2022-10-13

A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships

Kapalidis, C

10.3390/jmse10101486
Journal of Marine Science and Engineering
MDPI

Journal of *Marine Science and Engineering*

MDPI

Article

A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships

Chronis Kapalidis [1,*], Stavros Karamperidis [2], Tim Watson [3] and Georgios Koligiannis [4]

[1] Cyber Security Centre, WMG, University of Warwick, Coventry CV4 7AL, UK
[2] Plymouth Business School, University of Plymouth, Plymouth PL4 8AA, UK
[3] Allan Turing Institute, London NW1 2DB, UK
[4] Hellenic Navy, 15561 Cholargos, Greece
* Correspondence: chronis.kapalidis.1@warwick.ac.uk

Abstract: The maritime sector is a vital component of the global economy. Its international nature supersedes state boundaries and any disruption in its operations could have consequent and collateral global effects, affecting the socio-economic wellbeing of regions, states and peoples. The increasing adoption of digitalisation in the sector, primarily increases efficiency, minimize cost and maximise benefit, while improving safety, simultaneously introduces a new cyber threat landscape. The attack surface has broadened further due to the COVID-19 pandemic, as recent, high-profile cyber attacks to shipping companies have indicated. Cybersecurity is not limited to technology but involves people and business processes. Hence, to mitigate the security risk introduced by cyber threat actors, the industry, like any other, should initially focus on identifying its most critical assets and then adopt risk mitigation measures, spreading from legislative initiatives to company-specific technology solutions. Industry-led initiatives should promote the adoption of cyber-related policies and mechanisms that focus on business continuity. It should be the role of international bodies, classification societies and national authorities to ensure compliance and full implementation of these measures. This paper adopts a System of Systems Analysis to carry out a vulnerability assessment of port and ship ecosystem, while providing insights on the role of the aforementioned entities. Our analysis decomposes the industry's major assets; ports and ships, to specific subcomponents which are used as the basis of the vulnerability assessment. According to our findings, this approach highlights that the majority of these subcomponents; ports and ships, are increasingly vulnerable to cyber attacks.

Keywords: maritime sector; maritime security; cybersecurity; ports; ships

Citation: Kapalidis, C.; Karamperidis, S.; Watson, T.; Koligiannis, G. A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships. *J. Mar. Sci. Eng.* **2022**, *10*, 1486. https://doi.org/10.3390/jmse10101486

Academic Editors: Mihalis Golias, Jin Wang and Dong-Sheng Jeng

Received: 28 June 2022
Accepted: 11 October 2022
Published: 13 October 2022

1. Introduction

Over the last decade, cybersecurity attracted a significant attention in the maritime domain. Reports for cyberattacks on ports and ships have increased substantially from 2017 to 2022 [1,2]. The impact of cyber-related incidents on the maritime economy is emerging dramatically, especially during the COVID-19 pandemic, as illustrated in Appendix A, where office staff are, in their majority working from home, and ship crew demand increased connectivity to keep in touch with people ashore. Maritime transport and all related activities, holistically defined as the Maritime Transportation System (MTS), are conducted by technology-intensive platforms, which today rely heavily on information systems [3].

This evolution of the maritime sector, based on innovation and digitalization, is helping the sector flourish. With the introduction of digital services apart from the reduction of burdens and the administration costs, time required to load and locate cargo, control the performance of critical onboard systems, and manage ship traffic has significantly reduced [4]. As a result, this has introduced a widened set of access points to maritime Industrial Control Systems (ICS). Considering that cyber attacks are becoming ever more

sophisticated and commonplace [5], there is growing pressure from governments, regulatory bodies and international institutions for immediate action in prioritizing cybersecurity in the maritime sector.

The maritime domain consists of multiple and diverse components both on the infrastructure level and the services provided. Specifically, the MTS infrastructure consists of two key components: ports and ships. This argument does not intent to limit the components of a MTS but only to highlight the two predominant ones. According to the EU NIS Directive States can determine which essential service providers are to be considered as part of their CNI cybersecurity landscape. In January 2019, the Danish Maritime Authority released Order 46 which argues that service providers like VTS or AIS providers are essential services. Therefore, MTS infrastructure consists of ships, ports and other essential services. Any disruption to these systems can cause major disruption not only to the directly affected business, but even to the global supply chain. Due to increased maritime cyber threats policy should be targeted not only at the specific threat but to each component too, and provide a holistic security posture.

In June 2017 A.P. Moller Maersk's terminal in Ukraine was affected by the notPetya ransomware, in one of the most notable maritime-related cyber incident presented in Appendix A [6]. According to Gronholt-Pedersen [7] all business units at Maersk were affected including those in Rotterdam, Los Angeles, Mumbai and Auckland. Operations were forced either to completely shut down or temporarily slow down, resulting in a loss of revenue for the shipping giant initially estimated around $300 m [8–10]. Among other lessons learned from this incident, what is also highlighted is the importance of testing the adopted cybersecurity policies and measures in order to identify vulnerabilities and back doors to corporate systems, since the specific malware code was a known vulnerability that could have been spotted if an efficient assessment was conducted [9]. As the chairman of the company stated, A.P. Moller Maersk was also forced to change all its affected IT equipment and applications and restructure its global network, cyber policy and procedures to prevent and minimise the effect of any potential future attack [11].

This paper looks at the unique nature of cyber threats to the MTS by presenting the findings of new research conducted by the authors. These findings were based on a combination of desk-based research and stakeholder engagement. Specifically, semi-structured interviews and a roundtable discussion were conducted with subject matter experts, academics and practitioners (representatives from the public and private sectors along with international experts). Through a System-of-Systems Analysis (SOSA) the paper provides an overview of the cyber vulnerabilities that exist in ports and ships, the potential consequences of cyber attacks against them and the consequent affected fields. To illustrate the extent of such consequences on a socio-economic level, the paper uses the Persian Gulf and the Strait of Hormuz, one of the world's most important maritime chokepoint as a case study. Within that scope, the aim of the paper is to raise awareness on the importance of cybersecurity for the maritime sector, identify gaps in existing policies and consider how these should be addressed, while looking briefly at potential solutions. Section 2 demonstrates the current issues and highlights contemporary research directions of cybersecurity in the maritime sector. Section 3 demonstrates the methodology adopted for data collection and analysis. Section 4 demonstrates a thorough analysis of the vulnerability of the most critical assets in MTS. Section 5 demonstrates the findings of a case study of an MTS related cyber incident at the Persian Gulf through a socio-economic lens. Finally, Section 6 demonstrates the conclusion and recommendations.

Having reviewed the existing literature for the topic, the academic contribution of the paper focuses on providing initially a research-based identification of port and ship subcomponents through the lens of technology, and secondly a qualitative vulnerability assessment of cyber risks. Our paper provides useful insights to academics, researchers, students but also to industry practitioners.

2. Overview of the Current Landscape

The security of the maritime sector has been in the focus of the IMO for several years. In the aftermath of the 9/11 terrorist attacks in New York the organisation assembled expert groups to work on securing the sector from similar threats. This led to the introduction of the International Ship and Port Facility Security (ISPS) Code, which is an amendment to the Safety of Life at Sea (SOLAS) Convention (1974/1988) on minimum security arrangements for ships, ports and government agencies. Similarly, for cybersecurity, the IMO published the Interim Guidelines on Maritime Cyber Risk Management in 2016 and the consequent MSC-FAL.1/Circ.3 in 2017 (Guidelines on Maritime Cyber Risk Management) [12]. This document suggests that as of 1 January 2021 all organisations in the shipping industry must demonstrate cyber capability. Judging from the IMO's reactive approach to security, like the publication of the ISP code indicates, the fact that the IMO has already published an official documentation for cybersecurity indicates the importance of protecting the MTS against cyber threats.

Hence, risks related to cybersecurity are one of the main threats that the MTS faces with disruptive consequences that could lead even to loss of life, as elaborated later in the paper. Apart from the direct effects of a cyber attack on the system itself, the potential consequences of such an attack to areas intertwined with the industry, namely the economic and social sphere, should not be neglected. In order to examine the broader picture, we should look at: (1) The impact to the economy of an attack on a major port, (2) The consequences to people's everyday life, (3) The disruption to shipping routes if a ship is mishandled due to GPS spoofing and is run aground or causes a collision at a chokepoint.

