Advanced Research on Information Systems Security

ISSN: 2795-4609 | ISSN: 2795-4560
Print & Online

A literature review and a bibliometric analysis of cybersecurity in ships maritime navigation

Carine Dominguez Péry[a]*, Pedro Merino Laso [b, c]

[a]*University of Grenoble Alpes – Grenoble INP, CERAG laboratory, 38000 Grenoble, France*

[b] *French Maritime Academy (ENSM), Nantes, France*

[c] *Arts et Métiers Institute of Technology, École navale, IRENAV EA 3634, BCRM de Brest, CC 600, 29240 Brest cedex 9, France*

[a]*Email: carine.dominguez-pery@univ-grenoble-alpes.fr*

[b]*Email: pedro.merino-laso@supmaritime.fr*

Abstract

Cybersecurity of ships constitutes a hot topic with increased vulnerabilities in the context of digitalization. Interestingly, little is known about ships cyberattacks both in terms of types, frequencies and potential responses and/or mitigation plans. By mobilizing Admiral dataset, we set up a few statistics to present the problem of cybersecurity in the maritime sector focusing on ships cyberattacks. Owing to a bibliometric co-citation analysis, we described the main themes developed by the top four cited papers of each cluster and provide a literature review with the most recent papers highlighting the most recent themes and concepts of interest to increase ships' cyber resilience.

Keywords: Maritime navigation; cyber risks, cybersecurity; bibliometric analysis; statistics.

Citation: C. Dominguez-Pery and P. Merino Laso, "A Literature Review and a Bibliometric Analysis of Cybersecurity in Ships Maritime Navigation", ARIS2-Journal, vol. 4, no. 2, pp. 111–131, Dec. 2024.

DOI: https://doi.org/10.56394/aris2.v4i2.49

---

* Corresponding author. Email address: carine.dominguez-pery@univ-grenoble-alpes.fr

1. Introduction

In the context of increased digitalization, ships cyberattack constitute a hot topic with potentially drastic economic losses and supply chain blockages. The cyberattacks of the two majors ship owners (MAERSK in 2017 and CMA CGM in 2020) hinder major future important risks for the whole maritime transportation industry which could potentially lead to total blockage of maritime supply chains in case of multiple attacks in different geographic areas. According to "Maritime Cyber Priority 2023" survey conducted by DNV (2023), a significant proportion of maritime professionals predict serious consequences from cyber incidents. Specifically, 76% believe that such incidents could likely lead to the closure of a strategic waterway. Additionally, 60% anticipate that cyber-attacks could result in ship collisions and 68% see the possibility of groundings. Furthermore, 56% of these professionals even expect such incidents to potentially cause physical injury or death.

Even though the technological and economic consequences can be drastic, there is still limited information regarding the current extent of the phenomenon as professionals may underreport these threats and attacks. In the keywords co-occurrence analysis of [64] (2023:455), ships appear as a separate phenomenon of interest in their search related to cybersecurity in maritime transportation. To our knowledge, no paper proposes an analysis of the literature specifically based on ships' cyber risks and resilience apart from [41] that provides a technological approach, not integrating the human and organizational aspects. Most papers in the literature are related to the "maritime transportation" or the "maritime industry" with a larger focus.

In this paper, we wish to describe the phenomenon and provide a state of the art on the main challenges to increase ships' cyber security digital resilience. We develop the following research question: What do ships' cyber-attacks represent and what are the main challenges to increase their digital resilience? Following a few definitions and a characterization of the particularities of ships' cyber risks [2], we propose an assessment of the phenomenon of ships' cyber attacks with a few statistics, present our research methodology [3] followed by a bibliometric analysis [4] and a literature review of most recent themes [5].

2. Cybersecurity in maritime transportation: definitions and particularities

90% of maritime trade is made by the seas. Because of new regulations and economic reasons, the maritime sector is digitalizing systems in order to become more efficient. Digital systems allow performing complex procedures automatically or with remote assistance. Thanks to the evolution called the "Industry 4.0 revolution", IT (Information Technology) systems have started to communicate with OT (Operational Technology) systems bringing new capabilities to the industrial procedures. Also, this evolution includes communication capabilities with different objectives i.e., fleet monitoring or preventive maintenance.

At the same time, attackers have seen in these systems an opportunity to penetrate in critical systems and affect their security. These attacks targeting digital systems, called frequently as cyberattacks, are more and more

numerous. There exist databases as Admiral[a] [30] that list known cyberattacks impacting the maritime sector. Figure 1 represents the evolution of the number of maritime cyberattacks. We can easily appreciate that since 2018, the number of cyberattacks is rising fast. Also, some important companies as Maersk in 2017 had suffered important consequences.

