently receiving increased attention ([52,53]) owing to its growing economic importance. However the quest to optimise the efficiencies of industry practices within the sector has motivated migration to increasing levels of digitisation of operations and infrastructures which in turn has resulted in the proliferation of cyber security challenges ([6,54,55]). There is clear evidence that a deep knowledge of skills, strategies and objectives of cyber criminals is a fundamental strand in the goal of establishing secure infrastructures; confidentiality, integrity and availability of sensitive data remain essential targets for hackers. The accepted framework that enables the identification and surfaces routes to the exploitation of system vulnerabilities harnesses attack vectors. A recent example is a model-based tool [56] observed as a three-dimensional matrix, decomposing the problem with different variables such as “attacker” and “target”, identified and quantified maritime cyber-risks. The target application for the development was to facilitate increases in the levels of maritime-cyber awareness and informing the most appropriate decision making. Another example is the MARitime Threat INtelligence FRAMEwork (MAINFRAME) [57] established to aid the collection of threat intelligence and analysis in maritime ecosystems.

The identification of potential in-port cyber threats has also been the subject of significance driven by the interests of governments of the world. A study centered on Colombian ports [58] to identify cyber threats and to carry out a comparison with respect to International Maritime Organization (IMO) recommendations observed a lack of a security plan with enabled easy access to and unauthorized intrusions of on-vessel information systems. Another study [59] based on data collated during two industry workshops from two targeted groups in the sector (one in Europe and the second in Asia) revealed that cyber security is perceived differently between geographies. An insufficiency of protocol and associated tools for the identification of intrusions was demonstrated [60]. The Office of the Chief of Naval Operations (OPNAV), which provides security policies for the US Navy, proposed a limit to the use of portable storage devices and cellular phones to avoid potential cyber attacks [61]. A framework describing guidelines to determine the risk of infrastructure in order to improve security strategies following IEC 63154 standard was reported in [62]. The framework is founded on scanning the shipboard Electronic Chart Display and Information System (ECDIS) using the data gathered from sensors. Results of tests on the Wärtsilä NaviSailor 4000 ECDIS revealed a relationship between the web server and medium vulnerabilities, reinforcing that obsolete versions of software represent a high risk, allowing hackers to execute DoS attacks. The study confirmed the importance of cyber testing within security policies. The classification of hackers by expertise (high, medium and low) or by skills and motivations based on NIST SP800-30 [63] was reported in [64–67]. A defence strategy using mathematical models that identify attacks and guide the selection of the most appropriate training method is detailed in [68].

The Cyber Security National Security Action Plan (CNAP) [69] describes the strategy of the US Government to reduce the risks of cyber crimes on critical infrastructures, comprising solutions to improve cyber protection in the transportation sector. The use of new technologies in Ship Information System (SIS) implementations [70–74] such as the IoT, artificial intelligence and machine learning increases the scope of vulnerabilities and, as a result, entice hackers to invoke new attack classes. As a consequence, these evolving threats have stimulated the extensive development of mathematical models of ship architecture as a foundation for an accurate simulation environment that can predict cyber attacks [75]. Another consideration is the impact of global events on cyber security, and the most striking recent example brings the outbreak of the COVID-19 pandemic; a dramatic increase in cyber attacks on the maritime industry has been reported [76,77] since February 2020 with cyber criminals targeting home computers by using ransomware and phishing emails.

4. The Maritime Infrastructure

The maritime infrastructure can be represented by two essential platforms: on vessel and in port ([78,79]). Descriptions of each platform, the connections between components and the relationship between services are presented in Figure 3.

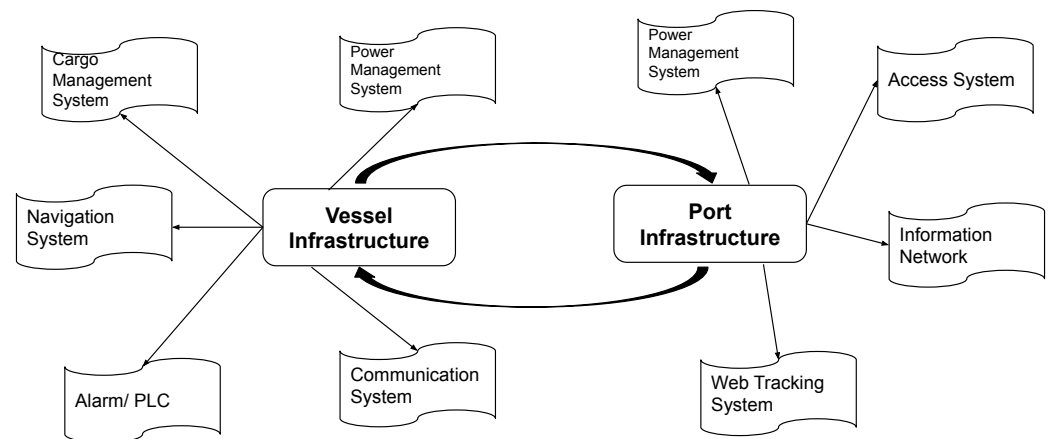


Figure 3. Vessel/port infrastructure.

4.1. On-Vessel Architectures and Services

New technologies and smart communication devices have and will continue to promote advances within the industry. Enhancing vessel design and functionality by using new technologies results in increases in operational efficiencies, the levels of safety and improves the quality of service to customers. As shown in Figure 4, on-vessel infrastructure can be segmented into two systems: electro-mechanical and communications. The former comprises elements related to the engines/power—the safety of which depends on human observation and preventive maintenance—whilst the latter enables exchange of information between port and vessel to facilitate the execution of critical stages of processes within the industry.

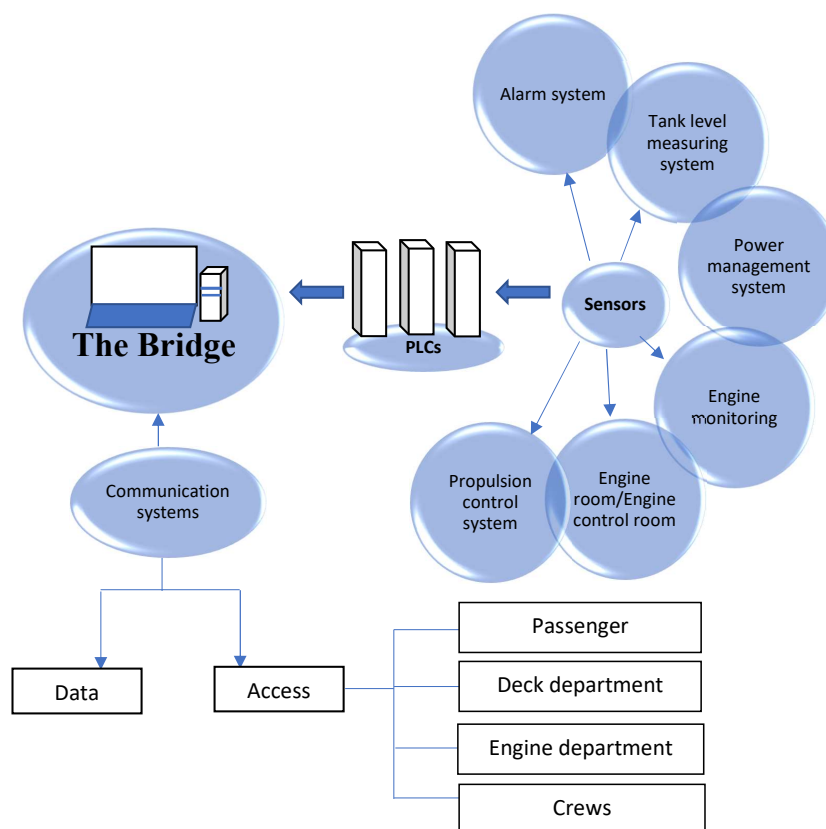


Figure 4. Vessel elements interaction.

4.1.1. Electro-Mechanical and Electronic Systems

Table 3 presents a classification of on-vessel electro-mechanical and electronic components/systems segmented into three groups, power, security and control, and the latter ensures coordination between key function of the vessel.

- A. **Power Management System (PMS):** The primary function of the PMS is to automatically control the diesel generator ensuring optimal performance and power consumption ([80,81]). The stability of on-vessel generators is implemented by using optimal equal load divisions based on real-time information from monitoring and analysis of the load, choosing the optimal operational settings under particular conditions [75].
- B. **Engine:** The selection of the most appropriate engine depends on the size and the type of vessel. Diesel turbines are the most popular, transforming thermal into mechanical power [82], and other usages include wind, nuclear and solar energy [83] depending on the weather condition and the duration of available sunshine. Hybrid diesel/electric engines are used on some vessels, mostly adapted to large ships, providing high power and constant torque at the expense of complex and expensive installation. A recent trend, in an effort to ensure more security and safety, has been on remote engine control (autonomous vessels).
- C. **Main Switchboard:** The main switchboard maintains the total control of a vessel's functions, providing real-time data on the status of engines, key sensors and presents alarms. It is fundamental that the on-ship electrical systems, including the main switchboard, is earthed.
- D. **Programmable Logic Controllers (PLCs):** Generally, PLCs are used to automate a process and on-vessel PLCs are combined with the power management system, alarms and engines ([84,85]). PLCs are integral to the control of the navigation system and to prevent defaults delivering high operational efficiency with low maintenance cost. Moreover, PLCs provide critical data such as temperature, engine status, pressures

and electrical defaults, as well as information to execute the overall management of the vessel.

- E. **Water Ingress Detection System (WIDS):** Each vessel must be equipped with a WIDS-Based, a regulated requirement under SOLAS Chapter XII Reg.12. If a specific level of water is detected, an audible and visual alarm must be issued. WIDS systems must be powered by two different systems and an alarm is raised if the primary source fails.
- F. **Bow thrusters:** The bow thrusters are used at low speed for efficient maneuvering. Large vessels are equipped with tunnel thrusters driven by electric motors, regulating the ship's resistance through the water, which is critical to successful docking.
- G. **Emergency Shut Down (ESD):** The ESD is activated in an emergency such as fire detection and overfilling of tanks by executing a sequential shutdown of on-vessel pumps and valves to ensure safety and reduce damages. A rapid ESD response time is mandatory.
- H. **Marine Heavy Fuel Oil (HFO) Treatment System:** The HFO produces power from the energy extracted from the burning process and is used by most commercial ships [86]. The HFO is treated before use in the following stages: Firstly, HFO is heated to 50–60 °C and then connected to an inlet pump. The solution is subsequently heated to 80 °C and treated with a centrifugal purifier. The fuel is ready to be used after being processed with a centrifugal clarifier.
- I. **Fuel Oil System (FOS):** The FOS is a system that provides the fuel to the injection system and secondly an injection mechanism for receiving, storing and distributing to the tank. The FOS is composed of several essential parts: piping, stocking, distribution and the treatment of fuel oil.
- J. **Lubricating Oil System (LOS):** LOS is a fundamental internal subsystem of the engine, ensuring the efficiency and a long operational lifetime of the machine. A number of lubrication oil systems were used, the most popular being Hydrodynamic Lubrication (HL). HL produces a layer of oil between the moving parts, e.g., a layer of oil is covered by the main bearing, ensuring the motion of the crankshaft' journal.
- K. **Starting Air System (SAS):** The SAS is composed of two air compressors and two reservoirs to generate the minimum 28 bars for the engine to start. For safety, valves are installed in the reservoirs to discharge the air in over-pressure cases.
- L. **Gyro compass:** The gyroscope is an essential tool used for navigation, providing an indication of the true north with deviations as a function of the direction and the speed of the vessel ([87,88]). The most important feature of this component is the total ineffectiveness of external magnetic fields.
- M. **Echo-sounder:** The echo-sounder measures the depth of the sea. A sonar signal is transmitted and the 'echo' received, with the time between the two operations determining the depth. The information given by the sensor is used for a number of purposes.
- N. **Electrical Crane Equipment:** On-vessel cranes load or discharge goods and equipment. Therefore, their regular maintenance is mandatory as downtime can compromise ship operations. Visual inspection of the cranes for damage is carried out by the chief engineer and reported immediately for scheduling repairs([89,90]). General maintenance is required to ensure uninterrupted operation with a particular focus on the protection of electrical systems against water ingress.
- O. **Navigation Lights:** Light signals are used to communicate dangerous actions, e.g., navigation lights in vessels play an essential role in preventing collisions as a visual signal has been proven to illicit rapid reactions, which is core to the prevention of critical events.
- P. **Loading and Stability Computer:** The on-board loading computer provides standard functions and stability scenarios as, under specific circumstances, the captain needs to know the status of several components in order to inform the optimum plan of intervention to resolve an operational challenge.