In an effort to minimize the likelihood of these disruptive incidents occurring, we should, initially, identify the vulnerabilities of the systems used in the sector. Second, we should analyze the consequences of a cyber breach to these systems and third, the fields that may be affected by such an incident, since, as it will be highlighted throughout this paper the cyber-physical nature of these systems should not be neglected. To achieve the aforementioned, we have adopted SOSA. Such methodology brings together isolated systems to form a new more complex system, which offers more functionality and performance than the sum of its parts [13]. For the purposes of this paper, the port and ship ecosystems are regarded as system of systems and thus analyzed through a SOSA lens. Nowadays, as the adoption of digital technologies and services in the maritime domain is increasing, cybersecurity is becoming rather relevant in most maritime related activities. Ships, shipping companies' offices, port facilities, and any other company or organization, directly or indirectly, related to the shipping industry are increasingly incorporating digitalization into their daily operations. Computers and cyber-enabled technologies are being increasingly used for navigation, communications, cargo and ballast management, engineering, emergency systems, safety and security, environmental control, and many other purposes [14–16]. Digitization acts as an enabler to further improve the impressive record of efficiency and reliability for the MTS [17]. Building on the existent safety and security culture developed in the sector over the years, everyday operations, conducted manually in the past, are beginning to be facilitated using digital systems.

Great benefits come at great risk. The maritime sector could be described as a high value target for those engaged in unlawful acts, like smuggling, drug and human trafficking, piracy, terrorism and any other malicious activities due to large amounts of revenue involved in daily operations and the unpreparedness of the sector with regards its cyber protection [9,18]. The results of a cyber attack, depending on the threat actors' motivators, may vary from data loss or manipulation to disruption of trade activity, physical damage, environmental disaster or even injury or loss of life.

The predominant concern in the MTS is safety at sea. Maritime traffic control centres depend heavily on ICT equipment, such as navigation aid systems (GPS, GALILLEO, GLONASS, and AIS), safety communication systems (GMDSS, ship-to-ship and ship-to-shore, UHF/VHF/HF), satellite and GSM communications, in order to remain connected

and monitor ships, while coordinating with port authorities, national shipping authorities, pilot agencies and other maritime organisations.

As an example, the Automatic Identification System (AIS), an automatic tracking system that uses transponders on ships to facilitate the safety of navigation at sea is vulnerable to jamming and spoofing attacks affecting the confidentiality and integrity of the system. Consequently, if a ship's navigation is tampered, it could lead to the ship running aground or cause collision and, in the worst-case scenario, an extended oil spill or even a gas explosion. The potential of a similar attack in offshore drilling units can have devastating effects [19]. Similarly, as it is analysed in the next section, ports, usually constituting part of a state's Critical National Infrastructure have several systems and services prone to cyber attacks.

3. Methodology

3.1. Justification of the Research Approach

It would be reasonable to approach this research in a rigorous way by constructing a simulation or theoretical environment, and then exploring how it might be attacked by developing a proof-of-concept attack, based on MITRE's ATT&CK framework [20] together with estimates of the likely resources and capabilities of attackers. However, this would highlight particular risks, but would be in danger of missing the more important aspects of the emergent risk in real, very large-scale systems of systems. As a consequence, the most appropriate approach to this research is based on a qualitative analysis of the component systems, and how they combine in modern port and maritime facilities. Identifying the key security controls, and how they are changing in the latest port and maritime systems of systems, provides insights into the areas of focus that ought to be highlighted to enable effective cybersecurity.

This approach, combined with sense-checking analysis by industry subject matter experts, balances appropriate academic rigour. It also provides a focus on the right scale of system of systems, to guard against an oversimplified test environment not capturing some of the most important aspects of cyber risk.

3.2. Data Collection and Analysis

Our research followed a qualitative approach. Research had three stages: (1) Desk-based research, (2) Stakeholder engagement, (3) Findings validation.

For the 1st stage (desk-based research) we conducted a semi systematic literature review, to identify main research on maritime cybersecurity. The literature review was conducted using an exploratory design and a thorough qualitative analysis of primary and secondary literature. Preliminary research identified a total of 295 documents using the following search terms:

"maritime cybersecurity"; "maritime cybersecurity"; "maritime" AND "cybersecurity"; "maritime" AND "cybersecurity"; "maritime" AND (cyber* or security*); "marine cybersecurity"; "marine cybersecurity"; "port cybersecurity"; "port cybersecurity".

These documents were then filtered using the following inclusion/exclusion criteria:

- The documentation should be in English
- The documents should be academic journal papers, reports, white papers, non-journal conference papers, books and international or national publications. No opinion articles, news agencies articles, blogs or any other online resource was assessed
- The document should be cyber-specific

2nd stage (Stakeholder engagement): Primary data was collected during the stakeholder engagement. Fifteen semi-structured interviews were conducted with a variety of stakeholders including: (1) shipowners and port operators, (2) Chief Information Security Officers (CISO), (3) Information security and technology providers, (4) Marine insurers, (5) Brokers, (6) Academics and (7) Policy makers. Saturation was achieved thus we stopped our data collection at 15 interviews. The interview questionnaire is presented in Appendix B. The years of experience of all interviewees is presented in Figure 1. Data collected was anal-

ysed to identify key challenges and it was then presented during three targeted workshops (3rd stage). Please see Figure 2 below, where a schematic representation of the three stages is demonstrated.

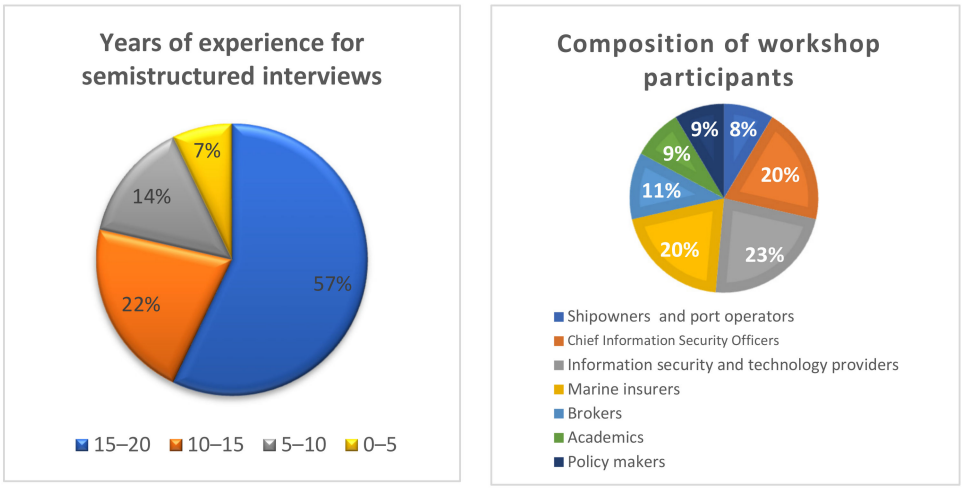

Figure 1. Participants' data. Source: Authors.

Figure 2. Research design. Source: Authors.

These three industry focused workshops were designed as validation activities of primary research findings. All the participants were senior representatives of the broader maritime sector as illustrated in Figure 1, with more than 15 years of experience. The total number of participants was 35. Both workshops were conducted under the Chatham House Rule facilitating participants in sharing sensitive information and real-life case studies. The outcomes of these workshops informed the findings presented in this paper.

A visual illustration of the research findings is demonstrated at Figures 3 and 4, in Sections 4.1 and 4.2 below, providing a detailed overview of vulnerabilities and consequences of a cyber incident to the industry's most valuable assets; the port and the ship.

3.3. Limitations of the Methodology

The authors applied a qualitative approach, focusing on understanding the vital cyber challenges in the MTS. Consequently, all the primary data collected could not be quantified and analysed through statistical procedures as in quantitative research. Compared to the quantitative methods, a significant constraint was encouraging more experts to participate in our research project, and thus we did not use a large sample that could numerically be considered a representative population. Mixed method research could further triangulate the findings and minimise the drawbacks of a traditional approach; however, the paper's purpose is not to present numerical parameters. Another limitation of the research is that the systematic literature review (i.e., 1st stage (desk-based research)) focused on scientific articles and reports published only in English.