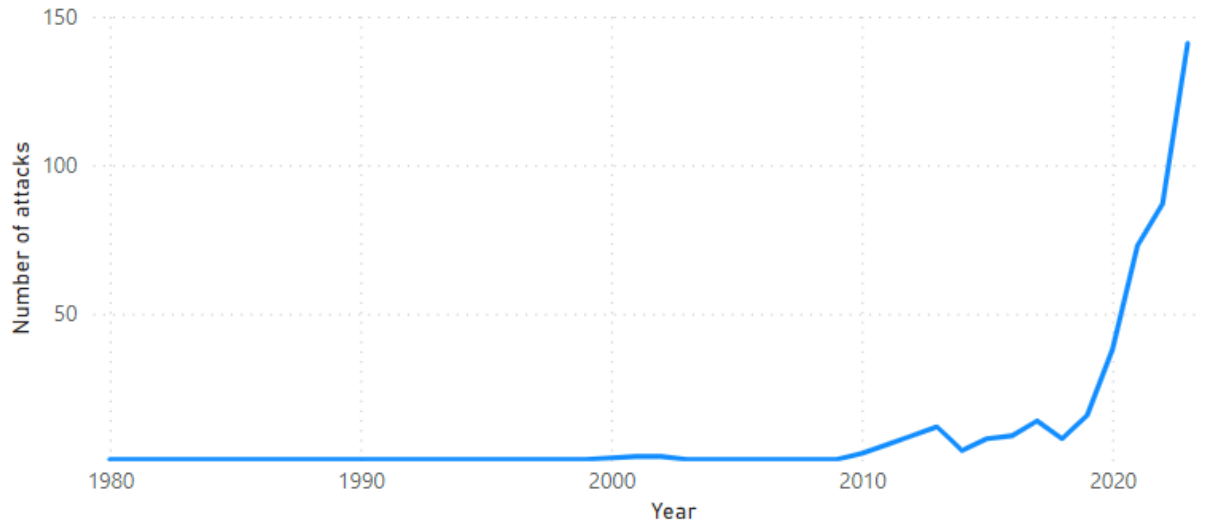

Figure 1: Number of cyberattacks in maritime sector per year

Due to this situation, the International Maritime Organization (IMO) adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management System (SMS) in 2017. IMO stated through this resolution that shipowners should consider in the SMS cyber risk management in accordance with the objectives and functional requirements of the (International Safety Management) ISM Code. This resolution has been followed by a second publication where the IMO present high-level recommendations on maritime cyber risk management. Although resolution MSC.428(98) has been published in 2017, administrations had started to verify if cyber risks are appropriately addressed in SMS since 1 January 2021.

Multiple definitions exist for all the terms used in maritime and cybersecurity domains. For our work, we have decided to follow the definitions of BIMCO's guidelines because this guide regroups the needs of the conjunction of these two domains [14]. All common terms and types of cyberattacks are well defined taking in account maritime specificities. For instance, cyberattack is defined as follows:

Cyberattack *is any type of offensive maneuver that targets IT and OT systems, computer networks, and/or personal computer devices and attempts to compromise, destroy or access company and ship systems and data.*

Maritime systems present multiple particularities due to used systems, size, and the environment. When maritime vessels are navigating offshore, communications become difficult. For this, ships are commonly quite isolated and the information exchanges with the shore are limited. This isolation is also applied for the crew. That is, a

[a] Admiral (Advanced Dataset of Maritime cyber incidents Released for Literature) database is available online at: https://gitlab.com/m-cert/admiral/ Accessed 06 February 2024.

reduced crew with limited knowledge of cybersecurity needs response to crisis scenario and take experts aboard is not always possible. Also, they embark numerous industrial systems as engines, pumps, or water treatment. All of them are critical systems due to their importance and potential consequences in case of malfunctioning. It is important to understand that often the reaction times are important because of the size of vessels reducing the maneuverability. Also, these industrial systems use specific protocols that are only used in the maritime sector as NMEA. In addition, the seas are regulated by organizations as the IMO but also by multiple countries for shore navigation or when entering into a port. The hierarchy and different actors as the Maritime Rescue Coordination Centres (MRCC) can impact the definition of response procedures.

3. Methodology

In this section, we present the followed methodology for making and statistical analysis of known cyberattacks in maritime sector and the bibliometric analysis for research works.

3.1. Statistics

Admiral database is available for free in a Gitlab repository and regularly updated with new information. All this data can be downloaded in a CSV (Comma Separated Values) file. This format allows importing this data into numerous software as LibreOffice Calc or Microsoft Power BI. These two software solutions have been used to make a basic statistical analysis based on the columns of the table. The last column includes external links that allows exploring further details.

3.2. Bibliometric analysis and literature review

We developed a bibliometric review on ship cyber-attacks and threats with the software VosViewer [66]. A key benefit of bibliometric methods is their ability to help reduce reviewers' subjectivity and bias, which are inherent in conventional qualitative reviews [77]. We followed the four-step procedure as outlined by Kovacs et al. [36]. First, we started to select our sample of articles by identifying the 4 most cited papers in Web of Science (WoS) core collection databases, in the research area « business economics », with the key words "« cyber security » and « maritime transportation » which led to a set of 72 articles. Finally, we conducted a co-citation analysis (CCA) of cited references with a threshold of 3 co-cited references that lead to the core 43 articles that constitute the main historical themes in ship cyber security and resilience. Finally, we interpreted the results of the CCA by labelling each of the 5 clusters obtained, describing their content with the top 4 more cited papers and analyse the links among these clusters.

4. Statistics

In this section, we present the results of statistic and bibliometric analysis. We also include the description of the most know relevant cyberattacks impacting the maritime sector impacting maritime navigation.

4.1. Statistics with graphs

In this subsection, we analyze the evolution and distribution of cyberattacks based on the cyberattacks identified in Admiral Database. It is important to understand the limitations of this database. First, only the attacks impacting the maritime sector directly are listed. Cyberattacks impacting organizations out of this perimeter, as several logistic companies, are not taken into account. Second, only attacks having a significant impact are cited. For example, little phishing campaigns with no success are not listed. Third, each cyberattack is categorized in one category when it can impact multiple actors, or a set of vulnerabilities can be exploited by different means. Finally, Admiral only includes cyberattacks where public information has been shared.

In the maritime sector, there exist numerous actors as ports, logistics, shipowners, and shipyards. All of them can be a target for a cyberattack as we can appreciate in Figure 2. This figure illustrates that cyberattacks targeting shipowners, ports and logistics represent nearly half of the total. This can be caused because of their economic importance and because they communicate with numerous actors through exposed systems as websites and e-mail. Other actors are less exposed to cyberattacks because they are more isolated and more protected due to its critical importance.