- Q. **Fresh Water Generator (FWG):** FWG produces freshwater from seawater, primarily for drinking but also for use by several other on-vessel components. The FWG consists of a condenser and evaporator, as the process is based on evaporating seawater using a heat source and decreasing atmospheric pressure by creating a vacuum in the evaporating compartment, and the decrease in temperature allows the transformation of vapour to cool water.
- R. **Central Cooling Water System:** A range of on-vessel equipment requires cooling to maintain their efficiency and reduce the loss of heat energy. Generally, two kinds of cooling systems are used on ships: a seawater cooling system, and the other using freshwater—the central cooling system—to control the temperature of the engine room. The central cooling system comprises three circuits: a seawater circuit in which the seawater cools freshwater; a low-temperature circuit used in low-temperature components of the machine; and a high-temperature circuit.
- S. **Waste Incinerator Plant:** According to regulation 16 of MARPOL Annex VI [91], ships must install an incinerator to transform waste into flue gas and heat by burning. It must, however, be noted that the process outputs hazardous smoke that both pollutes the environment and causes several diseases such as cancer.
- T. **Sewage Treatment Plant:** The treatment of sewage before discharging into the sea is mandated by regulations. A biological method based on anaerobic bacteria, in which the sewage is decomposed and generates H₂S and methane gases, is the most popular technique. The alternative method, Sewage Treatment Plant (STP), relies on a screen filter to remove all solids, a biofilter decomposing organic substances by the aerobic micro-organisms and a pump.
- U. **Air Condition Plant:** The refrigeration or air-condition plant maintains a stable temperature of living quarters and the quality and protection of transported goods. Therefore, the refrigeration system must be regularly charged with refrigerant gas.
- V. **Stabilisers:** Roll stabilization systems, classified as passive and active, are used to maintain the stability and reward motion caused by the sea. Bilge Keels are the most used passive systems, and their motion opposes rolling. Anti-Rolling Tanks are active systems based on tanks at the sides of the ship.
- W. **Anchor and Mooring Winch Control System:** Anchor and mooring systems operate automatically to control anchors and moorings by using actuators to keep a steady tension. The winch is equipped with a frequency converter and PLC controller to monitor the motor and to guarantee an ideal pulling speed.

Table 3. On-vessel components classification.

Power and Electronic Components	Communication Components	Services and Management
PLCs	ECDIS	Cargo Management
SCADA	GPS	Nautical Decision Support
Power Management	VHF antenna	Bon Voyage System (BVS)
Engine	IDS	Voyage Data Recorder (VDR/S-DR)
Water Ingress Detection System	The Ship Information System (SIS)	Fleet Management System (FMS)
Bow thrusters	Navigation Equipment	Passenger/Visitor Services and M.S
Propulsion, machinery, and power control systems	Passenger-facing networks	
Engine Control Room Console	Internal Communication	
Engine Governor System		

Table 3. Cont.

Power and Electronic Components	Communication Components	Services and Management
Access Control Systems <ul style="list-style-type: none"> • Closed Circuit Television (CCTV) Camera System • Maritime safety management • Bridge Navigational Watch Alarm System (BNWAS) • Shipboard Security Alarm Systems (SSAS) 	Core Infrastructure <ul style="list-style-type: none"> • Routers • Firewalls • Switches • Wi-Fi • VPN • IDS/IPS • Speed and Distance Log Device (SDLD) 	
Emergency Response System	Integrated Bridge systems	
Air Condition Plant	RADAR	
Sewage Treatment Plant	Echosounder	
Anchor and Mooring Winch Control System		

4.1.2. Communications Systems

On-vessel communications deliver information exchanges between ship elements.

- A. **Internal communication** : VHF communications plays an important role in the safety of the ship, for example, in requesting assistance and/or transmitting a distress message. Furthermore, hand-held VHF is also used for applications such as localization by authorities. The Global Maritime Distress and Safety System (GMDSS) uses satellite and terrestrial communication to connect with authorities ([92,93]) throughout international voyages, which is a mandatory requirement. Digital Selective Calling (DSC) is another means of transmitting distress message transmission and the current position of the ship.
- B. **Network**: Networked systems within the maritime industry are designed with high levels of reliability due to business critical data generated by a suite of sensors and the necessity to manage communications. The networked information systems gather and process data from sensors and execute on the exchanges the information between equipment. Table 4 summarises that several types of network technologies used for information transport, for example, the U.S. Navy uses a fiber-optic infrastructure (SAFENET) [94].
- C. **Navigation**: The GNSS is recognised as the most vulnerable infrastructure within the maritime industry with respect to potential cyber breaches [95]. The network of satellites provide, in real time, the location and speed of ships and, in turn, the time remaining to destination. The Global Positioning System (GPS), GALILEO, and GLONASS provide flexibility and easy public access ([96–99]), and they are rich attack surfaces for a hacker to inject fake information or degrade the fidelity of the signal.
- D. **RADAR**: RADAR is a core tool in collision-free navigation and in the control of ever increasing levels of maritime traffic. All vessels must be equipped with the capability as mandated by Regulation 19 presented by SOLAS Chapter 5 ([100,101]). Marine radars utilise two frequencies bands, 10 GHz and 3 GHz, most readily yielding accurate distances between the ship and other detected objects.
- E. **Passenger-facing networks** include the following:
 - Passenger segregated WiFi or Local Area Network (LAN) Internet access: The provision of high quality on-ship Internet access for both passengers and crews is non-negotiable. The on-sea options are limited and the service is only reliably delivered through satellite connections. Specific on-vessel hardware is required and the cost of the service is often prohibitive. VoIP services are not possible as satellite connections are subject to significant latency.

- TV-Entertainment system: Similarly, the provision of TV entertainment is a necessity. Satellite-delivered TV is the only option, and examples include SAILOR or Sea Tel systems.
- F. **ECDIS:** The Electronic Chart Systems (ECS) ECDIS system is a mandatory real-time navigation tool providing essential on-ship information. Regulated by the International Maritime Organization (IMO) as a replacement for the more traditional approach using paper-based nautical charts, the system eases the planing of journeys considerably by reducing effort and in the optimisation of speed. The ECDIS is a real-time system that provides the location of the ship as it is connected to both the RADAR and AIS system.
- The ECDIS generates several chart, such as Electronic Navigational Charts (ENC) and Admiralty Raster Chart Service (ARCS) provided by hydro-graphic offices; updates of the ECDIS are vital using the Internet or e-mail ([102,103]). The update is loaded into the planning station most readily by using a USB or e-mail, followed by the export of data and refresh of ECDIS status.
- G. **Cargo Management:** The cargo management system in commercial vessels optimises efficiency in the management of goods. The application uses a dynamic database in which details of the progress of the cargo are updated, where it has been stored and tracked from the port to final destination ([104–106]). The system also provides information on stock status and informs plans to prevent losses.
- H. **Automatic Identification System (AIS):** The AIS provides static, dynamic and voyage-related data according to the Safety Of Life At Sea (SOLAS) convention, refs. ([107–109]). AIS data are detailed in Figure 5; thus, the mappings of the architecture of the vessel and the transmitted signals are both essential to the identification of its vulnerabilities. A successful strategy to exploit vulnerabilities within AIS and to define attacks that an impact the vessel is based on the following:
- Identify vulnerabilities;
 - Gather information about the infrastructure;
 - Map the architecture of the information system.

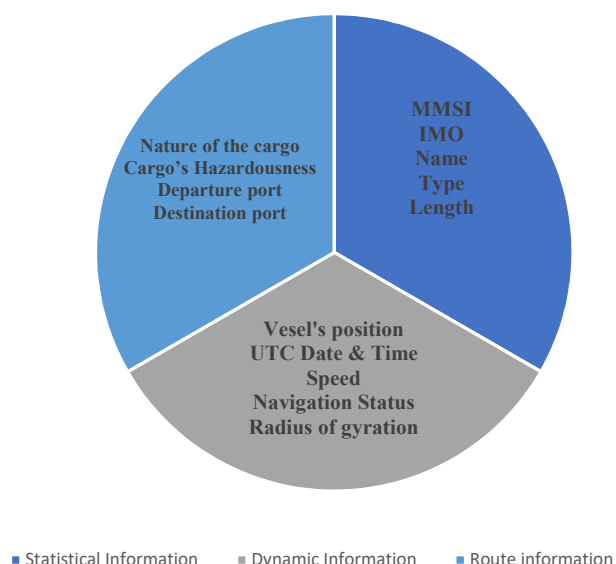


Figure 5. AIS data.

The AIS architecture (Figure 6) is essentially composed of the following:

- **Time-division Multiple Access (TDMA):** Communication between vessels shares the same frequency, and the transmitted frame is divided into time slots, each one containing data such as location and the identity of the vessel. As presented in Figure 6, the duration of the frame is 60 s, and it is divided into 2250 time slots.
 - **Digital Selective Call (DSC):** The International Telecommunications Union (ITU) recommends the necessity of the DSC, as it is responsible for issuing alerts to a rescue authority anywhere in the world. It also allows vessels to receive distress calls from others. A fault in the DSC could have serious consequences.
 - **Gaussian Minimum Shift Keying (GMSK):** The GMSK modulation is characterized by high spectral efficiency and low inter-channel interference.
 - **Global Navigation Satellite System (GNSS):** A GNSS provides the location of a vessel using networked satellites and is operated by the AIS.
- I. **The Ship Information System (SIS):** The development of electronic devices and the advances in communication technologies in military vessels have been central to high performance Ship Information Systems (SIS) that have improved services on and enhanced the safety of ships. As shown in Figure 7, SIS consists of the following:
- Sensors;
 - Network architecture;
 - Information processing;
 - Information transmission.

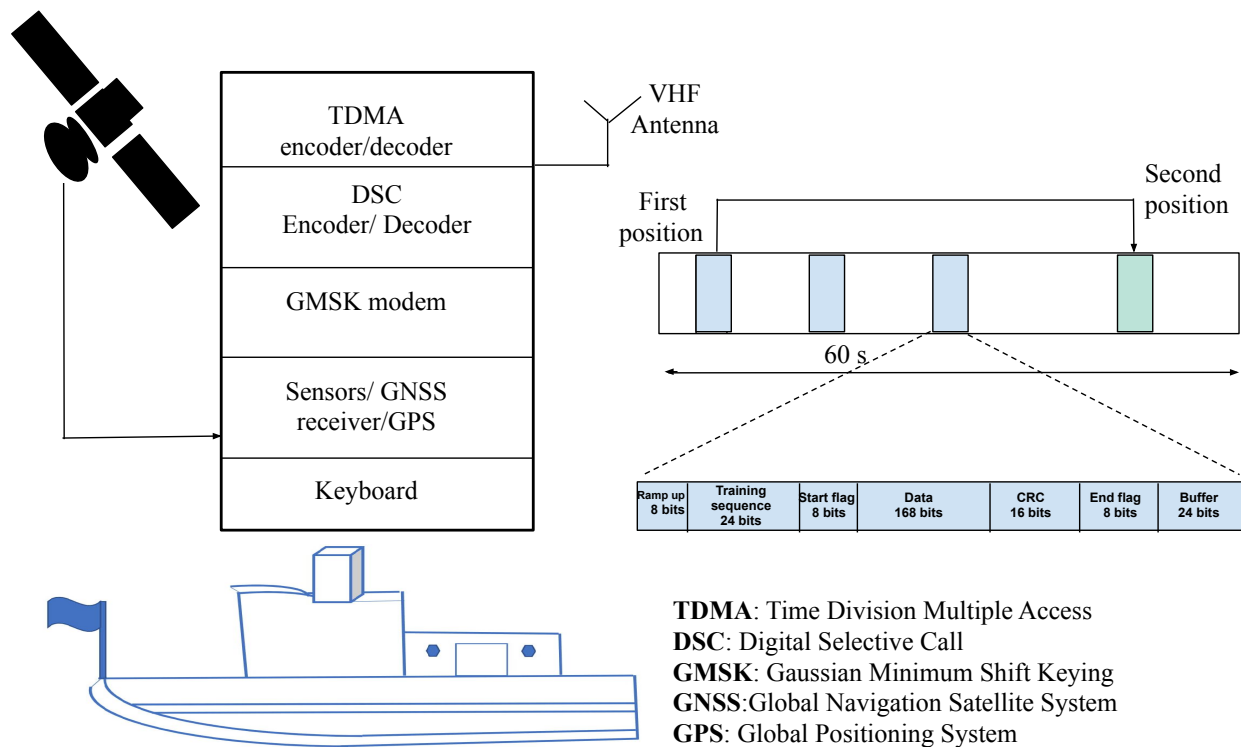


Figure 6. Simplified AIS class A architecture.