4. The Vulnerabilities of the Most Critical Assets in the MTS: An Analysis

This part of the paper analyses the two main components of the MTS as identified initially and tries to examine how vulnerable these are to potential malicious cyber related activities. The paper will try to untangle the complexity of the sub-components of ports

and ships, highlight the consequences of a cyber-related disruption to these components, while categorising the affected fields from such an incident. Consequent findings are the result of research conducted by the authors, consisting of desk-based research and qualitative, semi-structured interviews with industry practitioners, government officials, and academics, and were informed by the discussions instigated during a workshop with industry experts.

4.1. Port's Cyber Ecosystem

A port, as a cyber ecosystem, is a complex set of land and waterside systems and procedures, where the human factor still retains a predominant role. Over the last few years this ecosystem has rapidly become more digitalized, allowing the sector to thrive [21]. Naturally, this increased digitalization is expanding the attack landscape for cyber criminals and other threat actors, but also increases the likelihood of unintentional human error by, unfamiliar to the new technologies and cyber-hygiene practices and standards, company rotating crew staff. According to Allianz Global Corporate & Specialty [22], more than 75% of the marine casualties and accidents are attributable to human errors. The adoption of software-enabled systems and services offer a wide range of access points from where malicious software may infiltrate one or more of the port's systems. A breach to any of these systems or services may cause a wide range of disruptions to the port environment, varying from tampering with timely, efficient, and safe port operations, jeopardising health and safety of port and third-party staff, causing financial losses, environmental pollution and damaging an entity's reputation to facilitating smuggling or trafficking [23,24].

The cyber ecosystem or "cyber environment", as defined in the UK Department for Transport (DfT) Code of Practice, comprises the interconnected networks of both information and cyber-physical systems that use electronic, computer-based, and wireless systems, including information, services and social and business functions that exist only in cyberspace [14]. Applying this definition to ports, four main components can be identified: buildings, linear infrastructure, plant and machinery, and information and communication systems [14]. These four main components consist of 18 sub-components as illustrated in Table 1.

Table 1. Port ecosystem components.

Buildings (IT Based Systems)	Linear Infrastructure	Plant, Machinery and Operational Facilities (OT Based and SCADA Systems)	Information and Communication Systems
Port Facility offices	Roads	Cargo handling vehicles, cranes and conveyer assets	Financial Management and Monitoring
Port Facility accommodation	Access control points	Refineries	Container and vehicle movement systems
Warehouse and storage (chemical, gas, bulk and dry cargo) facilities	Rail systems	Power plants	Asset management systems (cargo, vehicle)
Vessel Traffic Control Tower	Utilities	Terminal Facilities (Container Terminal, Oil tank terminal)	Access control management system
Maintenance areas	Cargo handling systems such as pipelines and conveyer systems		

Source: Authors.

These four main components are interconnected with a wide range of operational and administrative processes, run by port staff and external third-party providers. In the event of a cyber incident occurring to one or more of these components, the consequences can be categorized in four distinct fields: data, human element, physical and environmental. The vulnerabilities, consequences, and affected fields within the port environment are

illustrated in Figure 3. Specifically, each of the sub-components is coloured based on the level of vulnerability (green: low, amber: medium, red: high). Consequently, a triangle colour based on the severity of the consequences is placed on its subcomponents (green: low, amber: medium, red: high). Finally, a circle consisting of the initial of each affected field (D: Data, E: Environment, H: Human, P: Physical) is placed on each sub-component.

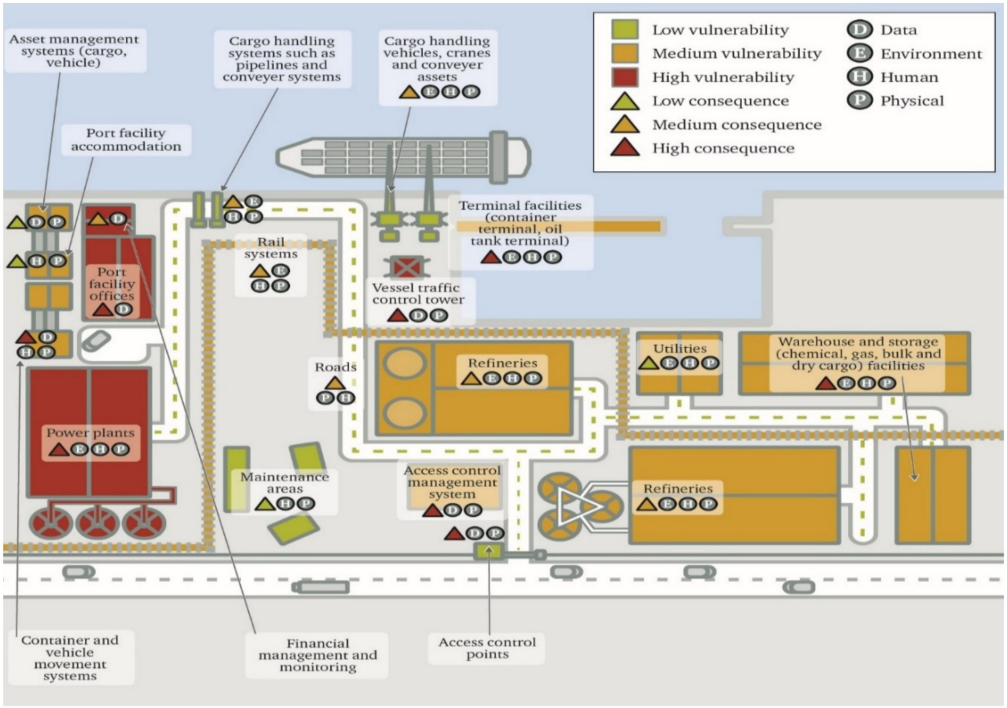

Figure 3. Port Components (Vulnerabilities, Consequences and Affected Fields). Note: This graphical illustration was generated with the support of Chatham House. Source: Authors.

Looking at the four port components initially, the buildings, linear infrastructure, plant and machinery and information and communication systems, as the diagram illustrates, **plant and machinery** used for cargo handling and port management, is the most vulnerable of the four aforementioned components, since it relies heavily on Operational Technology (OT) and, predominantly, Supervisory Control and Data Acquisition (SCADA) systems. These systems are the bulk systems of every port and regardless of the level of vulnerability, the consequences of a cyber attack on most of them are classified as severe, having an impact on more or less all of the aforementioned fields (data, environment, human, physical). Having said that, the most vulnerable sub-systems are the power plants, which are usually continuously connected to the regional main power controlling stations, forming, in this way, a part of the entire Critical National Infrastructure (CNI).

The second most vulnerable component is **the information and communication systems**, which are, a priori, related to data manipulation. Even though all the subcomponents are based on software, most of them are only connected to the internal port IT or OT network. An exception is the financial management and monitoring services used in order to conduct all financial activities of the port-based companies and port authority, which are constantly connected to the internet. Even though limited access to these services and systems may not halt port operations, it will certainly lead to financial instability, which in its turn could lead to other related disruptions, such as reputational damage and third-party compensation. Such an escalation could result in major disruptions of the port's business cycle.

Thirdly, the Vessel Traffic Control Tower (VTCT) is the most vulnerable sub-component of the **Building** category. The VTCT's operations rely on ship-to-shore, ship-to-ship communications, all of which use non-encrypted channels of the electromagnetic spectrum,

and vessel management software. Port offices are also vulnerable to cyber-attacks as the entire breadth of port operations is monitored and, in some cases, managed by this facility. The consequences of a cyber attack to these two subcomponents are ranked as severe since such an incident would result in major disruption to port operations, from a seaside and shore side perspective. Port gates in one of Maersk's terminals at a major port in Europe, where all office-based systems were not usable due to the NotPetya malware, were shut as a result, causing lengthy delays and queues of trucks waiting to pick up containers.