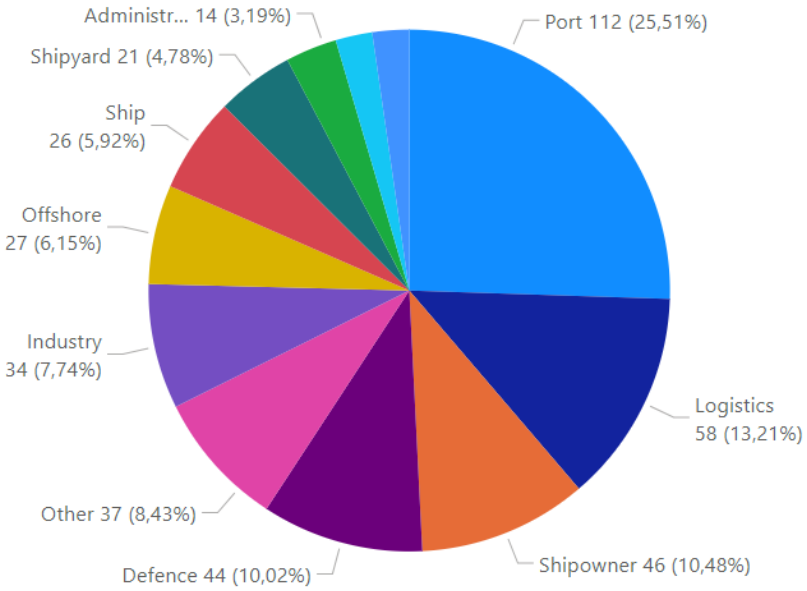

Figure 2: Type of cyberattacks in maritime sector per target types

Figure 3 presents the distribution of listed cyberattacks by type. The most common used attacks are malware and ransomware. These types of attacks exploit different vulnerabilities to access and compromise IT and OT systems. In the case of ransomware, attackers demand a ransom to the organization to recover the normal functioning of their systems. In second place, Denial of Service (DoS) attacks compromise the availability of servers. Intrusion and data leak are attacks with similar objectives that are often related to economic or industrial spying interests. Finally, GPS and AIS jamming and spoofing impacts on the security of navigation and the quality of the data used

by the fleet centers.

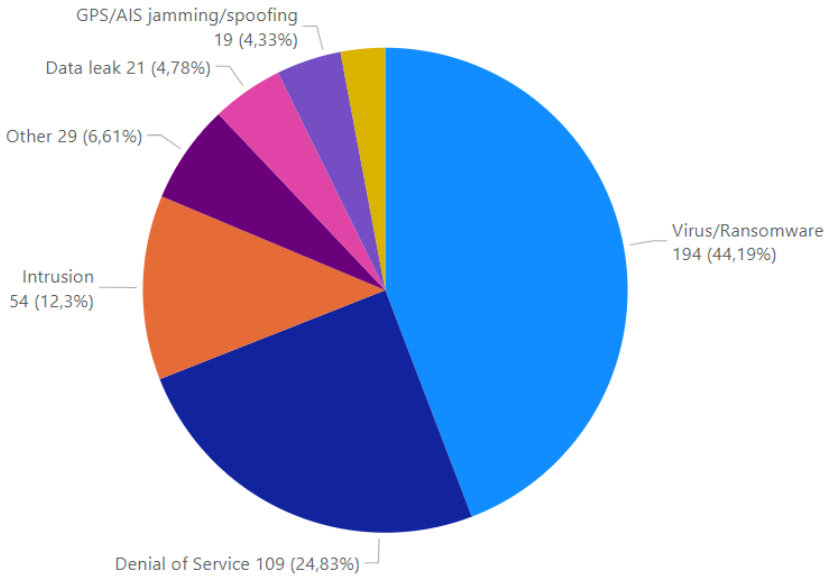

Figure 3: Type of cyberattacks in maritime sector

Figure 4 presents the distribution of cyberattacks targeting ships by type. The most common attacks impact GNSS (Global Navigation Satellite System) position and AIS systems. It is difficult to dissociate GNSS and AIS attacks because AIS transponder transmits the received GNSS position. That is, if GNSS position is attacked, AIS position is also corrupted. In addition, GNSS attacks are often detected analysing AIS data. In Admiral database, attacks targeting GNSS are presented in the category "GPS/AIS/jamming/spoofing". That is because GPS is the most used and known GNSS and sometimes these two acronyms are misused. It is important to note that some cyberattacks as GNSS Jamming and AIS spoofing are not anymore listed because they have become ordinary scenarios. They are only listed when their impact is notable for maritime navigation. Nevertheless, attacks targeting vessels can produce bigger consequences than in other targets because of the criticality of impacted

systems i.e., loss of human lives or produce environmental catastrophe.

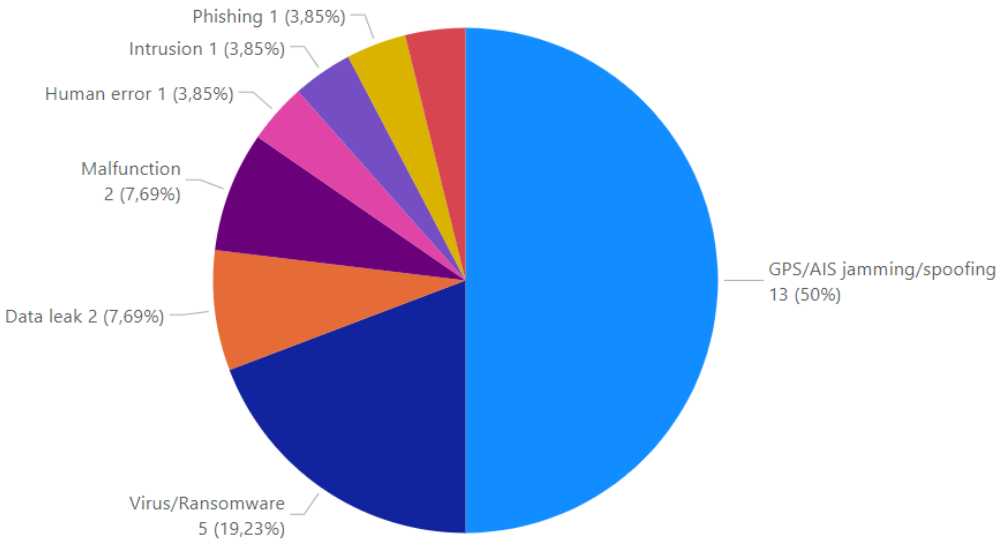

Figure 4: Type of cyberattacks in ships

Until now, no major incidents impacting navigation safety have been recorded. In recent years, some cyberattacks were directly targeted on ships. As we can appreciate in Figure 5, the number of cyberattacks targeting ships is low. However, until today ships were quite isolated to external connections because of poor communication links. Today, they exist better communication possibilities thanks to new satellite constellations as Starlink or Marlink. They bring new applications but also new risks. In addition, industrial systems offer more connection possibilities as the result of industry 4.0 revolution that will take advantage of these high bandwidth and low latency connections.