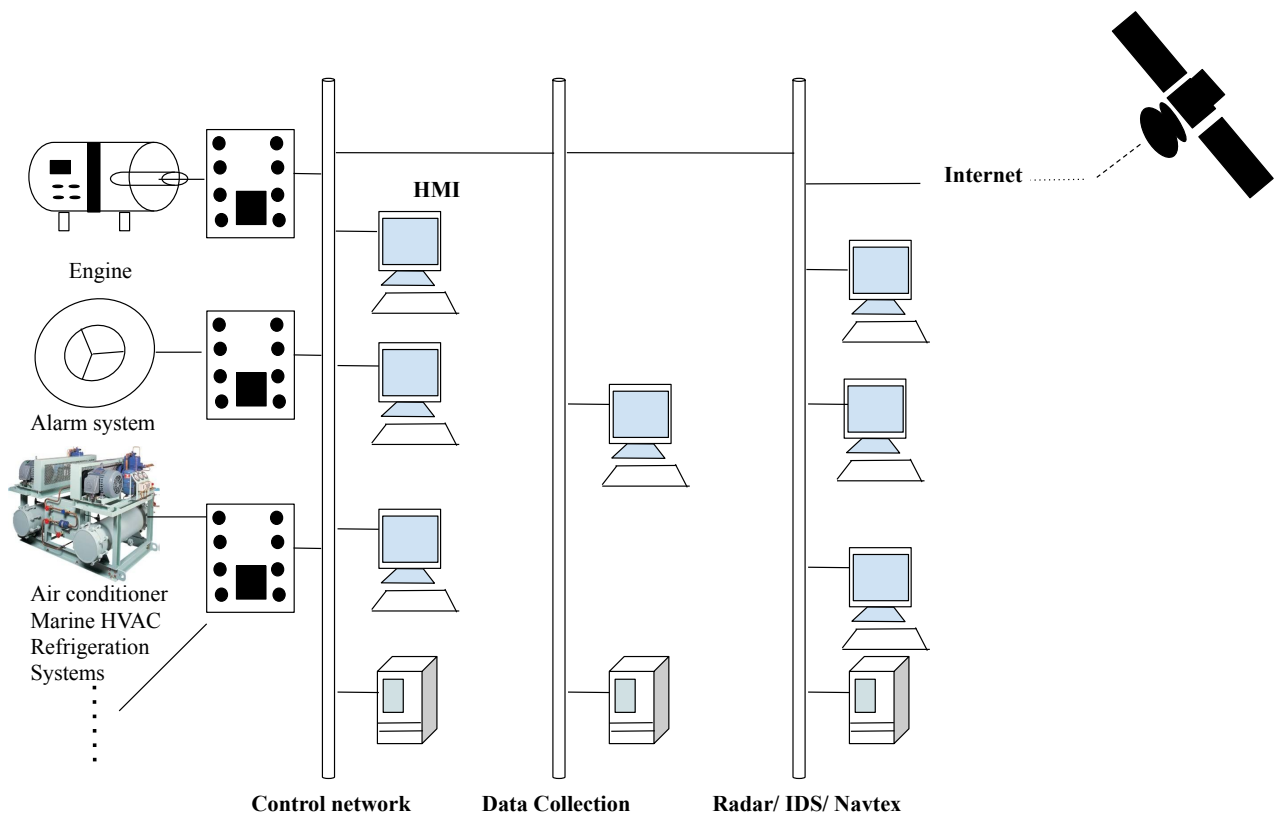


Figure 7. Ship Information System architecture.

4.2. The Port Infrastructure

The port is the interface between the vessel and land. The management and efficient execution of transportation and tracking of goods and vessels are heavily reliant on in-port service quality. The port is the home of three important groups of services (Figure 8): all services related to vessels, commercial transportation and tracing services and a set of facilities linked to security.

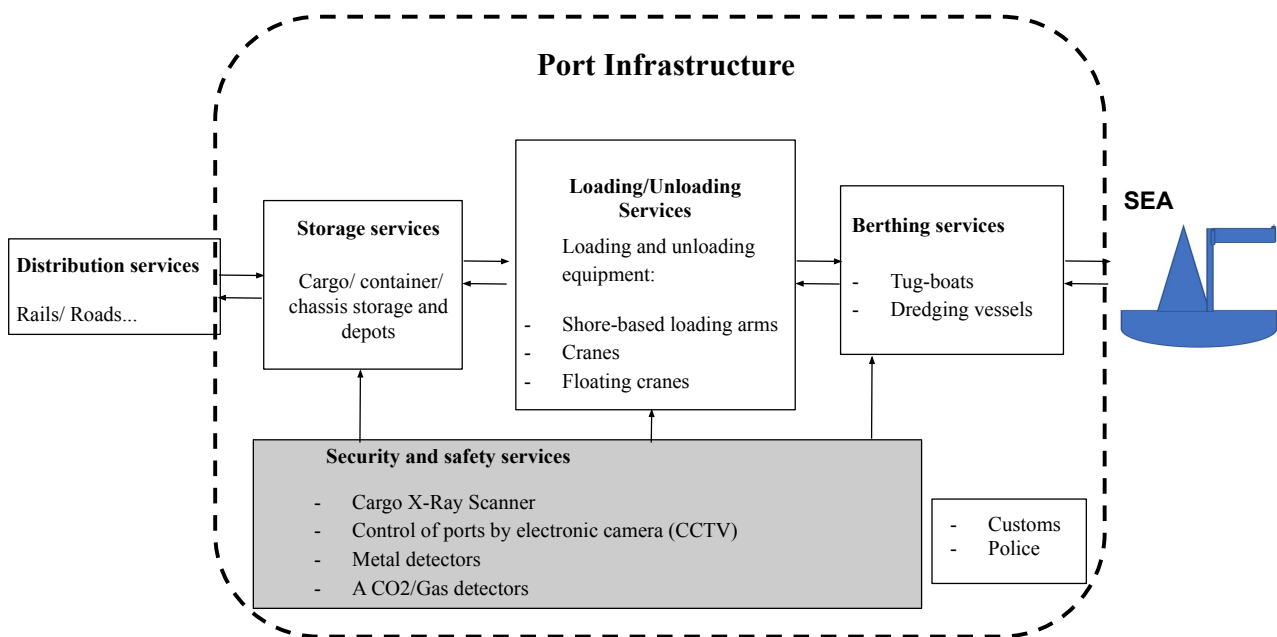


Figure 8. Port architecture.

Table 4. Network types.

Network	Specification	Ref.
SHIPNET	A real-time messaging system/IEEE 802.2 LLC and 802.5 standard	[110,111]
SAFENET	Survivable Adaptable Fiber optic Embedded NETwork/US Navy's combat ships	[94,112,113]
C3I system	Command, Control, Communication and Intelligence/Supervisor controller systems	[114,115]
RICE 10	Digital internal communications system	[116]
SHIP system 2000	Using nodes for routing	[117]
Smart Ship	linking the different systems by the the ship area networks	[118]
TSCE	Total Ship Computing Environment	[119]

4.2.1. In-Port Safety

The following are several safety-enteric capabilities/services that target the delivery of the effective security of people and to safeguard life.

- Cargo X-ray Scanner: In port, the optimisation of the time to execute key tasks is essential. X-ray reduces the inspection time of containers and plays a fundamental role in the safety of the port by detecting suspicious goods.
- Control of ports by electronic camera (CCTV): The port is a critical space that requires the real-time control of dynamic human and vehicle activity. IP-HD camera-equipped CCTVs monitor the environment in real time, and the quality of the images enables monitoring the port with high precision, increasing security and minimising human intervention.
- Metal detectors: The International Ship and Port Facility Security Code (ISPS) proposed by the IMO under the SOLAS Convention, Chapter XI-2, mandates the use of metal detectors to protect port operations, ensures the safety of the workers and counters terrorism [120].

4.2.2. In-Port Operational Equipment

- Cranes: The recent trend in the utilisation of new technologies in the quest to improve service delivery has also targeted next generation cranes. The use of micro-computer and wireless connectivity communication has implemented their remote control but this evolution has also created new vulnerabilities for hackers to assume control with malicious intent to create significant damage.
- Tugboats: Tugboats are essential for maneuvering large-size vessels in port by towing large vessels through narrow water channels. Generally, a tugboat is equipped with diesel engines and firefighting equipment.
- Dredging vessels: Dredging maintains the required in-port water depth by removing disposals such as sand and sediments. Dredge vessels can be mechanical or hydraulic.

4.2.3. The Port Community System (PCS)

PCS is a platform that provides port users with real-time information about the tracking of goods and managing the declarations of customs ([121–123]). Ready access to the most relevant information at the right time at each stage of port operations minimises delays, reducing paperwork and enhancing the quality of services.

- Core module: contains general services information such as the name and IMO number of each vessel. The interface presents user profiles, allowing changes of passwords and databases searches. For security, access to the system is allowed only to authorized users as, for example, confidential information such as the number of crew members and passengers details are at risk.
- Cargo module: contains information related to cargo such as the type and quantity of goods, the date/time of arrival/departure and editing services. The user is allowed to verify certificates related to the cargo.

- Tracking and tracing module: These modules source information from the AIS system. The user is able to visualize the real-time trace of the vessel and can view the CCTV video stream. Interrogation on the departure and arrival of the vessel is also available.
- Berth management module: organizes the berthing of a vessel by providing real-time information related to the operation. The user is able to generate the berthing plan automatically and accesses information such as loading/unloading times by using the interface. The user can also extract a graphical representation of the berth to guide the execution of a successful berthing by port workers.
- Storage allocation module: provides a graphical representation of the warehouse to optimise the collection of particular goods.
- Interface to other transport modes: provides services related to the link between the storage area and the next transportation mode. The interface facilitates the governance of goods and provides real-time statuses of shipments.
- Billing module: creates and manages all invoices. The interface provides berthing data and collects all information related to energy and water consumption.
- Statistics module: provides periodic updates and creates statistical reports concerning previous operations and generates alerts on specific anomalies related to port services.

4.2.4. Single Window (SW) Environment

The SW facilitates communications between ports by standardizing services related to international goods transportation and unifying rules between governments ([124,125]). All documents, including authorizations and certifications, are submitted once through one input for all users yielding a considerable gain in time and cost as all government authorities have adopted the same governance with respect to marine transportation. SW optimises international maritime trade by obviating differences between nations in terms of governance and information systems and is a formal system for tracking the transportation of illegal products and limiting suspicious relationships.

4.2.5. The Maritime Transport Life Cycle

The port/container terminal is an intermediate environment in the transport of goods, a temporary storage area allowing the preparation of containers before the vessel's loading phase. Consequently, the management of the terminal is vital to efficient container transportation. The terminal comprises four subsystems ([126,127]):

1. Ship-to-shore: carried out by quay cranes (QR) to load or discharge the ship, conducted with references to a specific plan executed by the operator.
2. Transfer: transferring the container from the QR to the storage area using crewed or automated vehicles.
3. Storage: serves as a buffer, necessary to optimize the waiting time, due to the lack of synchronization between loading and unloading phases.
4. Delivery and receipt: The container is transferred by means of a port's internal vehicle to the trains or barges for onward delivery to the final destination. The time taken to execute this final port phase depends on the location of the container.

5. Cyber-Attacks in the Maritime Industry

Table 5 presents a classification of cyber attacks and their associated vulnerabilities as a function of key equipment and systems.

Table 5. Attacks classification and security impact.

Index	Localization	Attacks	Vulnerabilities	S.I		
				C	I	A
1.	AIS	Liste1: • Spoofing • Frequency mapping • Timing attack	Liste1: • Open system • Lack of encryption algorithms	•	○	•
2.	R and RC	Liste1: • Spoofing using GPS	Liste1: • Insufficient data protection • Autonomous Vessels • Vessel Identity Theft (GPS spoofing)	•	•	•
3.	PM/PCS	Liste1: • Spoofing	Liste1: • Usage of digital systems • Integration with communications equipment	○	○	•
4.	AS	Liste1: • Spear-phishing technique • Key loggers installation • Malware attack • Viknok Trojan	Liste1: • Insufficient e-mail protection • Using external devices	•	○	○
5.	ALS	Liste1: • General attacks	Liste1: • Equipment connected to the internet	•	○	•
6.	CMS	Liste1: • Spoofing • Man-in-the-middle attack	Liste1: • Shipment-tracking tools • The tracking is via the internet	•	•	○
7.	B.S	Liste1: • DoS attack	Liste1: • Using of removable media for update	○	○	•
8.	PCMS	Liste1: • DoS attack • Spoofing • Malware attack	Liste1: • Digital systems • Access control	•	•	•
9.	PPN	Liste1: • All kinds of cyber-attacks	Liste1: • Internet connection	•	•	•
10.	ACWS	Liste1: • All kinds of cyber-attacks	Liste1: • Computer networks of the ship connected to the internet	•	•	•

5.1. On-Ship Cyber-Attacks

1. **AIS attack:** The flowchart presented in Figure 9 maps the signal processing steps for Automated Indicator Sharing (AIS), providing the framework to examine vulnerabilities and to capture the behaviour of the hacker. The identification of the data is carried out by calculating the Frame Check Sequence (FCS); the 6-bit ITU-T Cyclic Redundancy Check (CRC) polynomial equation is also presented in the flowchart. The transmission of a message by the hacker in the appropriate radio channel of the AIS receiver utilising a FCS similar to the calculated FCS of the target AIS decoder executes a successful spoofing attack, potentially resulting in a collision between ships. The hacker could perform the following ([128–130]):

- Change the localisation: latitude, longitude and altitude;
- Inject a false message.