Finally, the **linear infrastructure**, consisting of road and rail networks, access control points, utilities, and cargo handling systems, is, as easily understood, the least vulnerable of the four, due to its physical nature and the limited cyber elements incorporated in this. Having said that, even though the physical component of rail systems and utilities are not vulnerable, the monitoring, control and alarm systems encapsulated in them can, potentially, be affected by a cyber incident that could affect their normal operations, from a safety perspective. Such an incident would, consequently, affect the overall port operations.

4.2. Ship's Cyber Ecosystem

The ship, as a cyber environment, is what sets the challenges of the maritime sector apart from other industries. While the other components of the MTS are frequently similar to components present in other industries, the ship is the sector's most valuable asset and one which is, most of the time, operating independently at sea. While a port may operate similarly to other CNI assets, a ship, currently, when at sea does not rely on internet connectivity in order to conduct its main operations, i.e., navigation, engine control and cargo monitoring. There are although several subcomponents, critical to the ship's operations, that have moved from analogue to digital mode of operation. For that reason and due to the importance of the ship as a key asset of the MTS, the same SOSA is adopted.

Unlike the port, where four key components were identified, in the ship environment the various systems used to maintain reliable and consistent ship operability can be categorised in two main components: deck and engine. These two main components consist of 20 sub-components as illustrated in Table 2.

Table 2. Ship ecosystem components.

Deck		**Engine**	
Signal light column	Anchor and mooring winch control system	Engine Control Room System	Switchboards
Internal communications	TV-Entertainment-Internet Access Systems	Bow Thruster Control System	Water Ingress Detection System
GMDSS Console	Fleet Management system	Alarm Monitoring and Control System	Power Management
Navigation Equipment	Bridge control console	Cabling	
VDR/S-DR	Electrical Crane Equipment		
Reefer Container Monitoring System	Navigation Lights		
Loading and Stability Computer			

Source: Authors.

Based on research findings and as illustrated in Figure 4, there are several subcomponents which present low vulnerability to cyber attacks, a few of the deck's subcomponents are extremely vulnerable. The deck comprises of both IT and OT systems, which are in most cases interconnected. According to the research findings, the most vulnerable subcomponent of the entire ship are the **crew entertainment facilities**, including internet access. Even though it is gradually becoming common practice for most shipping companies to introduce network segregation to their IT infrastructure, separating the business from the crew network, it could be argued that this is not adequate to protect the ship's operations. Although the two networks may be segregated, they both still use the sole IT infrastructure

available on the ship. It only takes a careless seafarer to plug a malware-affected flash drive into the engine control system, to affect the engine management software, which in several cases still runs on a more vulnerable Windows XP environment [25].

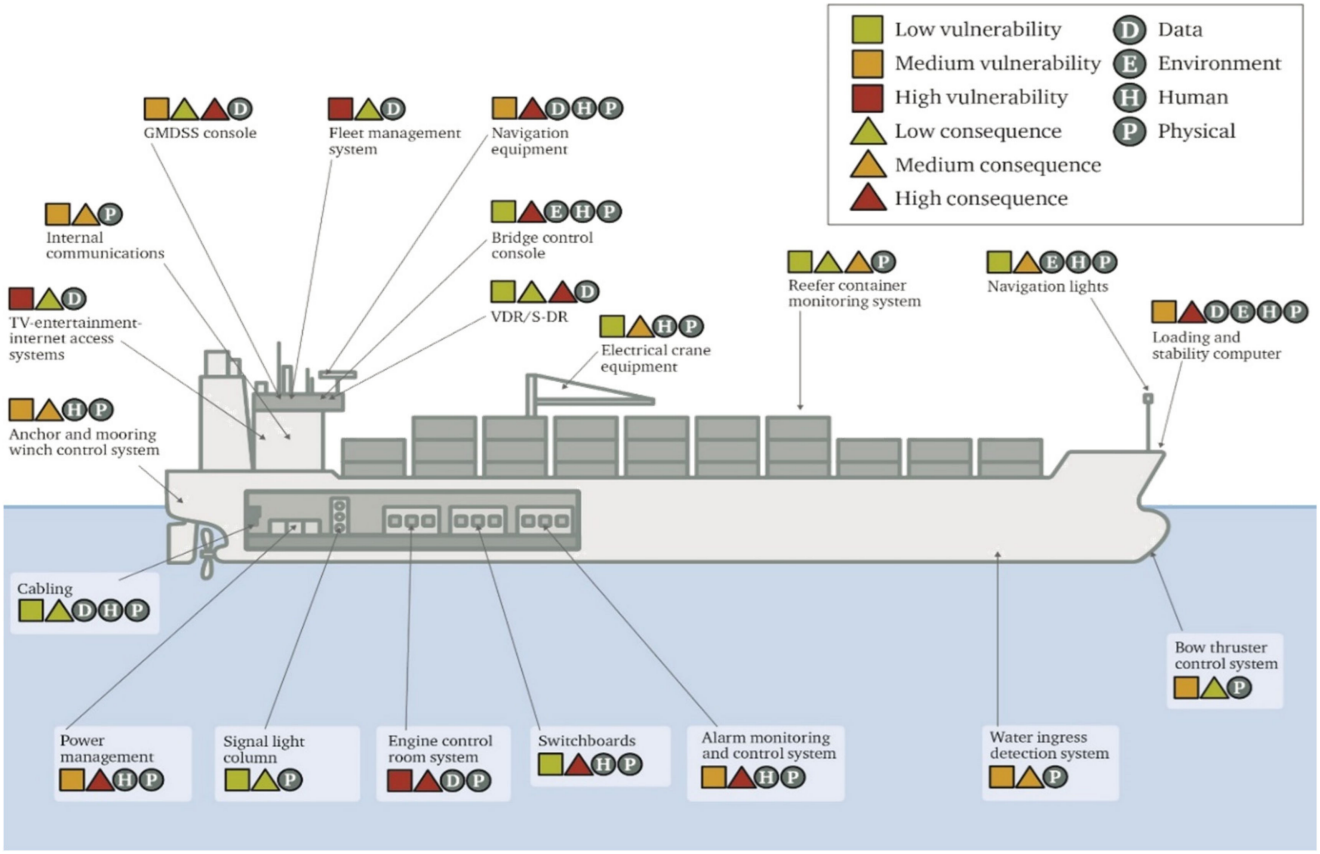

Figure 4. Ship Components (Vulnerabilities, Consequences and Affected Fields)**.** Note: When two triangles exist, they are introduced to indicate the difference in consequences based on the nature of the cyber incident. Source: Authors.

Additionally, the main subcomponent of the ship's deck is the **Bridge Control Console**, where most of the other subcomponents are connected to facilitate the ship's steering, navigation, cargo handling and most of its routine operational activities. Since modern ships operate with no more than three persons on duty at the bridge, it is important for the duty officer to have centralised control and monitoring of the ship's main operations via such a console. This integrated console includes systems that require internet connectivity, such as the Fleet Management System, and others that require frequent updates, such as the Electronic Chart Display and Information System (ECDIS), constituting it as one of the most important and, at the same time, most vulnerable components in a ship's bridge. If one of these components is exposed to malware, the ship's safety can be jeopardised.

The second component, the engine, is primary composed of OT and SCADA systems that provide the ship with electrical power, propulsion, and safety monitoring. Even though most of these subcomponents operate independently, they could still be described as cyber-physical systems, since they are remotely controlled by the **Engine Control Room System** (ECRS) over computer-based software. Following the same centralised principle of operation, the ECRS, is the heart of the entire engine component, making it vital for the ship's undisturbed continuity of operations. In that context, although on most ships, the ECRS is not connected to the internet, lately, at an increasing rate, vendors are requesting access to their shipboard installed systems, to monitor efficiency, performance, and consistency, which in turn, offers a potential back door to any malicious actors in accessing the ship's cyber environment.

These findings illustrate the need for a holistic risk management approach, since the cyber threat landscape is growing in unprecedented rate and, as practice has indicated, no system can ever be 'cyber proof'. This cyber risk management practice should focus on three main areas; (a) advising; (b) threat intelligence support; and (c) training. Cybersecurity is not limited to technology but involves people and business processes. Hackers will take advantage of the power of repetition that every individual is accustomed to and make their way into the enterprise ecosystem. Thus, comprehensive cyber risk management should be practised constantly within the maritime sector.