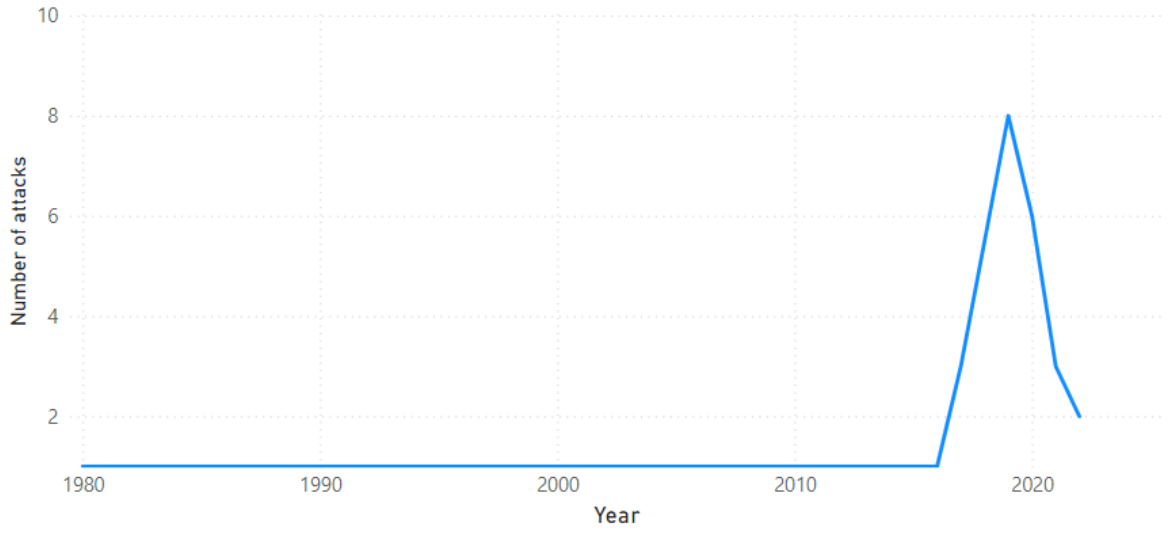

Figure 5: Evolution of the number of cyberattacks on ships

To aboard these risks, IACS (International Association of Classification Societies) had adopted new requirements in terms of cybersecurity that are listed in two documents: UR E26 and UR E27. These requirements will be applied to new ships contracted for construction on and after 1 January 2024.

All this data and statistical analysis let us conclude that maritime cyberattacks have in general big economic consequences and even if they do not target ships directly, they can compromise the navigational safety. The most common incidents that can impact ships are related to GPS and AIS jamming and spoofing. As well, exploitation of common vulnerabilities through malware and more precisely ransomware is usually employed. Additionally, multiple attacks that had been classified for ports and shipowners had been an impact on maritime navigation creating delays and potential safety risks. These attacks prove that cybersecurity is not only a technological challenge but also, they require new procedures for human organization and management.

4.2. Major known maritime cyberattacks impacting ships and lessons learned

Some cyberattacks had been widely known because of their impact and the importance of the targeted companies. The three biggest companies in the maritime shipping industry have suffered important cyberattacks: MSC (2020), Maersk (2017) and CMA-CGM (2020). These cyberattacks serve as a reminder of the ongoing cybersecurity challenges faced by large corporations and the need for robust defense strategies. Also, these attacks highlighted the vulnerabilities of critical infrastructure and global supply chains to cyber threats. In this section, we describe these three cyberattacks in addition to GPS attacks in the black sea. They evidence that every actor is concerned and can be impacted because collateral consequences.

One of the most cited attacks has been performed against the shipowner Maersk in 2017. This cyberattack has been the first known major attack against a major actor in maritime shipping. Maersk is one of the biggest companies of maritime transport with a fleet of more than 900 ships transporting about 20% of the world's GDP. In June 2017, the malware Notpetya allows entering Maersk's networks and spread over all IT systems, that is, more than 55,000 computers and 4,000 servers in less than 7 minutes. In consequence, they have lost access to more than 2000 business applications. The repercussions were a drop of 20% of transported volume with a cost of 300M$. After 14 days, Maersk recover the most critical systems. And 1 month after, they have reached a total recovery. Even if this cyberattack had targeted office IT systems, ships had been also impacted losing important communications with the shore creating important potential security risks. The company had communicated and shared abundant details about the impacts and recovery measures.

In September 2020, CMA-CGM, the third world's largest shipping companies, fell victim to a cyberattack. The attack targeted the company's IT systems, leading to disruptions in its global operations. CMA-CGM's booking, and documentation systems were affected, causing delays in cargo shipments. The cyberattack impacted various aspects of the company's operations, including customer service and communications. CMA-CGM initially confirmed the incident as a ransomware attack but did not disclose the specific ransom demands. CMA-CGM worked to restore its systems and services while cooperating with law enforcement agencies to investigate the incident. The company assured customers that its core shipping operations remained functional despite the

cyberattack.

MSC suffered a cyberattack in April 2020[b] with limited operational impacts thanks to well-defined Business Continuity Plans (BCP). However, multiple digital tools as well as their website (www.msc.com) were unavailable for a few days because of the strategy of the contingency plan. MSC shared technical information with its partners to prevent this from happening again.

In 2023, DNV said its ShipManager software had been hit by a ransomware attack impacting 1000 shipping vessels[c]. This modular software solution supports management of vessels and fleets in all technical, operational and compliance aspects. In consequence, users worked with an offline and disconnected solution.

Also, some examples of cyberattacks impacting ships are presented in the guidelines avoiding identification details [14]. Most of them are caused by not respect of IT hygiene measures. A dormant worm that spreads via USB devices was discovered in a disconnected power management system. Ransomware attacks are also capable to brute force password because poor policies and impact the availability and confidentiality of critical systems.

In recent years, incidents of GNSS spoofing have been reported all across the globe as in the Black Sea, posing significant challenges for maritime navigation (C4ADS, 2019). This type of incident had also appeared in Shanghai. GNSS spoofing involves the transmission of false signals to deceive GNSS receivers, leading vessels to believe they are in a different location than they actually are. False positions are shared by the AIS system with stakeholders producing serious consequences for maritime safety and security. Ships relying on GNSS for navigation may experience misalignment of their positions, potentially resulting in collisions, groundings, or other navigational hazards.