The model of the transmitted on-ship AIS signal is provided by the following ([131–133]):

$$S_{AIS}(t) = \exp i\phi(t, I) \tag{1}$$

with the following.

$$\phi(t, I) = \pi \sum_{k=0}^n I_k q(t - kT) \tag{2}$$

$nT \leq t \leq (n + 1)T$, $I_k = \pm 1$ and $q(t)$: Gaussian wave form given by the following:

$$q(t) = \int_0^t g(\tau) d\tau \tag{3}$$

with

$$g(t) = Q\left[\frac{2\pi B}{\sqrt{\ln 2}}\left(t - \frac{T}{2}\right)\right] - Q\left[\frac{2\pi B}{\sqrt{\ln 2}}\left(t + \frac{T}{2}\right)\right] \tag{4}$$

and the following obtains.

$$Q(\alpha) = \int_{\alpha}^{\infty} \frac{1}{\sqrt{2\pi}} \exp -x^2 dx. \tag{5}$$

At the satellite receiver, the AIS signal is provided by the following.

$$r_{AIS} = AS_{AIS}(t - \tau) \exp i(2\pi f_D t + \theta) + n(t) \tag{6}$$

2. **Global Navigation Satellite Systems (GNSS):** GPS (US), GLONASS (Russia), Galileo (EU) and BeiDou (China) all fall under the Global Navigation Satellite Systems (GNSS) umbrella. Cyber attacks on GNSS have been—facilitated by the lack of authentication and encryption—rendering the system vulnerable to breaches [134,135]. Fake position information significantly increases the probability of collisions, and the most striking exemplars occur in the Black Sea. Equation (7) and Figure 10 presents the GPS method to determine position. A GNSS spoofing attack is carried out in two steps: synchronization with the satellite’s signal followed by increases in the power of the transmitted signal.

As shown in Figure 10, the position (x,y,z) of GPS receiver is the intersection of d_0, d_1, d_2 and d_3 with the following:

$$d_i = \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} - \sqrt{(x_0 - x)^2 + (y_0 - y)^2 + (z_0 - z)^2} \tag{7}$$

with $i \in [0, 3]$.

The local time is given by the following:

$$t_l = t_n + \frac{\sqrt{(x_n - x)^2 + (y_n - y)^2 + (z_n - z)^2}}{c} \tag{8}$$

with t_n being the transmitted time, x_n, y_n and z_n are the positions of satellite n and c is the speed of light. The highest levels of protection of location data are mandatory for the successful operation of a fleet of autonomous vessels. Therefore, a significant body of research on GNSS spoofing attack detection has been undertaken [134,136–138]. In [139], spatial processing methods are used to determine sources of the signal. Recently, a GNSS detection method based on deciphered Ring Alert (IRA) messages transmitted by the IRIDIUM satellite has been reported [134]. The proposed method maintains an acceptable receiver complexity and satellite signal availability.

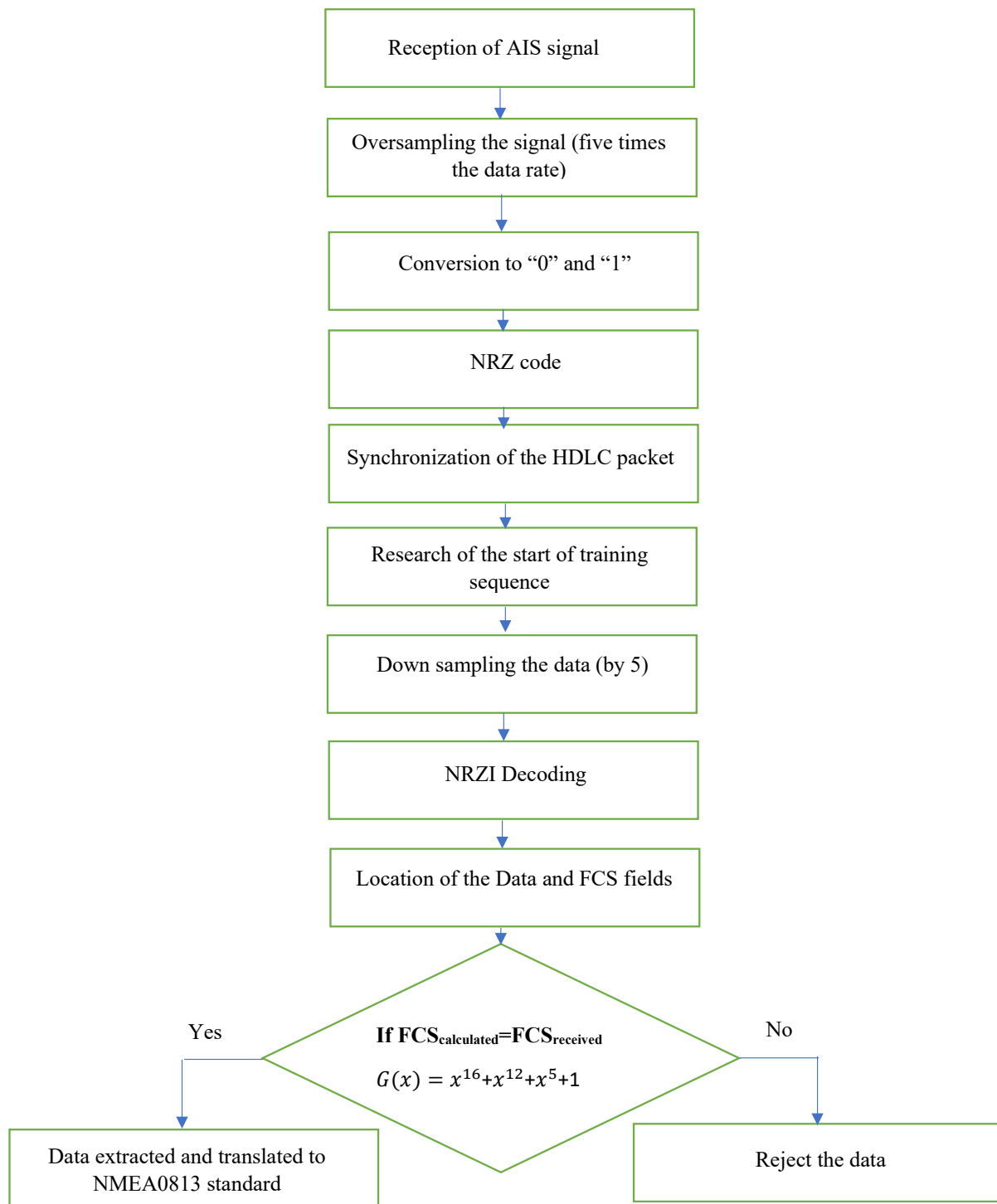


Figure 9. AIS decoder.

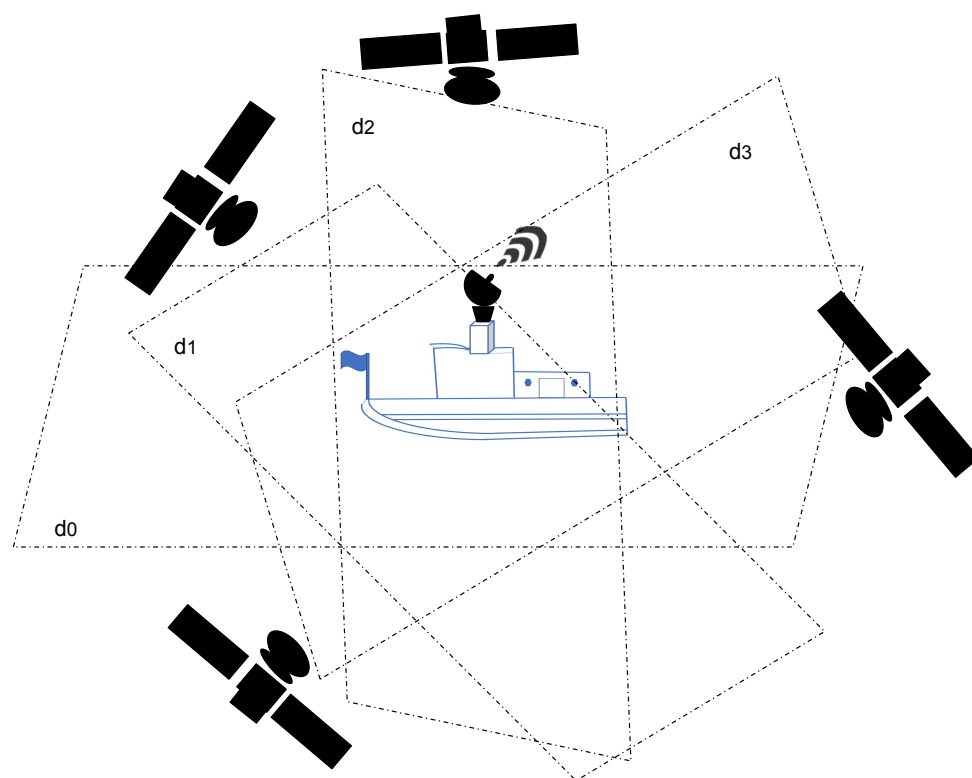


Figure 10. GPS receiver position.

5.2. In-Port Cyber-Attacks

- A. **Spear-phishing:** Spear-phishing, created by e-mails containing suspicious links to obtain unauthorized access, is one of the most common attacks ([140–142]). After accessing the information system, the hacker installs key-loggers to capture logins/passwords and determines the identity of the individual workers, building a precise mapping of the status of the port. Although a substantial number of spear-phishing attacks occur, due to the sensitivity of the maritime sector, port managers prefer to keep reporting to a minimum as breaches affect not only confidentiality of individual but also economic relationships between nations.
- B. **Distributed Denial of Service (DDoS):** Distributed Denial of Service (DDoS) attacks are criminal acts. The port information system is compromised by flooding the network with excessive traffic levels and denying access to its sites ([143,144]). As a result, maritime services and the ability to track goods are compromised. The impact of DDoS attacks on cyber-physical maritime systems is evaluated in [145] by using simulation. The model comprises a vessel, controller and a gate with the simulated attack targeting communication between these different elements, and performing this exceeds the time safety limit.
- C. **Port Scanning:** Attackers verify the most vulnerable network ports by using the classic technique of scanning. The goal is to discover the status of services, define the optimum strategy to access databases and identify which users monitor services. At the highest level, the attacker uses IP fragmentation to confuse the firewall, and, as a result, the packet filters are bypassed. Another technique is based on interrogating an open User Datagram Protocol port—the fourth layer of OSI model layer (Transport Layer)—to scan IP addresses by testing several protocols and other ports. The test-models used by a hacker are randomly generated [146]. TCP-wrappers are preferred in order to mitigate such attacks, empowering the network manager to allow or block server access depending on the IP address.
- D. **Supply chain:** Supply chain attacks center on creating damage through the most vulnerable part of the end-to-end network ([64,147]). International shipping from origin

to final destination relies on key processes and stakeholders for container tracking, assurance and international authorizations. The most easily understandable example of a damaging outcome of an attack is changing the destination of a container, which requires knowledge of the supply chain and the vulnerabilities therein, to modify critical information.

- E. **Social Engineering:** Generally, social engineering attacks depend on the exploitation of human curiosity or compunction to execute a malicious act ([148,149]). The study of human behaviour is core to a successful attack, and in this respect, social media or instant messaging usage patterns are a means for hackers to gather information on in-port network activity. As an example, the hacker can obtain critical information by creating a false identity through Facebook/Instagram. Other classes of social engineering attacks are Baiting and Quid Pro Quo. Software updates by security managers through a USB is often the means to install malware, a file used by the hacker to obtain access to the system. Protection based on strictly applied security policies is the only method to mitigate such attacks.
- F. **Malware/Ransomware/Trojans:** Generally, the aim of these classes of attacks is to damage the information system or server by targeting the networked computers ([150–154]). On the 8 July 2019, an attack targeted a US vessel causing critical credential mining. The Coast Guard and the FBI reported that the lack of security strategies on the vessel was the main reason for enabling such an attack; all of the crew on the vessel shared the same login and password of the vessel's computer. Furthermore, the use of external devices and the absence of antivirus software protection facilitated the task of the hacker. The second example is the attack of the 27 June 2017, named Petya, that affected computer servers in both Europe and India. The encrypted malware targeted all services of the Maersk shipping company, affecting 17 terminals and inflicting damages in excess of USD 200 million. The attack destroyed the computer operating system by infecting its master boot record (MBR).

6. Internet of Things in Maritime Industry

The IMO created the International Safety Management Code (ISM) and International Ship and Port Facilities Security Codes (ISPS), and they are the standards that are followed to ensure safe shipping and harbour operations, also encompassing the safety operational codes of personnel both on shore and on vessel [155]. The industry has recently adopted new technologies with the goal of optimising evolution to digitalisation. One route has deployed Internet of Things (IoT), a technology platform that interconnects 'objects' through the Internet to exchange data [156]; within the maritime industry, the 'things' connected are predominately sensors monitoring operational equipment and environment. A suite of appropriate sensors has been deployed in on-vessel ships and in-port operations to reduce the risk of vital component failures due to negligence as well as increasing the efficiencies of key practices ([157,158]). More extensive monitoring provides real-time information such as cargo temperature, gas emissions and other vital data that can inform the optimisation of operations, thereby lowering the cost of maintenance and increasing the safety of the entire ecosystem [155]. However, the growing reliance on data and complex network connectivity has gated a proliferation of new vulnerabilities that cyber attackers are leveraging to launch attacks.