5. The Socio-Economic Consequences of a Cyber Incident at the MTS: A Case Study of the Persian Gulf

Maritime transportation is carrying more than 80% of the international trade with absolute numbers increasing year on year [26]. Maritime transport plays a key role in the socioeconomic development and wellbeing of most states, including the states around the Persian Gulf. As approximately 30% of the global oil trade and 30.2 million TEU, to and from these states is carried through MTS [27]. Cooperation between the Arab Peninsula's states in protecting and maintaining a sustainable MTS will contribute to people's wellbeing and prosperity.

A unique characteristic of the region is that its trade activities depend heavily on the availability of the Strait of Hormuz. When looking at the geographical distribution of ports in the Persian Gulf, as identified in Figure 5, the importance of the Strait of Hormuz is immediately noticed, since the bulk of the region's seaborne trade is transported through its waters. The Strait has been at the heart of regional tensions for decades. Political instability in the past raised fears around the matter. In 2018, the possibility of closing the Strait from Iran re-emerged in public discourse [28]. It is worth noting that, in the events that occurred in May, June and July 2019, there was a cyber element in them, as ships transiting the Strait experienced GPS interference, bridge-to-bridge communications spoofing, and/or other communications jamming [29].

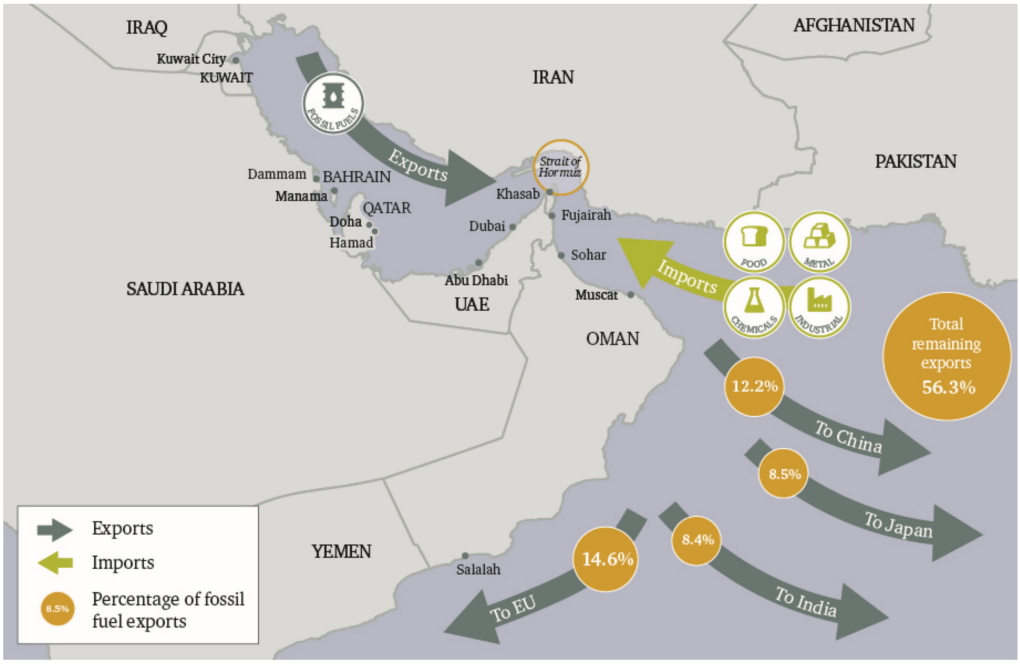

Figure 5. Major Gulf Cooperation Council Ports and the Strait of Hormuz Trade Flows. Source: Authors.

Ports act as an enabler for the region's economic growth, as they are the main gateway for trading industrial and agricultural products, fossil fuels and related by-products, along with facilitating transportation and delivery of services. The Persian Gulf is strategically considered as the starting point of one of the world's most important shipping lanes [30,31]

for the transportation of oil and containerised goods. Investment by local and multinational companies in port development in the region [32], with the notable example of the Hamad Port in Qatar [33], also contribute to creating jobs and business opportunities. Shipping is the primary means of transportation for the main export product of the region; fossil fuel. Very Large Crude Carriers (VLCC) or Liquefied Natural Gas (LNG) and Liquefied Petroleum Gas (LPG) carriers are used to carry oil, gas, and related by-products globally, as the area has the biggest oil reserves, constituting of 47.6% of global share [34].

An attack or any disruption to a port's daily operations or a ship's scheduled trip could result in side effects including loss of revenue, environmental disaster, or even loss of life. From an economic perspective, the late delivery of a ship's cargo consequently can lead to lost revenue across the supply chain, including penalties that must be paid by the shipbroker or the contracting company to its final consumers. The Maersk cyber incident analysed in Section 2 and the closure of Suez Canal by Ever Given on the 23 March 2021 [35] demonstrate some of these consequences.

Apart from the economic impact of such an incident, in the social sphere, a disruption to the MTS affects a wide range of people's livelihoods. Varying from necessary food supplies to spare parts needed for urgent repairs, medical supplies to support medical emergencies, fuel, minerals lubricants and other oil by-products needed to run heavy industry, the consequences of a belated delivery can be easily understood. Even though fossil fuels are the primary export product for the GCC, metals, minerals and primarily agricultural products are mainly imported to support business development and social wellbeing. A disruption to the MTS delivering these products would have serious consequences.

6. Lessons to Be Learned from International Responses, Key Takeaways and Future Steps

This last part of the paper builds on the findings presented in the previous sections and tries to pinpoint lessons learned from use cases on how similar efforts to address cybersecurity concerns have been implemented. It also looks at the key research takeaways, while briefly presenting the most recent, worth noting, initiatives on the matter.

6.1. Legislative Frameworks: The EU Network and Information Security Directive (NISD)

Currently, there is a broad range of frameworks, national legislations, guidelines, best practices, and recommendations regarding cybersecurity, globally. Much of the material is written from an information systems security perspective and needs to be carefully interpreted when applying it to systems and processes used in MTSs around the world. One of the most applicable examples is the NISD adopted by the EU in 2016. This first piece of EU-wide cybersecurity legislation aims to enhance cybersecurity among EU members. One of the Directive's three parts focuses on state supervision of critical sectors, one of which is transport.

Prior to its departure from the EU, the UK was one of the first states to implement NISD. For the maritime transport, namely, ports, the government has assigned Associated British Ports (ABP) as one of the Operators of Essential Services. What was made apparent throughout the research activities was that compliance to NISD and similar mandatory legislation is a stepped approach. In order to meet the objectives of the Directive, ABP has adopted a risk-based approach. In that context, aiming to achieve compliance and cyber resilience, each port operator needs to ensure adequate cyber risk management is practised constantly. This process is monitored by the Cyber Assessment Framework (CAF) [36]. Similar approaches have been adopted by other EU states in the implementation of the Directive [37].

What is worth noting is that, even though the NISD is a good start to improve the cyber risk landscape, it leads to an uneven implementation from each EU state. That is because the various stakeholders are introducing their own requirements, such as state-related security measures, NISD trade bloc size set of requirements, and the IMO set of requirements, creating a very complex policy and security landscape. Overcoming this complexity is a major challenge for regulators and maritime operators.

6.2. The Role of Top Management

What is important to understand is that, as the Maersk cyber case study highlighted, in the event of a cyber incident, probably, the only asset that a company will have at the initial stages of incident response and recovery is people [38]. During the research team's stakeholder engagements there was a consensus on the role of top management on promoting cybersecurity awareness and best practices within each organisation. This can be achieved in several ways. Initially, senior managers should use appropriate language tailored to the responsibilities and background of their staff, to simplify terms and concepts and make it easy for everyone within the organisation to understand what is at stake. Leading by example is certainly the way forward in this case. Managers should follow all existing procedures and best practices in their everyday activities to set acceptable behaviour standards regarding cybersecurity. It should be mentioned that within the maritime sector specifically, the IMO has been promoting the role of top management in achieving promoting cultural changes, in other instances in the past [39].