These attacks taught us that the maritime sector is vulnerable to cyberattacks that result in significant financial and operational losses. They also showed us how quickly attacks propagate through networks, affecting globally interconnected systems and causing ripple effects throughout the industry. For instance, a cyberattack against a shipowner can have an impact on multiple actors participating in the maritime supply chain. Attackers exploit vulnerabilities from heterogeneous IT and OT systems complicating the protection of maritime networks.

All these attacks can disrupt communication and coordination among vessels, port authorities, and maritime traffic management systems. These incidents highlight the vulnerability of the maritime industry to cyber threats and underscore the need for enhanced cybersecurity measures and resilient navigation systems to mitigate risks and ensure the safety of maritime operations.

5. Bibliometric analysis and a literature review of most recent themes

5.1 Bibliometric analysis

Figure 6 shows the bibliographic map of five clusters based on CCA. We made the interpretation of these clusters

[b] https://www.msc.com/en/newsroom/news/2020/april/network-outage-resolved Accessed 06 February 2024.
[c] https://www.dnv.com/news/cyber-attack-on-shipmanager-servers-update-237931 Accessed on 06 February 2024.

based on the top-four articles cited. In addition, to provide a vision of the clusters with most weight within the overall map, we provide in Table 1 the number of total articles per cluster and the average number of citations per article (based on the top-four most cited articles).

Table 1: Indicators of references output and citation impact cited by 2432 articles included in the dataset; core of 43 articles that constitute the CCA

Cluster	Label	Number of articles	Top 4 most-cited articles
A	AIS vulnerabilities	16	[12], [11], [58], [61]
B	Cyber risks scenario and human training	11	[2], [50], [64], [16]
C	AIS cyber threats and defences	8	[15], [62], [53]
D	Economic consequences	4	[55], [18], [47], [19]
E	Data-driven cyber security	4	[49], [45], [40], [71]

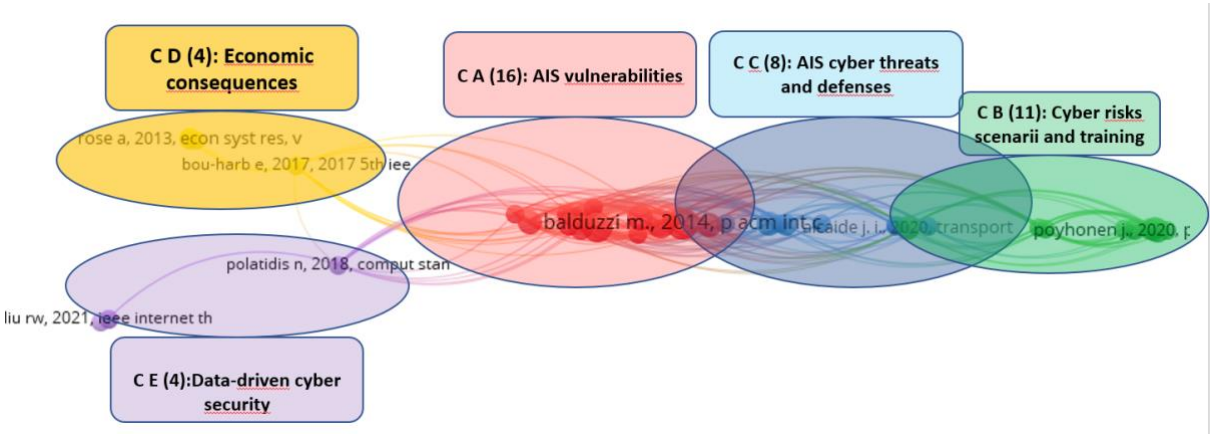

Figure 6: CCA of ships cyberattacks and resilience

In the overall map of CCA, there are two central clusters that dominate the field (Clusters A and Cluster C) that share the central AIS technology that is currently the most vulnerable in ships. On the right side, Cluster C provides responses to cyber-attacks by highlighting the main role of human training. On the left side, Cluster D concentrates on the main economic impacts and consequences of cyberattacks both on ships and ports. Finally, Cluster E

proposes several data-driven methods to cope with cyber risks.

5.1.1. Main cyber threats and vulnerabilities for ships

- Cluster A (Red): AIS cyber threats and vulnerability patterns

Cluster A gathers the most cited papers of the whole CCA, historically the most influential papers in ships' cyber security and resilience, by order of importance: Tam and Jones [61], Balduzzi et al. [12] and Svilicic et al. [58]. These papers use both qualitative method and simulations to provide surveys that highlight the main cyber threats and vulnerabilities on ships, potential causes and frameworks to cope with them. Tam and Jones [61] introduce a model-based risk assessment framework which considers a combination of cyber and maritime factors. Confronted with a range of ship functionalities, configurations, users, and environmental factors, this framework aims to comprehensively present maritime cyber-risks and better inform those in the maritime community when making cybersecurity decisions. By providing the needed maritime cyber-risk profiles, it becomes possible to support a range of parties, such as operators, regulators, insurers, and mariners, in increasing overall global maritime cybersecurity. Svilicic et al. [58] focused on the integrated navigational system (INS) that enhances the effectiveness and safety of ship navigation by providing multifunctional display on the basis of integration of at least two navigational functions, the voyage route monitoring with Electronic Chart Display and Information System (ECDIS) and collision avoidance with radar. The identified threats were analyzed qualitatively to study the source of cyber risks threatening the INS. The results obtained point out cyber threats related to weaknesses of the INS underlying operating system, suggesting a need for occasional preventive maintenance in addition to the regulatory compliance required. With the same objective of identifying the main vulnerabilities on ships, Awan et al. [11] focused on 59 historical accidents reported in literature and highlighted various vulnerability patterns, their causes, and consequences, with geographical as well as temporal relationships with different vulnerable IBS components. Finally, Balduzzi et al. [12] provide technical responses to AIS threats with protocol specifications that are tested with a simulation.

Closely related to Cluster A, Cluster C extends and details concrete responses to the main cyber vulnerabilities identified in Cluster A.