6.1. The Role and Impact of IoT On-Vessel and In-Port

Sahay et al. [159] provided a detailed insight on the on-vessel role that sensors and actuators are playing in ship automated systems, becoming an integral part of the physical components of the bridge, engine and propulsion control systems. The generated data are central to on-ship key systems, most notably the Integrated Bridge Control and Autonomous Engine Monitoring Controller. Visualisation and analysis enabled by the multiple streams of data inform on entire on-vessel operations, a full view of the critical system components and associated IoT devices with their inter-connectivity. However,

the resultant increase in levels of automation creates new security vulnerabilities [160]. The components integral to the bridge, engine and propulsion control have been largely discussed in Section 4.1; thus, this subsection is devoted to a mapping of reported IoT-enabled cyber attacks both on vessel and in port.

6.2. Data and IoT

The use of data gathered using IoT to derive meaning has recently gathered pace [161]. There is a body of evidence on the benefits of the use of Industrial Internet of Things (IIoT) in safety-critical industrial applications. Big Data Analytic (BAD) tools have now been proven to enhance productivity within the maritime industry. The ability to have access to more information practical methods of acquiring large volumes of data has enabled the control of physical resources, processes and environments. Al-Gumaei et al. [162] have explored the inter-relationship between IIoT and the beneficial business benefits from data.

The use of Big Data in maritime traffic data analysis has been categorised under two regimes: on-vessel traffic and external information such as in wind, sea and tidal wave in [163]. For example, an estimate of real fuel consumption function for speed optimisation has been achieved using archived weather data in [164]. Brouer et al. in [165] provided insights into the future of integrating predictive Big Data analysis in solving large scale optimisation. Nita and Mihailescu in [166] and Mirovic et al. [167] reported the use and applications of IIoT in real-time decision support.

6.3. Attack Surfaces in IoT Devices in Ships and Ports

The type of IoT-associated cyber attacks depends largely on IoT technology implementation—architectural design and components modus operandi and the protocol and application areas [168]. Furthermore, the vulnerability exposure of IoT can only be deciphered by having knowledge on component inter-dependencies, strengths and weaknesses.

IoT attack surfaces are all the areas of the system an attacker can exploit so as to achieve authorised access in order to change the originally designed behaviour; steal or compromise data [168]; obtain essential a priori knowledge that helps identify the potential types of attack the system is vulnerable to; and, in turn, inform the optimum countermeasure. Examples of attack surfaces are as follows: Network Link by leveraging on any network-layer protocol vulnerabilities; Application Link through application-layer protocol vulnerabilities; network design flaws; and weak password key management [169].

IoT has inherent security challenges owing to bi-directional data storage and retrieval methods from the cloud [170]. Once this access and retrieval line of action is compromised, the entire system is compromised. One example of IoT-based attacks is LogicLocker (a self-spreading ransomware worm) [169,171], which is enabled through Programmable Logic Circuits (PLCs). Another example includes attacks on IoT-enabled field devices such as an Automated Tank Gauge (ATG) and small-scale SCADA systems that monitor fuel tank inventory levels and raise alarms, for instance, when a fuel spill is detected [169].

7. Future of Maritime

This section focuses on cyber-security concerns with regard to advancements in maritime industry. This is performed by looking at the concept of autonomous or unmanned vessels and the possible attack surfaces that exist therein for the research community in cyber security. This concern is raised by taking a cue from already existing unmanned systems and their various existing attack surfaces that attackers exploit to cause harm by gaining authorised access resulting in stolen data and information and system compromise.

7.1. Autonomous Vessels

Two classes of autonomous vessels—in this context defined as a self-driven vessels piloted by artificial intelligence—have been the subject of significant research and development: remotely monitored and operated vessel by shore-side operators and independently

operated vessel [172]. The industry goal is to create an independently operated vessel with an on-vessel decision support system undertaking all operational decisions. The evolution to autonomy will be phased, and initial implementation is a remotely operated before operating a complete independently operated vessel [172,173]. The adoption of autonomous vessels has a number of challenges at the operational, safety and ultimately regulatory levels, and the solutions need to be validated [172].

7.2. Remotely Operated Vessels

A remotely controlled vessel—similar to its completely unmanned vessel counterpart—comprise a large network of many sensors and is largely driven by algorithms that interpret data acquired to implement accurate navigation across international waterways. The extensive levels of inter-connectivity will, in turn, expose a large number of new attack surfaces in sensor networks, remote controls and communication links between remote on-shore operators and the vessel [173]. The requisite bi-directional links transporting streams of data is a source of concern with regard to data security.

7.3. Autonomously Operated Vessel

While autonomous vessels may not be susceptible to more traditional cyber attacks as a consequence of a human-in-the-control loop, e.g., crew members held hostage, increases in GPS spoofing by exploiting the communication link's attack surface are inevitable [173]. Concerns of an increase in cyber attacks that result in collisions with its attendant loss of life, environmental damages and hazards are related to leveraging numerous new attack surfaces owing the highly interconnected devices such as weak key management, bidirectional point of storage and retrieval of data from the cloud.

7.4. Digitalisation

There are undoubted benefits of migration to ever-increasing levels of digitalisation in the maritime industry, as shown in Figure 11. The business benefits derived from by data-driven applications include the following: transforming largely analogue operations that usually rely on traditional methods into more streamlined practices that optimise cargo handling; and improving maritime procurement and logistics processes mirrors trends in many other sectors. Moreover, it provides the basis for enhanced efficiencies, growth, innovation, safety and competitive advantage whilst minimising the negative impact of the environment [174]. The implementation of digitalisation relies on technologies such as blockchain and Big Data, real-time control, artificial intelligence, autonomous vehicles and robotics, network connectivity, communications, virtual reality and Internet of Things (IoT) [175]. What is essential to accelerating adoption is sharing knowledge and experiences between stakeholders across the industry so as to inculcate new methods of working, optimising customer engagement interfaces and service delivery.

Three phase are envisaged to reach this goal, optimisation, extension and transformation [176], with associated challenges including securing funding and managing concomitant cyber-security overheads. A review and future research directions in using Big Data and artificial intelligence technologies in the maritime industry segmented the path to digitalisation as follows: firstly, maritime transport, port community systems and innovation in maritime transport; secondly, on the applications of Big Data from Automatic Identification System (AIS) as it relates to surveillance, environmental and economic sustainability; thirdly, on optimising energy usage focusing on speed optimisation, route and crane planning; and finally, on predictive analytics as it relates to vessel performance, visual surveillance and other application areas. Lind-Olsen in [177] agreed that Big data and AI offer viable solutions to the digitalisation challenges of the industry, stressing further that the adoption of IoT will continue to provide improved shipping and fleet operations, while that of artificial intelligence will help in optimising decision making and safety. The more widespread application of robotics will facilitate the execution of operations in complex environments and will be integral to the emergence of unmanned vessels.

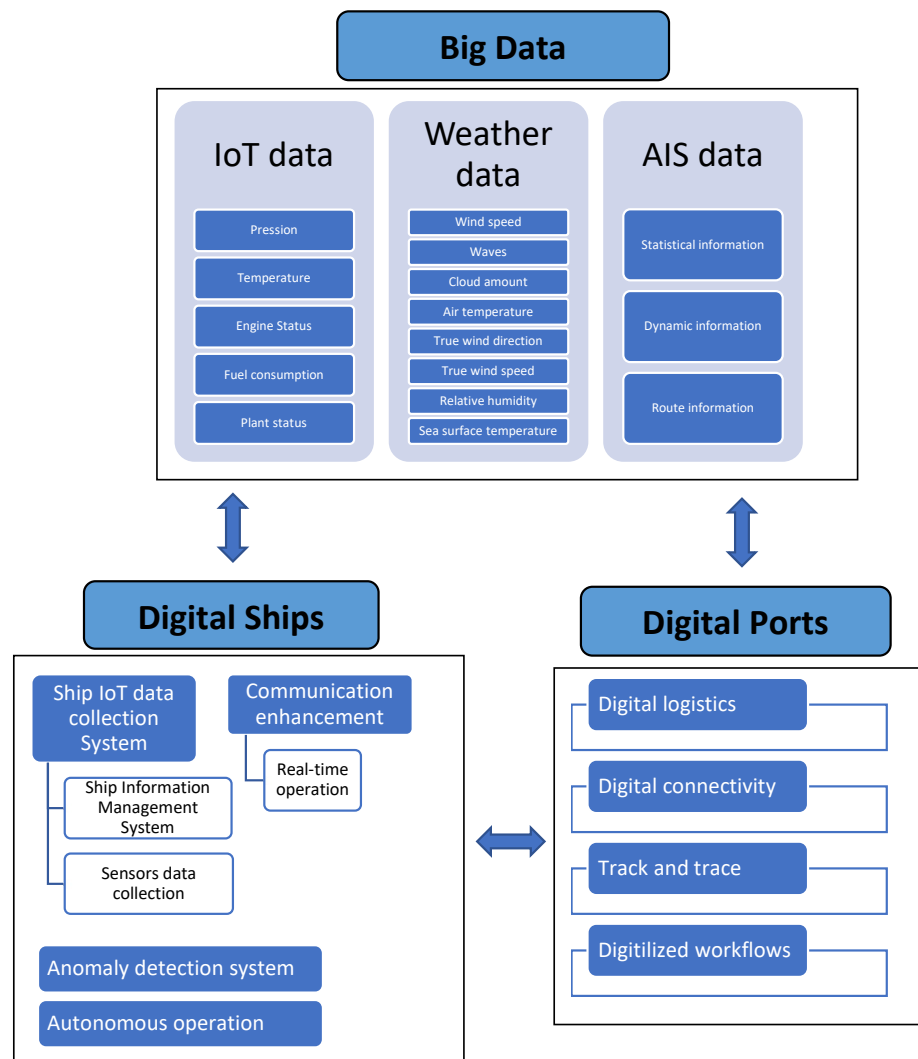


Figure 11. Digitalisation of maritime industry.

8. Conclusions

A review of current components, systems and services within the maritime industry, segmented as in-port and on-vessel, is presented as the foundation for the determination of future exposures of a critical global-wide infrastructure to cyber crimes. Cyber attacks reported to date are classified, and their impact is quantified in each core sub-infrastructure within the context of the state-of-the-art techniques. The sector migration to ever-increasing levels of smart in-port services and autonomous vessels necessitates the establishment of new cyber-security protocols and enhanced protection practices. Clear evidence exists that every port or vessel is at risk of cyber-attacks if key information systems are not adequately protected. The challenge is further exacerbated by the proliferation in the deployment of new technologies with concomitant increases in the scope of vulnerabilities within the most operation-critical infrastructures. As a result, the exposure to a significant risk of unauthorized access and new classes of cyber-attacks is heightened.

An important strand in achieving more robust cyber protection is improvement in cyber-security awareness across the community. In support of awareness, a legal framework and updated insurance methodologies should be established to further strengthen solutions to cyber threats. Moreover, all cyber security issues should be made transparent within stakeholders in order to increase understanding and, in turn, catalyse the development of practices collectively; the details and impact of new cyber-attacks should be communicated for information throughout the supply chain. The integration of acceptable governance

practices in ports, together with the adoption of a universal security protocol, will reduce further the probability of successful cyber attacks and inform effective protection strategies.

In the future, among the many challenges that remain, the development of a plan to the standardization of digital services for autonomous vessels is the most pressing. Furthermore, a new security standard that reduces the number and scope of cyber-attacks for autonomous vessels and smart ports has to be defined for the economic sustainability of the sector.

Author Contributions: Conceptualization and formal analysis, M.A.B.F., E.U., H.H. and X.B.; investigation, M.A.B.F., E.U. and H.H.; methodology, E.U., M.A.B.F., H.H., I.A. and X.B.; validation, M.A.B.F., E.U., D.B., M.B., I.A. and X.B.; writing—original draft preparation, M.A.B.F. and E.U.; and writing—review and editing, M.A.B.F., E.U., H.H., D.B., M.B., I.A. and X.B. All authors have read and agreed to the published version of the manuscript.

Funding: The research is supported by the European Union Horizon 2020 Programme under Grant Agreement No. 833673. The content reflects the authors' view only and the Agency is not responsible for any use that may be made of the information within the paper.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable, the study does not report any data.