On the other hand, for such an approach to be effective, senior management should understand what the risk to their organisation is. According to Shaikh [40] "a lot of people {senior managers} generally believe it (cyber threats} is hyped up". A noteworthy initiative is the research project on 'cyber readiness of boards' funded by NCSC and Lloyd's Register Foundation [41]. That project explored the factors shaping UK board (including maritime) decisions around cyber risk and developed interventions to provide guidance and support, bringing together experts from academia and industry.

6.3. The Role of Insurance

The role of insurance in enhancing resilience has been predominant in the maritime sector for decades. Insurance products and strategies are encouraging maritime companies to focus on risk reduction through provision of risk information and premium discounts for risk mitigation. Cyber insurance though, is limited, as there is insufficient data available that will assist insurers in establishing the cost of cyber attacks to set up insurance policies [42]. One way of filling this 'knowledge gap' to better inform insurance premiums, is to carry out a cyber risk assessment to identify the organisation's cyber exposure. Additionally, maritime stakeholders are reluctant in purchasing cyber insurance, since, as highlighted by several interviewees for this project, they do not believe the cyber domain is an area where their business can be interrupted.

Recent examples, presented in Appendix A, indicate that companies should start considering their own cyber insurance strategy. This is facilitated by the fact that Lloyd's of London has introduced cyber risk codes for product development [43]. These are CY- Data and Privacy Breach and CZ—Property Damage. Hence, insurance providers should focus on knowledge and information sharing, so maritime companies can prioritise and inform their decisions as to whether cyber insurance is appropriate for their organisation.

6.4. The Way Forward

Interconnectivity between ports, ships, external providers, and all relevant stakeholders engaged in the maritime industry is increasing. As such, we can arguably assess that the vulnerabilities to cyber breaches of ports' and ships' subcomponents, presented in Figures 2 and 3 will only increase. In shipping specifically, the provision of internet access has reached unprecedented heights, as new technologies become available [44]. Moreover, innovative digital technologies, such as autonomous operations of vessel docking [45], blockchain, automation and robotics [46], are adopted globally to facilitate port operations and maximise productivity. While these developments offer great benefits to the industry, they also introduce new risks, as malicious actors can exploit this increased connectivity to cause harm.

Industry-led initiatives should have cyber resilience policies and mechanisms in place that support business continuity. It should be the role of international bodies, classification societies and national authorities to ensure compliance and full implementation of these

measures. Within that scope, initiatives such as the launch of the US National Maritime Cybersecurity Plan to the National Strategy for Maritime Security, in December 2020 [47], should be embraced by the industry.

7. Conclusions

Ports and ships are the hubs of the supply chain and global trade between maritime and land-based transport routes. Considering that most of the global trade is carried by sea, a major disruption of a strategic port or of a maritime chokepoint can have devastating effects. Through the adoption of digitalisation most of the components within ports and ships, as illustrated in Figures 3 and 4, have an IT or OT system in their core operations. Hitherto air gapped, these systems are increasingly utilising the port's or ship's IT infrastructure to operate and monitor activities. The dissemination and analysis of data collected from these components shape command decisions that integrate a physical outcome as well. The intertwinement of these cyber-physical systems adds further complexity in any proposed or implemented cybersecurity policy.

This work has shed light in both the port and ship ecosystems, the two most critical components of the MTS. Adopting a SOSA research, findings highlighted the exposure of both ecosystems to potential malicious cyber related activities. The interesting realisation that, currently, only a small number of subcomponents within both ecosystems are highly vulnerable to cyber threats should not be taken as a reassuring factor. The increasing adoption of digital technologies will, consequently, increase this number in the years to come. Solutions like Port Community Systems and the concept of Smart Ports are notable case studies that should be analysed in future research.

Additionally, a second major realisation from this analysis is that most of the subcomponents in both ecosystems, if affected by a cyber-related disruption, may cause a physical, knock-on, effect. Disrupting the ship's main engine, the navigation aids or the safety thresholds of cranes may lead to accidents with devastating consequences, affecting, pending on their scale, the very socio-economic wellbeing of states and peoples.

Addressing cyber risks in the maritime sector is not solely a technology problem. Maritime stakeholders should act proactively and develop business continuity mechanisms to react efficiently and timely in the event of a cyber attack against any of the components of the MTS. States and national competent authorities should push ship, port and terminal operators to act accordingly, while keeping an eye on relevant international regulations, and geopolitical tensions that could impact regional security.

An attack on a ship is not a distant scenario, but what should be mentioned is that such an attack may not inevitably translate into a halt of operations for the vessel, as there are redundancy measures in place, but it will certainly affect normal operations. Current research and corporate initiatives to address security challenges such as AIS trustworthiness, GPS anti-spoofing techniques, sensor network monitoring for increased onboard safety, container monitoring and tracking, should be coupled with state-driven initiatives aiming to improve the industry's cybersecurity posture.

Future research, based on the findings of this paper, can follow several different angles. We would suggest an analysis of existing findings presented in the paper using FMEA (Failure Mode and Effect Analysis), in order to rank all candidates. In addition, as we recognised that this research was based on a qualitative analysis further research should be carried out bringing to surface more numerical elements through a quantitative methodology. Finally, inclusion of uncertainties in the transport system could provide an interesting angle in the future research.

Author Contributions: Conceptualization, C.K. and S.K.; methodology, T.W., C.K. and S.K.; formal analysis, C.K., S.K. and G.K.; investigation, C.K. and S.K.; resources, C.K.; data curation, C.K.; writing—original draft preparation, C.K., S.K. and T.W. and G.K.; writing—review and editing, C.K., S.K., T.W. and G.K.; visualization, C.K.; project administration, C.K. and S.K.; funding acquisition, T.W. and C.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partly funded by the Stavros Niarchos Foundation, as part of the main author's fellowship at Chatham House, and, partly, from the Alan Turing Institute, Department of Defence and Security.

Institutional Review Board Statement: Ethical review and approval were waived for this study, due to methodology limitations.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: Data available on request due to privacy restrictions. The data presented in this study are available on request from the corresponding author. The data are not publicly available due to GDPR restrictions.

Acknowledgments: The authors would like to thank the Stavros Niarchos Foundation for their funding and support of the main author's fellowship at Chatham House. We would also like to thank the Queen Elisabeth II Academy for Leadership in International Affairs and the International Security Department staff for their guidance, contributions, and trust in this work. The authors would also like to express their gratitude to all the people who contributed one way or another to the publication of this paper. Particular thanks go to the people who were interviewed for this project, along with all the participants who attended the roundtable discussions. The valuable feedback received from anonymous peer reviewers was incorporated, as far as possible, into the paper.

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

Appendix A

The following table summarises the most notable maritime related cyber incidents as identified during the research process. This is informed by the author's previous published work and the Risk Focus Cybersecurity prepared by Thomas Miller and the UK P&I Club [3].

Table A1. Notable Maritime Related Cyber Incidents.

Date	Victim	Incident Description
2010–2011	Greek Shipping Company	For 2 years a Greek shipping company suffered several successful piracy attacks in the Gulf of Aden, since local pirates hired hackers to gain access to the company's HQ and identify the most vulnerable ships along with route timetables. Hackers were able to gain access to the company's IT systems via wi-fi equipment that was installed at the company's offices.
August 2011	Iranian Shipping Line (IRISL)	The servers were hacked resulting in damage to data relating to rates, loading, delivery and location. Consequently, the location of many cargo containers remained unidentified and an undisclosed amount of financial losses were incurred as a result.
2011–2013	Port of Antwerp	The port had been a victim of an APT attack since 2011 commissioned by a drug cartel. The attack targeted terminal systems which were subsequently compromised by hackers and used to release containers without port authorities becoming aware. Illicit drugs and contraband worth approximately USD 365 million, firearms and approximately USD 1.5 million were seized when authorities finally became aware
2012	Australian Customs & Border Protection Service agency	Cargo systems controlled by customs and border protection were hacked in order to determine which shipping containers were suspected by authorities
2012–2014	Danish Port Authority	An email virus spread through the port network that was likely initiated through an infected pdf document. The virus spread and successfully reached other Danish government institutions
April 2016	South Korea	280 ships were forced to return to port due to problems on their navigation systems. The issue was largely blamed on North Korea however this remains unconfirmed