- Cluster C (Blue): AIS cyber threats and defenses

Grant et al. (2009) is one of the first papers that highlighted the Global Positioning System (GPS), possibly together with other GNSS, as potentially vulnerable targets to unintentional interference or jamming. These vulnerabilities can lead to a complete failure of the mariner's GPS receiver, or, possibly worse, the presentation to the mariner of hazardously misleading information (HMI) for navigation and awareness, depending on how the GPS receiver reacts to the jamming incident, The General Lighthouse Authorities of the United Kingdom and Ireland (GLA) in collaboration with the UK Ministry of Defense (MOD), Defense Science and Technology Laboratory (DSTL) were then one of the first to conduct a series of sea-trials with the aim of identifying the full effects of GPS jamming on safe navigation at sea. All the other papers of Cluster C provide defenses' techniques and strategies to cope with GNSS attacks and more precisely with GPS attacks. Bhatti et al. [15] explored civil maritime transportation's vulnerability to deceptive GPS signals and developed a detection technique that is

compatible with sensors commonly available on modern ships. It is shown that despite access to a variety of high-quality navigation and surveillance sensors, modern maritime navigation depended crucially on satellite navigation and that a deception attack could be disguised as the effects of slowly-changing ocean currents. In the same vein, Psiaki and Humphreys [53] investigated how GNSS could be spoofed by false signals, but special receivers can provide defenses against such attacks. This paper discussed numerous defenses strategies ranging from special signal processing within a traditional GNSS receiver to employing advanced encryption-based techniques on GNSS measurements. Finally, and totally aligned with the most recent cyberattacks like DNV, Tam and Jones [62] enlarged the scope of analysis of ships cyber-attacks by integrating ports as potential targets that can indirectly arm ships. They developed a critical analysis of current risk assessment tools and frameworks for the safety of ships and ports and individuals highlights the fact that they do not integrate and revise in real time dynamic factors such as the environment and change. In addition, operational risks can be affected by the relatively equal presence of information and operational technology (i.e. IT/OT). However, most quantitative risk assessment frameworks are normally limited to one of the other.

5.1.2. Perceived ship cyber risks and scenarios to improve training

The most cited papers mainly focus on training (Cluster B) as a human response to ships' cyber-attacks and threats as a way to mitigate the main threats and vulnerabilities highlighted in Cluster A and C.

- Cluster B (Green): Perceived ship cyber risks and scenarios to improved training

What distinguishes Cluster B from others is the fact that they highlight the key role in human training to improve cyber resilience. Alcaide and Llave [2] developed a questionnaire on maritime professionals that show that they are not well prepared in terms of training. They also highlighted the cyber risks in critical maritime infrastructures. Thai and Grewal [64] developed a study from the Maritime Security College in 2005-2006 (focus group of experts followed by a survey) on the Maritime Security Management System (MSMS) to identify key shore-based and near-shore activities associated with maritime operations that were not covered by the International Ship and Port Facility Security Code. Apart from the technical side stated as "security elements", they were one of the first and still very few to focus on the importance of humans in different aspects such as the attitude towards activities, the importance of relationships between different stakeholders at sea, the perceived effectiveness of security dimensions (information security only ranked 6), the attitude towards criteria of a good/effective MSMS and the attitude towards inputs of curriculum for education and training needs. Poyhonen et al. [50] questioned the trust of humans on the technological architecture. Finally, Bodeau et al. [16] identified ways in which a system-of-systems threat scenario could be used and demonstrated the potential utility of the general threat modelling framework by providing an initial system-of-systems scenario.

Clusters A, C and B focus on the main cyber threats and vulnerabilities toward ships. The other main cited papers focus on the potential economic consequences of cyberattacks (4.3.3) and on new computer-science methods that

propose a data-driven cyber security (3.3.4).

5.1.3. Economic consequences of cyberattacks

- Cluster D (Yellow): Economic consequences of cyberattacks

Cluster D clearly distinguishes from the others with an economic perspective of the potential losses of ship and port cyberattacks. As seen in the MAERSK ransomware on a port, port and ship cyberattacks are related among them. Park [47] studied the economic impact of a terrorist attack on Long Beach ports in Los Angeles (US) with a new supply-side National Interstate Economic Model (NIEMO) with political implications, notably the significant economic impacts among other states, finally it provides prevention measures. In the same vein, Rose [55]: developed an estimation of the total economic consequences of a seaport disruption (Beaumont and Port Arthur in Texas, US) factoring in the major types of resilience. She used a methodology with a combination of demand-driven and supply-driven input-output analyses. She showed that the gross regional output could decline by 13 billion dollars, but resilience can reduce these impacts by nearly 70%. Finally, Bou-Harb et al. [18] proposed a new approach to Cyber Physical systems (CPS) security in a coupled and a systematic manner that federates the cyber and physical environments to infer and attribute tangible CPS attacks. The methodology includes real cyber threat intelligence derived from empirical measurements and investigating CP data flows by devising an innovative CPS threat detector. The results present 3 case studies and remediation strategies. Last, DiRenzo [19] still stated that the vulnerabilities to cyberattacks of today's marine transportation system have not been well studied. This paper explored the vulnerabilities of shipboard systems, oil rigs, cargo and port operations.

5.1.4. Computer-science methods that propose a data-driven cyber security

- Cluster E (Purple): Data-driven cyber security

All the papers of Cluster E have in common to mobilize computer-science methods to propose a data-driven cyber security.

First, Polatidis [49] stated that existing attack graphs generation methods are inadequate to protect dynamic supply chain risk management environment as they do not integrate different important criteria (entry and target points, propagation length, location and capability of the attacker). This research proposed a new method using constraints and Depth-first search to effectively generate attack graphs with an application in a real maritime supply chain. Xiao [71] developed surveys the pattern mining with data collected from the maritime traffic safety management to constitute knowledge-based systems to improve traffic forecasting and safety. Liu [40]: highlighted that AIS data often suffers from undesirable outliers (i.e. poorly tracked timestamped points for vessel trajectories) during signal acquisition and analog-to-digital conversion. This data then had negative effects on VTS services such as maritime traffic monitoring, intelligent maritime navigation and vessel collision avoidance. This research proposed a two-phase data-driven machine learning framework to improve the quality of the AIS dataset. Finally, Munusamy [45] designed a blockchain-enabled edge-centric framework for analysing the real-time data at the edge of the networks with minimum latency and power consumption while meeting the security and privacy issue

of Maritime Transportation Systems (MTS).