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

Abbreviations

The following abbreviations are used in this manuscript:

AIS	Automatic Identification System
S.I	Security Impact
R	Radar
C	Confidentiality
RC	Radio-communication
I	Integrity
PM	Propulsion Management
PCS	Power Control Systems
AS	Access to the system
Al.S	Alarm System
CMS	Cargo Management Systems
B.S	Bridge Systems
PCMS	Passenger Servicing and Management Systems
PPN	Passenger facing public networks
ACWS	Administrative and crew welfare systems
DoS	Denial-of-service attack
GPS	Global Positioning System
A	Availability

References

1. Koukaki, T.; Tei, A. Innovation and maritime transport: A systematic review. *Case Stud. Transp. Policy* **2020**, *8*, 700–710. [[CrossRef](#)]
2. Davri, E.C.; Darra, E.; Monogioudis, I.; Grigoriadis, A.; Iliou, C.; Mengidis, N.; Tsirikas, T.; Vrochidis, S.; Peratikou, A.; Gibson, H.; et al. Cyber Security Certification Programmes. In Proceedings of the 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 26–28 July 2021; pp. 428–435.
3. Bures, M.; Ahmed, B.S.; Rechtberger, V.; Klima, M.; Trnka, M.; Jaros, M.; Bellekens, X.; Almog, D.; Herout, P. PatIoT: IoT Automated Interoperability and Integration Testing Framework. In Proceedings of the 2021 14th IEEE Conference on Software Testing, Verification and Validation (ICST), Porto de Galinhas, Brazil, 12–16 April 2021; pp. 454–459.
4. Mednikarov, B.; Tsonev, Y.; Lazarov, A. Analysis of Cybersecurity Issues in the Maritime Industry. *Inf. Secur.* **2020**, *47*, 27–43. [[CrossRef](#)]
5. Kapalidis, P. Cybersecurity at Sea. In *Global Challenges in Maritime Security*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 127–143.

6. de la Peña Zarzuelo, I. Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue. *Transp. Policy* **2021**, *100*, 1–4. [[CrossRef](#)]
7. Ivošević, S.Š. Envisioning Marketing in a Digital Technology-Driven Maritime Business. *Mednar. Inov. Posl. J. Innov. Bus. Manag.* **2021**, *13*, 22–28.
8. Androjna, A.; Brcko, T.; Pavic, I.; Greidanus, H. Assessing Cyber Challenges of Maritime Navigation. *J. Mar. Sci. Eng.* **2020**, *8*, 776. [[CrossRef](#)]
9. Goudosis, A.; Katsikas, S. Secure AIS with Identity-Based Authentication and Encryption. *TransNav Int. J. Mar. Navig. Saf. Sea Transp.* **2020**, *14*, 287–298. [[CrossRef](#)]
10. Mraković, I.; Vojinović, R. Evaluation of Montenegrin Seafarer’s Awareness of Cyber Security. *Trans. Marit. Sci.* **2020**, *9*, 206–216. [[CrossRef](#)]
11. Tam, K.; Moara-Nkwe, K.; Jones, K. The Use of Cyber Ranges in the Maritime Context. 2020. Available online: <https://pearl.plymouth.ac.uk/handle/10026.1/16067> (accessed on 11 November 2021).
12. Papastergiou, S.; Kalogeraki, E.M.; Polemi, N.; Douligeris, C. Challenges and Issues in Risk Assessment in Modern Maritime Systems. In *Advances in Core Computer Science-Based Technologies*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 129–156.
13. Tranfield, D.; Denyer, D.; Smart, P. Towards a methodology for developing evidence-informed management knowledge by means of systematic review. *Br. J. Manag.* **2003**, *14*, 207–222. [[CrossRef](#)]
14. 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](#)]
15. Bilotta, G.S.; Milner, A.M.; Boyd, I. On the use of systematic reviews to inform environmental policies. *Environ. Sci. Policy* **2014**, *42*, 67–77. [[CrossRef](#)]
16. Zhang, X.; Wang, C.; Jiang, L.; An, L.; Yang, R. Collision-avoidance navigation systems for Maritime Autonomous Surface Ships: A state of the art survey. *Ocean Eng.* **2021**, *235*, 109380. [[CrossRef](#)]
17. Menhat, M.N.; Zaiden, 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**, *209*, 105638. [[CrossRef](#)]
18. Pagano, P.; Antonelli, S.; Tardo, A. C-Ports: A proposal for a comprehensive standardization and implementation plan of digital services offered by the “Port of the Future”. *Comput. Ind.* **2022**, *134*, 103556. [[CrossRef](#)]
19. Alamoush, A.S.; Ballini, F.; Ölçer, A.I. Ports’ technical and operational measures to reduce greenhouse gas emission and improve energy efficiency: A review. *Mar. Pollut. Bull.* **2020**, *160*, 111508. [[CrossRef](#)]
20. Alzahrani, A.; Petri, I.; Rezgui, Y.; Ghoroghi, A. Decarbonisation of seaports: A review and directions for future research. *Energy Strategy Rev.* **2021**, *38*, 100727. [[CrossRef](#)]
21. 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.
22. Ahokas, J.; Kiiski, T.; Malmsten, J.; Ojala, L.M. Cybersecurity in ports: A conceptual approach. In *Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment, Proceedings of the Hamburg International Conference of Logistics (HICL)*; epubli GmbH: Berlin, Germany, 2017; Volume 23, pp. 343–359. Available online: <https://www.econstor.eu/handle/10419/209316> (accessed on 11 November 2021).
23. de la Peña Zarzuelo, I.; Soeane, M.J.F.; Bermúdez, B.L. Industry 4.0 in the port and maritime industry: A literature review. *J. Ind. Inf. Integr.* **2020**, *20*, 100173. [[CrossRef](#)]
24. Cheung, K.F.; Bell, M.G.; Bhattacharjya, J. Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transp. Res. Part E Logist. Transp. Rev.* **2021**, *146*, 102217. [[CrossRef](#)]
25. Larsen, M.H.; Lund, M.S. A Maritime Perspective on Cyber Risk Perception: A Systematic Literature Review. *IEEE Access* **2021**. [[CrossRef](#)]
26. Kessler, G.C. The CAN Bus in the Maritime Environment—Technical Overview and Cybersecurity Vulnerabilities. *Transnav Int. J. Mar. Navig. Saf. Sea Transp.* **2021**, *15*, 531–540. [[CrossRef](#)]
27. Kuhn, K.; Bicakci, S.; Shaikh, S.A. COVID-19 digitization in maritime: Understanding cyber risks. *WMU J. Marit. Aff.* **2021**, *20*, 193–214. [[CrossRef](#)]
28. Munim, Z.H.; Dushenko, M.; Jimenez, V.J.; Shakil, M.H.; Imset, M. Big data and artificial intelligence in the maritime industry: A bibliometric review and future research directions. *Marit. Policy Manag.* **2020**, *47*, 577–597. [[CrossRef](#)]
29. Ghaderi, H. Autonomous technologies in short sea shipping: Trends, feasibility and implications. *Transp. Rev.* **2019**, *39*, 152–173. [[CrossRef](#)]
30. Argles, C. A conceptual review of cyber-operations for the royal navy. *Cyber Def. Rev.* **2018**, *3*, 43–56.
31. Aslam, S.; Michaelides, M.P.; Herodotou, H. Internet of ships: A survey on architectures, emerging applications, and challenges. *IEEE Internet Things J.* **2020**, *7*, 9714–9727. [[CrossRef](#)]
32. Qiao, D.; Liu, G.; Lv, T.; Li, W.; Zhang, J. Marine Vision-Based Situational Awareness Using Discriminative Deep Learning: A Survey. *J. Mar. Sci. Eng.* **2021**, *9*, 397. [[CrossRef](#)]
33. Sullivan, B.P.; Desai, S.; Sole, J.; Rossi, M.; Ramundo, L.; Terzi, S. Maritime 4.0—Opportunities in digitalization and advanced manufacturing for vessel development. *Procedia Manuf.* **2020**, *42*, 246–253. [[CrossRef](#)]

34. Kavallieratos, G.; Katsikas, S.; Gkioulos, V. Cybersecurity and safety co-engineering of cyberphysical systems—A comprehensive survey. *Future Internet* **2020**, *12*, 65. [CrossRef]
35. Kapalidis, C. Cyber Security Challenges for the Maritime Industry. 2019. Available online: <https://safety4sea.com/cm-cyber-security-challenges-for-the-maritime-industry/> (accessed on 11 November 2021).
36. HMM Hit by Cyber Attack. Available online: <https://www.offshore-energy.biz/hmm-hit-by-cyber-attack/> (accessed on 11 November 2021).
37. Cyber Attack Targets Iranian Port near Strait of Hormuz. Available online: <https://www.jpost.com/breaking-news/cyber-attack-targets-iranian-port-near-strait-of-hormuz-627616> (accessed on 13 September 2021).
38. MSC Confirms Malware Attack Caused Website Outage. Available online: <https://www.seatrade-maritime.com/containers/msc-confirms-malware-attack-caused-website-outage> (accessed on 13 September 2021).
39. 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=6597dc5c41aa> (accessed on 13 September 2021).
40. Marine Firm James Fisher Reports Cyber Breach. Available online: <https://www.reuters.com/article/us-james-fisher-cybercrime-idUSKBN1XF1SQ> (accessed on 13 September 2021).
41. China Hackers Steal Data from US Navy Contractor—Reports. Available online: <https://www.bbc.co.uk/news/world-us-canada-44421785> (accessed on 13 September 2021).
42. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Available online: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> (accessed on 13 September 2021).
43. Ships Fooled in GPS Spoofing Attack Suggest Russian Cyberweapon. Available online: <https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/> (accessed on 13 September 2021).
44. 7 Sailors Missing, CO Injured after Destroyer USS Fitzgerald Collided with Philippine Merchant Ship. Available online: <https://news.usni.org/2017/06/16/destroyer-uss-fitzgerald-collides-japanese-merchant-ship> (accessed on 13 September 2021).
45. 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 13 September 2021).
46. 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 13 September 2021).
47. University of Texas Team Takes Control of a Yacht by Spoofing Its GPS. Available online: <https://newatlas.com/gps-spoofing-yacht-control/28644/> (accessed on 13 September 2021).
48. Virus Origin in Gulf Computer Attacks in Question. Available online: <https://phys.org/news/2012-09-virus-gulf.html> (accessed on 13 September 2021).
49. The ‘Icefog’ APT: A Tale of Cloak and Three Daggers. Available online: <https://media.kaspersky.com/en/icefog-apt-threat.pdf> (accessed on 11 November 2021).
50. Iran’s Top Cargo Shipping Line Says Sanctions Damage Mounting. Available online: <https://www.reuters.com/article/us-iran-sanctions-shipping-idUSBRE89L10X20121022> (accessed on 11 November 2021).
51. Police Warning after Drug Traffickers’ Cyber-Attack. Available online: <https://www.bbc.co.uk/news/world-europe-24539417> (accessed on 11 November 2021).
52. Wang, C.; Kim, Y.S.; Kim, C.Y. Causality between logistics infrastructure and economic development in China. *Transp. Policy* **2021**, *100*, 49–58. [CrossRef]
53. Muñoz-Villamizar, A.; Velázquez-Martínez, J.C.; Haro, P.; Ferrer, A.; Mariño, R. The environmental impact of fast shipping ecommerce in inbound logistics operations: A case study in Mexico. *J. Clean. Prod.* **2021**, *283*, 125400. [CrossRef]
54. Bocayuva, M. Cybersecurity in the European Union port sector in light of the digital transformation and the COVID-19 pandemic. *WMU J. Marit. Aff.* **2021**, *20*, 173–192. [CrossRef]
55. Senarak, C. Port cybersecurity and threat: A structural model for prevention and policy development. *Asian J. Shipp. Logist.* **2021**, *37*, 20–36. [CrossRef]
56. Tam, K.; Jones, K. MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU J. Marit. Aff.* **2019**, *18*, 129–163. [CrossRef]
57. Pitropakis, N.; Logothetis, M.; Andrienko, G.; Stefanatos, J.; Karapistoli, E.; Lambrinouidakis, C. Towards the Creation of a Threat Intelligence Framework for Maritime Infrastructures. In *Computer Security*; Springer: Cham, Switzerland, 2019; pp. 53–68.
58. Gamboa, Y.B.G.; Ramírez-Cabrales, F.; Jiménez, J.A.M. Cyber Security Vulnerabilities in Colombia’s Maritime Critical Infrastructure (MCI). *Dev. Adv. Def. Secur.* **2020**, *3*, 3–15.
59. Karamperidis, S.; Kapalidis, C.; Watson, T. Maritime Cyber Security: A Global Challenge Tackled through Distinct Regional Approaches. *J. Mar. Sci. Eng.* **2021**, *9*, 1323. [CrossRef]
60. Hindy, H.; Tachtatzis, C.; Atkinson, R.; Brosset, D.; Bures, M.; Andonovic, I.; Michie, C.; Bellekens, X. Leveraging Siamese Networks for One-Shot Intrusion Detection Model. *arXiv* **2020**, arXiv:2006.15343.
61. Office of Chief of Naval Operations Security Regulations Manual. Available online: [https://www.secnav.navy.mil/doni/SECNAV%20Manuals1/5510.1%20\(OPNAV\).PDF](https://www.secnav.navy.mil/doni/SECNAV%20Manuals1/5510.1%20(OPNAV).PDF) (accessed on 4 June 2021).