Table A1. *Cont.*

Date	Victim	Incident Description
June 2017	AP Moller Maersk	NotPetya also known as ExPetr ransomware led to outages on A.P. Moller Maersk computer systems impacting both oil and gas production and port operations. Following the incident, Maersk claimed to have changed its IT systems to prevent similar incidents from occurring in the future. The incident resulted in an estimated USD 300 million of losses
June 2017	Ships in Novorossiysk	At least 20 ships in the Black Sea were reporting false data was being transmitted, indicating the ships were 32 km inland of their actual position. It is now believed to have been as a result of a GNSS spoofing attack
November 2017	Clarksons	Perpetrators gained unauthorized access to computer systems, accessing confidential information and threatening to release information unless ransom payment is made. Company share prices decreased by 2.71%
July 2018	Cosco US	Cosco's Shipping Lines suffered from a cyber breach that affected email and network telephone initially in the US, but not ships. This expanded to their Americas facilities hence the company decided to shut down the connections with other regions for further investigation. The company was able to recover within a week. It is believed to have been a malware (ransomware) incident.
September 2018	Ports of Barcelona & San Diego	Within a week both ports suffered from a cyber-related business disruption event. Even though both organizations did not disclose a lot of information, they both claimed that this was not a major disruption and it affected mainly IT systems at shore. It is assumed that it was the same malicious content that affected both ports.
January 2018–September 2019	GPS and AIS interference in Eastern Mediterranean	Several ships and offshore platforms reported GPS interference in the region for a large period of time. NATO Maritime Command was forced to issue a notice requesting additional information by affected parties.
June–August 2019	GPS and communications interference in the Strait of Hormuz	During several maritime related incidents in the Strait of Hormuz, generated over a period of high tensions between Iran and the USA, several ships reported interference in their GPS and communications channels.
May 2020	Shahid Rajaee port, Iran	The Iranian Port of Shahid Rajaee suffered from a cyber attack, allegedly linked to Israel, that affected shipping traffic along with computers that regulate the flow of vessels, trucks and good, creating massive backups on waterways and roads leading to the facility.
Q1 and Q2 2020	Cyber attacks on shipping companies	During the first two quarters of 2020, amidst the COVID-19 pandemic, an increased number of cyber attacks to major shipping companies has been reported. Companies like Mediterranean Shipping Company (MSC), Toll Group (twice) and Carnival Cruises suffered from cyber breaches, where sensitive data of employees, clients, passengers and suppliers were exposed. These breaches appear to have common characteristics as data centers of these companies were mainly affected.

Appendix B. Interview Questionnaire

Q1 How many years of experience do you have in the maritime/cyber-security sector?

- 0–5
- 6–10
- 11–15
- 15–20

Q2 In which field of the maritime sector do you work?

- Shipowners and port operators
- Chief Information Security Officers (CISO)
- In-formation security and technology providers
- Marine insurers
- Brokers

- Academics
- Other/please specify

Q3 Which are the subcomponents of modern ship:

- Signal light column
- Anchor and mooring winch control system
- Engine Control Room System
- Switchboards
- Internal communications
- TV-Entertainment-Internet Access Systems
- Bow Thruster Control System
- Water Ingress Detection System
- GMDSS Console
- Fleet Management system
- Alarm Monitoring and Control System
- Power Management
- Navigation Equipment
- Bridge control console
- VDR/S-DR
- Reefer Container Monitoring System
- Navigation Lights
- Loading and Stability Computer
- Other (please specify)

Q4 Which are the subcomponents of a modern port:

- Port Facility offices
- Cargo handling vehicles, cranes and conveyer assets
- Financial Management and Monitoring
- Port Facility accommodation
- Access control points
- Refineries
- Container and vehicle movement systems
- Warehouse and storage (chemical, gas, bulk and dry cargo) facilities
- Rail systems
- Power plants
- Asset management systems (cargo, vehicle)
- Vessel Traffic Control Tower
- Terminal Facilities (Container Terminal, Oil tank terminal)
- Access control management system
- Maintenance areas
- Cargo handling systems such as pipelines and conveyer systems
- Other (please specify)

Q5 Classify the potential consequences of a cyber incident for the following subcomponents of a modern ship.

Sub Component	High	Medium	Low
Signal light column			
Anchor and mooring winch control system			
Engine Control Room System			
Switchboards			
Internal communications			
TV-Entertainment-Internet Access Systems			

Sub Component	High	Medium	Low
Bow Thruster Control System			
Water Ingress Detection System			
GMDSS Console			
Fleet Management system			
Alarm Monitoring and Control System			
Power Management			
Navigation Equipment			
Bridge control console			
VDR/S-DR			
Reefer Container Monitoring System			
Navigation Lights			
Loading and Stability Computer			
Other (please specify)			

Q6 Classify the potential consequences of a cyber incident for the following subcomponents for a modern port.

Sub Component	High	Medium	Low
Port Facility offices			
Cargo handling vehicles, cranes and conveyer assets			
Financial Management and Monitoring			
Port Facility accommodation			
Access control points			
Refineries			
Container and vehicle movement systems			
Warehouse and storage (chemical, gas, bulk and dry cargo) facilities			
Rail systems			
Power plants			
Asset management systems (cargo, vehicle)			
Vessel Traffic Control Tower			
Terminal Facilities (Container Terminal, Oil tank terminal)			
Access control management system			
Maintenance areas			
Cargo handling systems such as pipelines and conveyer systems			
Other (please specify)			

Q7 Rank the vulnerability against a cyber incident for the following subcomponents of a modern ship

Sub Component	High	Medium	Low
Signal light column			
Anchor and mooring winch control system			
Engine Control Room System			
Switchboards			
Internal communications			
TV-Entertainment-Internet Access Systems			
Bow Thruster Control System			
Water Ingress Detection System			
GMDSS Console			
Fleet Management system			
Alarm Monitoring and Control System			
Power Management			
Navigation Equipment			
Bridge control console			
VDR/S-DR			
Reefer Container Monitoring System			
Navigation Lights			
Loading and Stability Computer			
Other (please specify)			

Q8 Rank the vulnerability against a cyber incident for the following subcomponents of a modern port

Sub Component	High	Medium	Low
Port Facility offices			
Cargo handling vehicles, cranes and conveyer assets			
Financial Management and Monitoring			
Port Facility accommodation			
Access control points			
Refineries			
Container and vehicle movement systems			
Warehouse and storage (chemical, gas, bulk and dry cargo) facilities			
Rail systems			
Power plants			
Asset management systems (cargo, vehicle)			
Vessel Traffic Control Tower			
Terminal Facilities (Container Terminal, Oil tank terminal)			
Access control management system			
Maintenance areas			

Sub Component	High	Medium	Low
Cargo handling systems such as pipelines and conveyer systems			
Other (please specify)			

Q9 Identify the relevant affected fields in case of a cyber incident to each of the following subcomponents of a modern ship

Sub Component	Data	Environment	Human	Physical
Signal light column				
Anchor and mooring winch control system				
Engine Control Room System				
Switchboards				
Internal communications				
TV-Entertainment-Internet Access Systems				
Bow Thruster Control System				
Water Ingress Detection System				
GMDSS Console				
Fleet Management system				
Alarm Monitoring and Control System				
Power Management				
Navigation Equipment				
Bridge control console				
VDR/S-DR				
Reefer Container Monitoring System				
Navigation Lights				
Loading and Stability Computer				
Other (please specify)				

Q10 Identify the relevant affected fields in case of a cyber incident to each of the following subcomponents of a modern port

Sub Component	Data	Environment	Human	Physical
Port Facility offices				
Cargo handling vehicles, cranes and conveyer assets				
Financial Management and Monitoring				
Port Facility accommodation				
Access control points				
Refineries				
Container and vehicle movement systems				
Warehouse and storage (chemical, gas, bulk and dry cargo) facilities				

Sub Component	Data	Environment	Human	Physical
Rail systems				
Power plants				
Asset management systems (cargo, vehicle)				
Vessel Traffic Control Tower				
Terminal Facilities (Container Terminal, Oil tank terminal)				
Access control management system				
Maintenance areas				
Cargo handling systems such as pipelines and conveyer systems				
Other (please specify)				

Q11 Please add any comments, that you might have here. Thank you for your participation to our survey!