As a conclusion, we can summaries these clusters in four main themes: 1) Technological (Clusters A and C) with a main focus on the AIS technology; 2) Human role in cyber security and resilience with a main focus on lack or ill-adapted training; 3) Economic consequences of cyber-attacks and threats; 4) Research methods with a focus on emerging data-driven methods. In the paragraph below, we complete this bibliometric analysis with a summary of the most recent papers in each theme and add additional emerging themes and concepts of research.

5.2. Maritime ships cyber security: what are the most recent remaining challenges to increase ships' resilience?

Based on the most recent papers that provide a literature review ships cyberattacks and risks, we have summarized below the main technological, human, economic and research method gaps that yet appeared in the clusters of the bibliometric analysis. This will allow us to present other themes highlighted in most recent papers. In addition, we have added themes and concepts that come from organization and management science that we believe can add value added to future research.

Table 2: Most recent themes related to ships' cyber risks and resilience and suggested concepts of interest

Related clusters from CCA (Fig. 6) and new themes	Themes	Topics and references with an assessment of their level of use in research papers. [Classified to their level of development in research papers: * Still under developed, ** Developed regularly, *** Classical approaches]
A	Technological	Infrastructure and dedicated networks*** [43],[33], Infrastructure connecting IT and OT systems both in the bridge and the base station* [43], security of the information onboard **[43], specific research for Maritime Autonomous Surface Ship (MASS) * [3],[4],[9],[43], design of technical solutions** [17], engine devices*[13], digital transformation* [44], data challenges** [1], IOT-enabled cybersecurity* [10], [28], blockchain* [25], encrypt AIS* [27], cyber physical systems [31], cyber-attacks detection** [38], deep learning* [37]
B	Human	Human talent* [43], impact of social networks on crew's behavior with GNSS*[43], training** [17], [33], navigator knowledge to interpret cyber threat [21]
C	Economic	Weaver et al., [69] done on ports but not on ships; few assessments* [1]

	consequences	
D	Data-driven cyber security and others methods, models and frameworks	Platform to detect cyber-attacks* [43], build a platform* [1], machine learning* [7]
Other	Organizational	Strategic Communications* [43]; Risk Management and evaluation (mostly derived from industry) and need to be tailored to maritime* [43], maritime security culture* [43], cyber preparedness* [70], cyber surveillance of devices** [70], reporting systems* [21], cyber resilience training* [22]
Other	Strategic	Maritime security governance* [43], [21], hackers profiles beyond NIST SP 800-30* [13]
Other	Ecosystem	Cybernetic attack scenarios** [43], build resilient navigation supply chains* [1], ship to ship and ship to shore [63]
	Legal	Regulation* [5], [17], [43], evaluation of policies and standards* [1], [43], Insurance *frameworks [17],
	Transversal to these themes	Cyber resilience* [17], digital resilience*[26], cyber resistance* [17], communication systems** [13], evolving and dynamic issues of cyber security* [1], smart shipping** [8], cybersecurity guidelines for resilience [20], complex adaptive systems [34],[35]

In the most recent papers, the main research frameworks are related to computer-science and risk management but have a less emphasis on human and organizational issues that can be tackle at different units of analysis (team, organization, ecosystem. Table 2 suggests to pursue the research in human and economic consequences which are from far the less developed in comparison to technological papers. In addition, it provides further attention on new themes such as the organization, the strategic choices and the legal aspects.

6. Conclusion

We develop the following research question: What do ships' cyber-attacks represent and what are the main

challenges to increase its digital resilience? The consequences of ships cyberattacks and threats have been so far mainly technical with sometimes huge economic consequences. In the future, these attacks may potentially have larger impacts such as a whole supply chain blockage worldwide with indirect human losses.

This paper provides an overview of the statistics regarding ships cyberattacks and an analysis of the literature review through two stages: firstly, a bibliometric analysis based on the most cited papers of WoS core collection database and secondly an analysis of the most recent papers in WoS and in Google Scholar.

In terms of importance of the phenomenon, the figures show that ships cyber-attacks are very frequent, most of them are targeting the AIS and the GNSS. Different types of ships cyberattack occurred but the most frequent ones are currently the ransomware and, spoofing and jamming attacks targeting AIS or GNSS systems [6], [24]. This is because they are two of the most vulnerable devices on ships. Recently, a higher number of ships' cyber-attacks are related to war contexts such as Ukraine in the Black Sea or Iran in the Red Sea.

In terms of research methodology for data collection, finding empirical data regarding ships' cyberattacks remains a challenge for several reasons: firstly, the main maritime databases are incomplete and do not include cyberattacks and cyberthreats in their key words (the ADMIRAL French database has recently been recognized as one of the most complete by the OMI); secondly, many maritime organizations keep the information confidential on their cyberattacks or threats for different reasons (time-consuming, reputation effect, strategical to better prevent future risks....). Regulation and some State members like France incite shipping companies to declare make a declaration if they have faced a cyberattack to the National Agency of Information Systems Security - Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) and to the CNIL Commission Nationale de l'Informatique et des Libertés) in case of data leak; in Europe, stakeholders that have lost data during a cyberattack or threat should initiate a declaration to the European Union Agency for Cybersecurity (ENISA) platform [d]. Finally, a dew recent cyber-attacks combined multiple sites, potentially located in different geographical areas. Hence, cyber security and resilience policies should not only consider ships per se but also all the stakeholders in the maritime ecosystem [67] with whom the ship is potentially in contact through its IT systems (main headquarters of maritime companies such as ship owners/classification societies/IT and electronic providers/insurances, fleet management centers, ports).

Hence, a cyberattack on a ship owner or in a port will have potential indirect consequences on ships at sea (i.e. blockage, data leak) and vice versa to a lesser extent. To improve our knowledge on ships' cyber resilience, we argue that we should develop further research on the human, organizational and ecosystem units of analysis while developing case studies [63] in collaboration with practitioners and the main maritime associations such as BIMCO, IACS. Finally, we will need to further study the shared decision-making between the sea and the shore with diversified research methods including computer data-driven and human social science qualitative approaches.

References

[d] https://www.enisa.europa.eu/publications/reinforcing-trust-and-security-platform Accessed 06 February 2024.

[1] Afenyo, Mawuli, and Livingstone D. Caesar (2023). "Maritime cybersecurity threats: Gaps and directions for future research." Ocean & Coastal Management 236: 106493.

[2] Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia, 45, 547-554.