62. 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](#)]
63. *SP 800-30 Rev 1; Guide for Conducting Risk Assessments*; National Institute of Standards & Technology: Gaithersburg, MD, USA, 2012.
64. 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](#)]
65. Seebruck, R. A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digit. Investig.* **2015**, *14*, 36–45. [[CrossRef](#)]
66. Rogers, M.K. A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digit. Investig.* **2006**, *3*, 97–102. [[CrossRef](#)]
67. Snyder, P.; Vault, A. Playing hackers at their own game. *Netw. Secur.* **2016**, *2016*, 14–16. [[CrossRef](#)]
68. Peng, R.; Xiao, H.; Guo, J.; Lin, C. Optimal defense of a distributed data storage system against hackers' attacks. *Reliab. Eng. Syst. Saf.* **2020**, *197*, 106790. [[CrossRef](#)]
69. Trump, D. *National Cyber Strategy of the United States of America*; The White House: Washington, DC, USA, 2018.
70. Im, N.K.; Nguyen, V.S. Artificial neural network controller for automatic ship berthing using head-up coordinate system. *Int. J. Nav. Archit. Ocean Eng.* **2018**, *10*, 235–249. [[CrossRef](#)]
71. Palma, D. Enabling the maritime Internet of Things: CoAP and 6LoWPAN performance over VHF links. *IEEE Internet Things J.* **2018**, *5*, 5205–5212. [[CrossRef](#)]
72. Ozturk, U.; Birbil, S.I.; Cicek, K. Evaluating navigational risk of port approach manoeuvrings with expert assessments and machine learning. *Ocean Eng.* **2019**, *192*, 106558. [[CrossRef](#)]
73. Vicen-Bueno, R.; Carrasco-Álvarez, R.; Rosa-Zurera, M.; Nieto-Borge, J.C.; Jarabo-Amores, M.P. Artificial neural network-based clutter reduction systems for ship size estimation in maritime radars. *EURASIP J. Adv. Signal Process.* **2010**, *2010*, 380473. [[CrossRef](#)]
74. Khellal, A.; Ma, H.; Fei, Q. Convolutional neural network based on extreme learning machine for maritime ships recognition in infrared images. *Sensors* **2018**, *18*, 1490. [[CrossRef](#)]
75. Vozikis, D.; Darra, E.; Kuusk, T.; Kavallieros, D.; Reintam, A.; Bellekens, X. On the Importance of Cyber-Security Training for Multi-Vector Energy Distribution System Operators. In Proceedings of the 15th International Conference on Availability, Reliability and Security, Virtual, 25–28 August 2020; Association for Computing Machinery: New York, NY, USA, 2020. [[CrossRef](#)]
76. Lallie, H.S.; Shepherd, L.A.; Nurse, J.R.; Erola, A.; Epiphaniou, G.; Maple, C.; Bellekens, X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Comput. Secur.* **2021**, *105*, 102248. [[CrossRef](#)]
77. Report: Maritime Cyberattacks Up by 400 Percent. Available online: <https://maritime-executive.com/article/report-maritime-cyberattacks-up-by-400-percent> (accessed on 12 December 2020).
78. John, A.; Nwaoha, T. Safety critical maritime infrastructure systems resilience: A critical review. *Int. J. Marit. Eng.* **2016**, *158*, 209–218. [[CrossRef](#)]
79. Olba, X.B.; Daamen, W.; Vellinga, T.; Hoogendoorn, S.P. State-of-the-art of port simulation models for risk and capacity assessment based on the vessel navigational behaviour through the nautical infrastructure. *J. Traffic Transp. Eng.* **2018**, *5*, 335–347.
80. Yang, R.; Jiang, L. Technology Research and Experimental Simulation of Energy Management System for Diesel Electric Hybrid Ship. In Proceedings of the 2020 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China, 12–14 June 2020; pp. 671–675.
81. Perabo, F.; Zadeh, M.K. Modelling of a Shipboard Electric Power System for Hardware-in-the-Loop Testing. In Proceedings of the 2020 IEEE Transportation Electrification Conference & Expo (ITEC), Chicago, IL, USA, 23–26 June 2020; pp. 69–74.
82. Markopoulos, E.; Luimula, M.; Porrano, P.; Pisirici, T.; Kirjonen, A. Virtual Reality (VR) safety education for ship engine training on maintenance and safety (ShipSEVR). In Proceedings of the International Conference on Applied Human Factors and Ergonomics, San Diego, CA, USA, 16 July 2020; pp. 60–72.
83. Alanen, J.; Isotalo, M.; Kuittinen, N.; Simonen, P.; Martikainen, S.; Kuuluvainen, H.; Honkanen, M.; Lehtoranta, K.; Nyssönen, S.; Vesala, H.; et al. Physical Characteristics of Particle Emissions from a Medium Speed Ship Engine Fueled with Natural Gas and Low-Sulfur Liquid Fuels. *Environ. Sci. Technol.* **2020**, *54*, 5376–5384. [[CrossRef](#)]
84. Billard, D. Investigation of an alleged PLC hacking on sea vessels. *J. Phys. Conf. Ser.* **2019**, *1297*, 012035. [[CrossRef](#)]
85. Sawada, R.; Hirata, K.; Kitagawa, Y.; Saito, E.; Ueno, M.; Tanizawa, K.; Fukuto, J. Path following algorithm application to automatic berthing control. *J. Mar. Sci. Technol.* **2021**, *26*, 541–554. [[CrossRef](#)]
86. Zhao, J.; Zhang, Y.; Yang, Z.; Liu, Y.; Peng, S.; Hong, N.; Hu, J.; Wang, T.; Mao, H. A comprehensive study of particulate and gaseous emissions characterization from an ocean-going cargo vessel under different operating conditions. *Atmos. Environ.* **2020**, *223*, 117286. [[CrossRef](#)]
87. Felski, A.; Jaskólski, K.; Zwolak, K.; Piskur, P. Analysis of Satellite Compass Error's Spectrum. *Sensors* **2020**, *20*, 4067. [[CrossRef](#)] [[PubMed](#)]
88. Niklaus, M.; Zhan, K.; Wagner, J.F. Gyrolog—Creating a 3-Dimensional Digital Collection of Classical Gyro Instruments. In Proceedings of the 2019 DGON Inertial Sensors and Systems (ISS), Braunschweig, Germany, 10–11 September 2019; pp. 1–23.
89. Zheng, Y.; Zhao, F.; Wang, Z. Fault diagnosis system of bridge crane equipment based on fault tree and Bayesian network. *Int. J. Adv. Manuf. Technol.* **2019**, *105*, 3605–3618. [[CrossRef](#)]

90. Jo, J.H.; Kim, S. Key Performance Indicator Development for Ship-to-Shore Crane Performance Assessment in Container Terminal Operations. *J. Mar. Sci. Eng.* **2020**, *8*, 6. [[CrossRef](#)]
91. Čampara, L.; Hasanspahić, N.; Vujičić, S. Overview of MARPOL ANNEX VI regulations for prevention of air pollution from marine diesel engines. *SHS Web Conf.* **2018**, *58*, 01004. [[CrossRef](#)]
92. Bogens, K. GMDSS modernisation and e-navigation: Spectrum needs. In Proceedings of the ETSI Workshop Future Evaluation of Marine Communication, Sophia Antipolis, France, 7–8 November 2017; pp. 1–23.
93. Kopacz, Z.; Morgas, W.; Urbanski, J. The maritime safety system, its main components and elements. *J. Navig.* **2001**, *54*, 199. [[CrossRef](#)]
94. Kochanski, R.J.; Paige, J.L. Safenet: The standard and its application. *IEEE LCS* **1991**, *2*, 46–51. [[CrossRef](#)]
95. Grant, A.; Williams, P.; Shaw, G.; De Voy, M.; Ward, N. Understanding GNSS availability and how it impacts maritime safety. In Proceedings of the Institute of Navigation International Technical Meeting, San Diego, CA, USA, 24–26 January 2011; pp. 687–695.
96. Zhang, C.; Guo, C.; Zhang, D. Ship navigation via GPS/IMU/LOG integration using adaptive fission particle filter. *Ocean Eng.* **2018**, *156*, 435–445. [[CrossRef](#)]
97. DeSanto, J.B.; Chadwell, C.D.; Sandwell, D.T. Kinematic post-processing of ship navigation data using precise point positioning. *J. Navig.* **2019**, *72*, 795–804. [[CrossRef](#)]
98. Suárez-Alemán, A. Short sea shipping in today's Europe: A critical review of maritime transport policy. *Marit. Econ. Logist.* **2016**, *18*, 331–351. [[CrossRef](#)]
99. Yu, L.; Xing, Z. A GPS/GLONASS/INS data fusion algorithm. *Sci. Surv. Mapp.* **2017**, *5*. Available online: https://en.cnki.com.cn/Article_en/CJFDTotal-CHKD201709005.htm (accessed on 11 November 2021).
100. Schuster, M.; Blaich, M.; Reuter, J. Collision avoidance for vessels using a low-cost radar sensor. *IFAC Proc. Vol.* **2014**, *47*, 9673–9678. [[CrossRef](#)]
101. Wilthil, E.F.; Flåten, A.L.; Brekke, E.F.; Breivik, M.; Breivik, M. Radar-based maritime collision avoidance using dynamic window. In Proceedings of the 2018 IEEE Aerospace Conference, Big Sky, MT, USA, 3–10 March 2018; pp. 1–9.
102. Updating Your ECDIS Using Email. 2017. Available online: https://www.youtube.com/watch?v=Tam_lu-ySTA (accessed on 11 November 2021).
103. How to: Update Your ECDIS and Planning Station Permits and Data in 'Working Folio' via an Automatic AVCS/ARCS Weekly Update Email. 2017. Available online: https://www.admiralty.co.uk/AdmiraltyDownloadMedia/eNav%20Docs/20150205_WorkingFolio_V01.pdf (accessed on 11 November 2021).
104. Talley, W.K.; Ng, M. Note: Determinants of cargo port, hinterland cargo transport and port hinterland cargo transport service chain choices by service providers. *Transp. Res. Part E Logist. Transp. Rev.* **2020**, *137*, 101921. [[CrossRef](#)]
105. Johnson, D. System and Method for Tracking Ships and Ship Cargo. U.S. Patent US20100121770A1, 13 May 2010.
106. Yang, H. General Technology of Cargo Ship. In *Manned Spacecraft Technologies*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 57–98.
107. Perez, H.M.; Chang, R.; Billings, R.; Kosub, T.L. Automatic identification systems (AIS) data use in marine vessel emission estimation. In Proceedings of the 18th Annual International Emission Inventory Conference, Baltimore, MD, USA, 14–17 April 2009; Volume 14, p. e17.
108. 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](#)]
109. Carson-Jackson, J. Satellite AIS—Developing technology or existing capability? *J. Navig.* **2012**, *65*, 303–321. [[CrossRef](#)]
110. Simonic, R.; Weaver, A.C.; Cain, B.G.; Colvin, M.A. Shipnet: A real-time local area network for ships. In Proceedings of the 13th Conference on Local Computer Networks, Minneapolis, MN, USA, 10–12 October 1988; pp. 424–432.
111. Sun, S.; Lu, Z.; Liu, W.; Hu, W.; Li, R. Shipnet for semantic segmentation on vhr maritime imagery. In Proceedings of the IGARSS 2018 IEEE International Geoscience and Remote Sensing Symposium, Valencia, Spain, 22–27 July 2018; pp. 6911–6914.
112. Green, D.T.; Marlow, D.T. SAFENET—A LAN for Navy mission critical systems. In Proceedings of the 14th Conference on Local Computer Networks, Mineapolis, MN, USA, 10–12 October 1989; pp. 340–346.
113. Paige, J.L. SAFENET—A navy approach to computer networking. In Proceedings of the 15th Conference on Local Computer Networks, Minneapolis, MN, USA, 30 September–3 October 1990; pp. 268–273.
114. Thomsett, D. The evolution of successful C3I systems. *J. Nav. Eng.* **1993**, *34*, 299–307.
115. Carley, K.M.; Ren, Y.; Krackhardt, D. Measuring and modeling change in C3I architecture. In Proceedings of the 2000 Command and Control Research and Technology Symposium, Monterey, CA, USA, 26–28 June 2000; pp. 26–28.
116. Lister, J.; Rosie, J. A digital maritime integrated internal communication system. *J. Nav. Eng.* **1995**, *35*, 504–519.
117. Källberg, B.; Strähle, R. Ship system 2000, a stable architecture under continuous evolution. In Proceedings of the International Conference on Reliable Software Technologies, Leuven, Belgium, 14–18 May 2001; pp. 371–379.
118. Young, S.; Gubbins, V. Smart ship and reduced manning in the United States Navy. *J. Nav. Eng.* **1997**, *37*, 226–239.
119. Zhu, W.; Fan, Y.; Ban, S. Designing Security Architecture of Total Ship Computing Environment Based on Mimic Defense. *J. Digit. Technol. Appl.* **2018**. Available online: https://en.cnki.com.cn/Article_en/CJFDTotal-SZJT201801111.htm (accessed on 11 November 2021).