References

1. Hellenic Shipping News Worldwide. Available online: https://www.hellenicshippingnews.com/maritime-cyber-attacks-increase-by-900-in-three-years/ (accessed on 7 December 2021).
2. Norma Cyber. Available online: https://www.normacyber.no/news/norma-annual-threat-assessment-2022 (accessed on 30 April 2022).
3. Kapalidis, P. Cybersecurity at Sea. In *Global Challenges in Maritime Security*, 1st ed.; Otto, L., Ed.; Springer: Cham, Switzerland, 2020; Volume 1, pp. 127–143.
4. Mismarine. Available online: https://mismarine.com/benefits-and-challenges-digitising-the-shipping-industry/ (accessed on 1 January 2022).
5. ENISA. Available online: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021 (accessed on 3 February 2022).
6. Maersk. Available online: https://investor.maersk.com/news-releases/news-release-details/cyber-attack-update (accessed on 10 November 2021).
7. Reuters. Available online: https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19I1NO (accessed on 15 November 2021).
8. Digital Guardian. Available online: https://digitalguardian.com/blog/cost-malware-infection-maersk-300-million (accessed on 12 April 2022).
9. Kapalidis, P. 4 Cases of Cybersecurity Failures in Shipping History. *Collab. Shipp. Ind. Innov. Technol.* **2017**, 10–11.
10. Los Angeles Times. Available online: https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html (accessed on 2 October 2021).
11. CNBC. Available online: https://www.cnbc.com/2018/01/24/cnbc-interview-with-moller-maersk-ceo-soren-skou-from-the-world-economic-forum-2018.html (accessed on 2 February 2022).
12. IMO. Available online: https://www.imo.org/en/OurWork/Security/Pages/Guidance-home.aspx (accessed on 3 January 2022).
13. Jamshidi, M. *Systems of Systems Engineering: Principles and Applications*; CRC Press: Boca Raton, FL, USA, 2017.
14. Boyes, H.; Isbell, R.; Luck, A. *Cyber Security of Ports and Port Systems*; The Institute of Engineering and Technology: Stevenage, UK, 2016.
15. Boyes, H.; Isbell, R.; Luck, A. *Cyber Security of Ports and Port Systems v2*; The Institute of Engineering and Technology: Stevenage, UK, 2020.
16. Ablon, L. Cybersecurity Considerations for the Maritime Environment. In *Issues in Maritime Cybersecurity*, 1st ed.; DiRenzo, J., Drumhiller, N., Roberts, F., Eds.; Westphalia Press: Washington, DC, USA, 2017; Volume 1, pp. 17–24.
17. Allianz. Available online: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Safety-Shipping-Review-2017.pdf (accessed on 3 October 2021).
18. Global Maritime Forum. Available online: https://www.globalmaritimeforum.org/content/2019/10/Global-Maritime-Issues-Monitor-2019.pdf (accessed on 6 November 2021).
19. Progoulakis, I.; Nikitakos, N.; Rohmeyer, P.; Bunin, B.; Dalaklis, D.; Karamperidis, S. Perspectives on Cybersecurity for Offshore Oil and Gas Assets. *J. Mar. Sci. Eng.* **2021**, *9*, 112. [CrossRef]
20. MITRE. Available online: https://attack.mitre.org/ (accessed on 14 June 2022).
21. The Maritime Executive. Available online: https://www.maritime-executive.com/blog/digitalization-and-ship-connectivity-in-2018 (accessed on 14 November 2021).

22. Allianz. Available online: https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/human-error-shipping-safety.html (accessed on 22 December 2021).
23. ENISA. Available online: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector (accessed on 14 February 2022).
24. Polemi, N. Ports' Critical Infrastructures. In *Port Cybersecurity. Securing Critical Information Infrastructures and Supply Chains*, 1st ed.; Stover, T., Ed.; Elsevier: Amsterdam, The Netherlands, 2018; Volume 1, pp. 3–7.
25. Kapalidis, C. Maritime Threat: Is it Real? *Seatr. Marit. Rev.* **2018**, 115.
26. UNCTAD. Available online: https://unctad.org/system/files/official-document/rmt2021_en_0.pdf (accessed on 16 February 2022).
27. Notteboom, T.; Pallis, A.; Rodrigue, J.P. *Port Economics, Management and Policy*, 1st ed.; Routledge: New York, NY, USA, 2022; pp. 1–104.
28. The Guardian. Available online: https://www.theguardian.com/world/2018/jul/05/iran-retaliate-us-oil-threats-eu-visit-hassan-rouhani-trump (accessed on 7 October 2021).
29. U.S.Department of Transportation Maritime Administration. Available online: https://www.maritime.dot.gov/msci/2019-012-persian-gulf-strait-hormuz-gulf-oman-arabian-sea-red-sea-threats-commercial-vessels (accessed on 15 April 2020).
30. REUTERS. Available online: https://www.reuters.com/article/us-iran-oil-factbox/strait-of-hormuz-the-worlds-most-important-oil-artery-idUSKBN1JV24O (accessed on 9 January 2022).
31. U.S. Energy Information Administration. Available online: https://www.eia.gov/international/content/analysis/special_topics/World_Oil_Transit_Chokepoints/wotc.pdf (accessed on 6 October 2021).
32. Emirates NBD. Available online: http://www.emiratesnbdresearch.com/research/article/?a=gcc-maritime-strategy-enters-a-new-era-969 (accessed on 5 February 2022).
33. REUTERS. Available online: https://www.reuters.com/article/gulf-qatar-port/gulf-crisis-a-blessing-in-disguise-for-qatar-seaport-idUSL8N1JC2LJ (accessed on 8 January 2021).
34. BP. Available online: https://www.bp.com/en/global/corporate/news-and-insights/press-releases.html (accessed on 6 January 2021).
35. Forti, N.; d'Afflisio, E.; Braca, P.; Millefiori, L.M.; Willett, P.; Carniel, S. Maritime Anomaly Detection in a Real-World Scenario: Ever Given Grounding in the Suez Canal. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 13904–13910. [CrossRef]
36. It Governance. Available online: https://www.itgovernance.co.uk/nis-directive (accessed on 10 December 2021).
37. European Commission. Available online: https://digital-strategy.ec.europa.eu/en/policies/nis-transposition (accessed on 16 February 2022).
38. ZDNet. Available online: https://www.zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-notpetya-attack/ (accessed on 1 December 2021).
39. Transport Styrelsen. Available online: https://www.transportstyrelsen.se/en/shipping/ (accessed on 12 January 2022).
40. Qatar tribune. Available online: https://www.qatar-tribune.com/news-details/id/155546 (accessed on 3 January 2022).
41. RISCS. Available online: https://www.riscs.org.uk/project/cr4b-cyber-readiness-for-boards/ (accessed on 3 March 2022).
42. Informa Connect. Available online: https://informaconnect.com/how-will-the-marine-insurance-industry-respond-to-new-sources-of-risk/ (accessed on 2 January 2022).
43. Lloyd's. Available online: https://www.lloyds.com/market-resources/underwriting/risk-codes (accessed on 11 January 2022).
44. Futurenautics. Available online: http://www.navarino.co.uk/wp-content/uploads/2018/04/Crew_Connectivity_2018_Survey_Report.pdf (accessed on 16 October 2021).
45. Athanasoglou, C.; Papoutsidakis, M.; Papachristos, D.; Nikitakos, N. Automated Docking Procedure in Modern Shipping. *Int. J. Comput. Appl.* **2019**, *178*, 55–58. [CrossRef]
46. Zolich, A.; Palma, D.; Kansanen, K.; Fjørtoft, K.; Sousa, J.; Johansson, K.; Jiang, Y.; Dong, H.; Johansen, T. Survey on Communication and Networks for Autonomous Marine Systems. *J. Intell. Robot. Syst.* **2018**, *95*, 789–813. [CrossRef]
47. Maritime Cybersecurity. Available online: https://www.maritime-cybersecurity.com/National_Maritime_Cybersecurity_Plan.html (accessed on 21 October 2021).