120. Ukwandu, E.; Farah, M.A.B.; Hindy, H.; Bures, M.; Atkinson, R.; Tachtatzis, C.; Bellekens, X. Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *arXiv* **2021**, arXiv:2107.04910.
121. Carlan, V.; Sys, C.; Vanelslender, T. How port community systems can contribute to port competitiveness: Developing a cost-benefit framework. *Res. Transp. Bus. Manag.* **2016**, *19*, 51–64. [[CrossRef](#)]
122. Long, A. Port community systems. *World Cust. J.* **2009**, *3*, 63–67.
123. Aydogdu, Y.V.; Aksoy, S. A study on quantitative benefits of port community systems. *Marit. Policy Manag.* **2015**, *42*, 1–10. [[CrossRef](#)]
124. Tijan, E.; Agatić, A.; Jović, M.; Aksentijević, S. Maritime National Single Window—A Prerequisite for Sustainable Seaport Business. *Sustainability* **2019**, *11*, 4570. [[CrossRef](#)]
125. Simão, J.C.D.; da Anunciação, P.F. Port Single Window and Logistics Single Window: Two Competitiveness Proposals in the Port Value Chain. In *Handbook of Research on Information Management for Effective Logistics and Supply Chains*; IGI Global: Hershey, PA, USA, 2017; pp. 316–333.
126. Henesey, L.; Wernstedt, F.; Davidsson, P. Market-driven control in container terminal management. In Proceedings of the 2nd International Conference on Computer Applications and Information Technology in the Maritime Industries, Hamburg, Germany, 14–17 May 2003; pp. 377–386. Available online: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.15.2593&rep=rep1&type=pdf> (accessed on 11 November 2021).
127. Dragović, B.; Tzannatos, E.; Park, N.K. Simulation modelling in ports and container terminals: Literature overview and analysis by research field, application area and tool. *Flex. Serv. Manuf. J.* **2017**, *29*, 4–34. [[CrossRef](#)]
128. 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.
129. Iphar, C.; Napoli, A.; Ray, C. Detection of false AIS messages for the improvement of maritime situational awareness. In Proceedings of the Oceans 2015-MTS/IEEE Washington, Washington, DC, USA, 19–22 October 2015; pp. 1–7.
130. Coleman, J.; Kandah, F.; Huber, B. Behavioral Model Anomaly Detection in Automatic Identification Systems (AIS). In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; pp. 481–487.
131. Dembovskis, A. AIS Message Extraction from Overlapped AIS Signals for SAT-AIS Applications. Ph.D. Thesis, Universität Bremen, Bremen, Germany, 2015.
132. Hu, Q.; Jiang, Y.; Zhang, J.; Sun, X.; Zhang, S. Development of an automatic identification system autonomous positioning system. *Sensors* **2015**, *15*, 28574–28591. [[CrossRef](#)]
133. Prévost, R.; Coulon, M.; Bonacci, D.; LeMaitre, J.; Millerioux, J.P.; Tourneret, J.Y. Cyclic redundancy check-based detection algorithms for automatic identification system signals received by satellite. *Int. J. Satell. Commun. Netw.* **2013**, *31*, 157–176. [[CrossRef](#)]
134. Oligeri, G.; Sciancalepore, S.; Di Pietro, R. GNSS Spoofing Detection via Opportunistic IRIDIUM Signals. *arXiv* **2020**, arXiv:2006.10284.
135. Qiao, Y.; Zhang, Y.; Du, X. A vision-based GPS-spoofing detection method for small UAVs. In Proceedings of the 2017 13th International Conference on Computational Intelligence and Security (CIS), Hong Kong, China, 15–18 December 2017; pp. 312–316.
136. Dobryakova, L.A.; Lemieszewski, Ł.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](#)]
137. Bhatti, J.; Humphreys, T.E. Hostile control of ships via false GPS signals: Demonstration and detection. *NAVIGATION J. Inst. Navig.* **2017**, *64*, 51–66. [[CrossRef](#)]
138. Abramowski, T.; Bilewski, M.; Dobryakova, L.; Ochin, E.; Uriasz, J.; Zalewski, P. Detection of Spoofing Used against the GNSS-Like Underwater Navigation Systems. *Preprints* **2020**. [[CrossRef](#)]
139. Magiera, J.; Katulski, R. Detection and mitigation of GPS spoofing based on antenna array processing. *J. Appl. Res. Technol.* **2015**, *13*, 45–57. [[CrossRef](#)]
140. Clark, J. Cybercrime in the Shipping Industry. A Present. Hill Dickinson LLP. 2018. Available online: https://globalmaritimehub.com/wp-content/uploads/attach_908.Pdf (accessed on 11 November 2021).
141. Mraković, I.; Vojinović, R. Maritime Cyber Security Analysis—How to Reduce Threats? *Trans. Marit. Sci.* **2019**, *8*, 132–139. [[CrossRef](#)]
142. Vishwanath, A. Spear phishing: The tip of the spear used by cyber terrorists. In *Combating Violent Extremism and Radicalization in the Digital Era*; IGI Global: Hershey, PA, USA, 2016; pp. 469–484.
143. Kolev, K.; Dimitrov, N. Cyber threats in maritime industry-situational awareness and educational aspect. In Proceedings of the Global Perspectives in MET: Towards Sustainable, Green and Integrated Maritime Transport, Varna, Bulgaria, 11–13 October 2017; pp. 352–360. Available online: <https://www.semanticscholar.org/paper/CYBeR-tHReAt-In-MARItIeMe-InDUStRY-%E2%80%93StUAtIOnAL-AnD-Kolev-Dimitrov/6e92639d617f3aa54fdcdc260b2ac521ef9076c9> (accessed on 11 November 2021).
144. Kessler, G.C. Cybersecurity in the Maritime Domain. *USCG Proc. Mar. Saf. Secur. Counc.* **2019**, *76*, 34.
145. Bou-Harb, E.; Kaisar, E.I.; Austin, M. On the impact of empirical attack models targeting marine transportation. In Proceedings of the 2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), Naples, Italy, 26–28 June 2017; pp. 200–205.

146. Hindy, H.; Tachtatzis, C.; Atkinson, R.; Bayne, E.; Bellekens, X. Developing a Siamese network for intrusion detection systems. In Proceedings of the 1st Workshop on Machine Learning and Systems, Online, 26 April 2021; pp. 120–126.
147. Lam, J.S.L.; Bai, X. A quality function deployment approach to improve maritime supply chain resilience. *Transp. Res. Part E Logist. Transp. Rev.* **2016**, *92*, 16–27. [[CrossRef](#)]
148. Perez, G.F. Cyber Situational Awareness and Cyber Curiosity Taxonomy for Understanding Susceptibility of Social Engineering Attacks in the Maritime Industry. Ph.D. Thesis, Nova Southeastern University, Fort Lauderdale, FL, USA, 2019.
149. Jensen, L. Challenges in maritime cyber-resilience. *Technol. Innov. Manag. Rev.* **2015**, *5*, 35. [[CrossRef](#)]
150. Meyer-Larsen, N.; Müller, R. Enhancing the Cybersecurity of Port Community Systems. In Proceedings of the International Conference on Dynamics in Logistics, Bremen, Germany, 20–22 February 2018; pp. 318–323.
151. 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](#)]
152. König, S.; Rass, S.; Schauer, S. Cyber-attack impact estimation for a port. Digital Transformation in Maritime and City Logistics: Smart Solutions for Logistics. In Proceedings of the Hamburg International Conference of Logistics (HICL), Hamburg, Germany, 25–27 September 2019; Volume 28, pp. 164–183.
153. Schauer, S.; Kalogeraki, E.M.; Papastergiou, S.; Douligieris, C. Detecting Sophisticated Attacks in Maritime Environments using Hybrid Situational Awareness. In Proceedings of the 2019 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), Paris, France, 18–20 December 2019; pp. 1–7.
154. Guesmi, R.; Farah, M.B. A new efficient medical image cipher based on hybrid chaotic map and DNA code. *Multimed. Tools Appl.* **2021**, *80*, 1925–1944. [[CrossRef](#)]
155. Lagouvardou, S. *Maritime Cyber Security: Concepts, Problems and Models*; Kongens Lyngby: Copenhagen, Denmark, 2018.
156. Liu, G.; Sistemas, S.I.; Sistemas, S.I.; Sistemas, S.I. Internet of ships: The future ahead. *World J. Eng. Technol.* **2016**, *4*, 220. [[CrossRef](#)]
157. Kedari, S.; Vuppapapati, J.S.; Ilapakurti, A.; Vuppapapati, C.; Kedari, S.; Vuppapapati, R. Precision Dairy Edge, Albeit Analytics Driven: A Framework to Incorporate Prognostics and Auto Correction Capabilities for Dairy IoT Sensors. In Proceedings of the Future of Information and Communication Conference, Singapore, 5–6 April 2018; pp. 506–521.
158. Kamolov, A.; Park, S. An IoT-Based Ship Berthing Method Using a Set of Ultrasonic Sensors. *Sensors* **2019**, *19*, 5181. [[CrossRef](#)]
159. Sahay, R.; Meng, W.; Estay, D.S.; Jensen, C.D.; Barfod, M.B. CyberShip-IoT: A dynamic and adaptive SDN-based security policy enforcement framework for ships. *Future Gener. Comput. Syst.* **2019**, *100*, 736–750. [[CrossRef](#)]
160. Mileski, J.; Clott, C.; Galvao, C.B. Cyberattacks on ships: A wicked problem approach. *Marit. Bus. Rev.* **2018**, *3*, 414–430. [[CrossRef](#)]
161. Wang, H.; Osen, O.L.; Li, G.; Li, W.; Dai, H.N.; Zeng, W. Big data and industrial internet of things for the maritime industry in northwestern norway. In Proceedings of the TENCON 2015—2015 IEEE Region 10 Conference, Macao, China, 1–4 November 2015; pp. 1–5.
162. Al-Gumaei, K.; Schuba, K.; Friesen, A.; Heymann, S.; Pieper, C.; Pethig, F.; Schriegel, S. A survey of internet of things and big data integrated solutions for industrie 4.0. In Proceedings of the 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), Turin, Italy, 4–7 September 2018; Volume 1, pp. 1417–1424.
163. Kim, K.I.; Jeong, J.S.; Park, G.K. Assessment of external force acting on ship using big data in maritime traffic. *J. Korean Inst. Intell. Syst.* **2013**, *23*, 379–384.
164. Aydin, N.; Choi, Y.; Lekhavat, S.; Irani, Z.; Lee, H. A decision support system for vessel speed decision in maritimes logistics using weather archive big data. *Comput. Oper. Res.* **2018**, *98*, 330–342.
165. Brouer, B.D.; Karsten, C.V.; Pisinger, D. Big data optimization in maritime logistics. In *Big data Optimization: Recent Developments and Challenges*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 319–344.
166. Nita, S.; Mihailescu, M. Importance of Big Data in Maritime Transport. *Sci. Bull. Mircea Cel Batran Nav. Acad.* **2017**, *20*, 556.
167. Mirović, M.; Miličević, M.; Obradović, I. Big data in the maritime industry. *NAŠE MORE Znan. Časopis Za More I Pomor.* **2018**, *65*, 56–62.
168. Dineva, K.; Atanasova, T. Security in IoT Systems. In Proceedings of the 19th International Multidisciplinary Scientific GeoConference SGEM 2019, Albena, Bulgaria, 28 June–7 July 2019; Volume 19, pp. 576–577.
169. Stellios, I.; Kotzanikolaou, P.; Psarakis, M.; Alcaraz, C.; Lopez, J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 3453–3495. [[CrossRef](#)]
170. Jović, M.; Tijan, E.; Aksentijević, S.; Čišić, D. An Overview of Security Challenges Of Seaport IoT Systems. In Proceedings of the 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 20–24 May 2019; pp. 1349–1354.
171. Formby, D.; Durbha, S.; Beyah, R. Out of control: Ransomware for industrial control systems. In Proceedings of the RSA Conference, San Francisco, CA, USA, 14–17 February 2017.
172. Liu, D. Autonomous Vessel Technology, Safety, and Ocean Impacts. In *The Future of Ocean Governance and Capacity Development*; Brill Nijhoff: Leiden, The Netherlands, 2019; pp. 490–494.
173. Gu, Y.; Goez, J.C.; Guajardo, M.; Wallace, S.W. Autonomous vessels: State of the art and potential opportunities in logistics. *Int. Trans. Oper. Res.* **2021**, *28*, 1706–1739. [[CrossRef](#)]

174. Babica, V.; Sceulovs, D.; Rustenova, E. Digitalization in Maritime Industry: Prospects and Pitfalls. In *Workshop on ICTE in Transportation and Logistics*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 20–27.
175. Fernández Otero, R.M.; Bayliss-Brown, G.; Papathanassiou, M. Ocean literacy and knowledge transfer synergies in support of a sustainable Blue Economy. *Front. Mar. Sci.* **2019**, *6*, 646. [[CrossRef](#)]
176. Hoffmann, J.; Sirimanne, S. *Review of Maritime Transport*; United Nations Conference on Trade and Development: Geneva, Switzerland, 2017. Available online: https://unctad.org/system/files/official-document/rmt2017_en.pdf (accessed on 11 November 2021).
177. Lind-Olsen, M. *4 Digital Trends In The Maritime Industry*; Dialog: Tromso, Norway, 2019.