[3] Amro, A., Gkioulos, V., & Katsikas, S. (2019). Connect and protect: Requirements for maritime autonomous surface ship in urban passenger transportation. In Computer Security: ESORICS 2019 International Workshops, CyberICPS, SECPRE, SPOSE, and ADIoT, Luxembourg City, Luxembourg, September 26–27, 2019 Revised Selected Papers 5 (pp. 69-85). Springer International Publishing.

[4] Amro, A., & Gkioulos, V. (2023). Cyber risk management for autonomous passenger ships using threat-informed defense-in-depth. International Journal of Information Security, 22(1), 249-288.

[5] Al Ali, N. A. R., Chebotareva, A. A., & Chebotarev, V. E. (2021). Cyber security in marine transport: opportunities and legal challenges. Pomorstvo, 35(2), 248-255.

[6] Al-Mhiqani, M. N., Ahmad, R., Yassin, W., Hassan, A., Abidin, Z. Z., Ali, N. S., & Abdulkareem, K. H. (2018). Cyber-security incidents: a review cases in cyber-physical systems. International Journal of Advanced Computer Science and Applications, 9(1).

[7] Algarni, A., Acarer, T., & Ahmad, Z. (2024). An Edge Computing-based Preventive Framework with Machine Learning-Integration for Anomaly Detection and Risk Management in Maritime Wireless Communications. IEEE Access.

[8] Alop, A. (2019). The main challenges and barriers to the successful “smart shipping”. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 13(3).

[9] Ahvenjärvi, S., Czarnowski, I., Kåla, J., Kyster, A., Meyer, I., Mogensen, J., & Szyman, P. (2019). Safe information exchange on board of the ship. TransNav: *International Journal on Marine Navigation and Safety of Sea Transportation*, 13(1).

[10] Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2022). A survey on cyber security threats in iot-enabled maritime industry. *IEEE Transactions on Intelligent Transportation Systems*, 24(2), 2677-2690.

[11] Awan, M. S. K., & Al Ghamdi, M. A. (2019). Understanding the vulnerabilities in digital components of an Integrated Bridge System (IBS). *Journal of Marine Science and Engineering*, 7(10), 350.

[12] Balduzzi, M., Pasta, A., & Wilhoit, K. (2014). A security evaluation of AIS automated identification system. In *Proceedings of the 30th annual computer security applications conference* (pp. 436-445).

[13] Ben Farah, Mohamed Amine, et al. (2022) "Cyber security in the maritime industry: A systematic survey of recent advances and future trends." *Information* 13.1: 22.

[14] BIMCO (2020), Chamber of Shipping of America et al.. The guidelines on cyber security onboard ships, Version 4.0.

[15] Bhatti, J., & Humphreys, T. E. (2017). Hostile control of ships via false GPS signals: Demonstration and detection. NAVIGATION: *Journal of the Institute of Navigation*, 64(1), 51-66.

[16] Bodeau, D. J., & McCollum, C. D. (2018). System-of-systems threat model. The Homeland Security Systems Engineering and Development Institute (HSSEDI) MITRE: Bedford, MA, USA.

[17] Bolbot, V., Kulkarni, K., Brunou, P., Banda, O. V., & Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. International

Journal of Critical Infrastructure Protection, 39, 100571.

[18] Bou-Harb, E., Kaisar, E. I., & Austin, M. (2017). On the impact of empirical attack models targeting marine transportation. 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS) (pp. 200-205). IEEE, June.

[19] DiRenzo, J., Goward, D. A., & Roberts, F. S. (2015). The little-known challenge of maritime cyber security. In 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA) (pp. 1-5). IEEE

[20] Drazovich, L., Brew, L., & Wetzel, S. (2021). Advancing the state of maritime cybersecurity guidelines to improve the resilience of the maritime transportation system. In 2021 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 503-509). IEEE.

[21] Erstad, E., Lund, M. S., & Ostnes, R. (2022). Navigating through cyber threats, a maritime navigator's experience.

[22] Erstad, E, Hopcraft R, Harish AV, Tam K. (2023) "A human-centred design approach for the development and conducting of maritime cyber resilience training." WMU Journal of Maritime Affairs 22.2 (2023): 241-266.

[23] Fenton, A. J. (2024). Preventing Catastrophic Cyber–Physical Attacks on the Global Maritime Transportation System: A Case Study of Hybrid Maritime Security in the Straits of Malacca and Singapore. Journal of Marine Science and Engineering, 12(3), 510.

[24] Filić, M. (2018). Foundations of GNSS spoofing detection and mitigation with distributed GNSS SDR receiver. TransNav: *International Journal on Marine Navigation and Safety of Sea Transportation*, 12(4).

[25] Gai, K., Tang, H., Li, G., Xie, T., Wang, S., Zhu, L., & Choo, K. K. R. (2022). Blockchain-based privacy-preserving positioning data sharing for IoT-enabled maritime transportation systems. IEEE Transactions on Intelligent Transportation Systems, 24(2), 2344-2358.

[26] Godé, C., & Pascal, A. (2021). La résilience digitale : une notion à explorer. Management et Datascience, 5(5).

[27] Goudossis, A., & Katsikas, S. K. (2019). Towards a secure automatic identification system (AIS*). Journal of Marine Science and Technology*, 24, 410-423.

[28] Gyamfi, E., Ansere, J. A., Kamal, M., Tariq, M., & Jurcut, A. (2022). An adaptive network security system for iot-enabled maritime transportation. *IEEE Transactions on Intelligent Transportation Systems*, 24(2), 2538-2547.

[29] Hemminghaus, C., Bauer, J., & Padilla, E. (2021). BRAT: A BRidge Attack Tool for cyber security assessments of maritime systems. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 15.

[30] Jacq, O. (2021). Détection, analyse contextuelle et visualisation de cyber-attaques en temps réel: élaboration de la Cyber Situational Awareness du monde maritime (Doctoral dissertation, Ecole nationale supérieure Mines-Télécom Atlantique Bretagne Pays de la Loire).

[31] Kampourakis, V., Gkioulos, V., & Katsikas, S. (2023). A systematic literature review on wireless security testbeds in the cyber-physical realm. Computers & Security, 103383.

[32] Karahalios, H. (2020). Appraisal of a Ship's Cybersecurity efficiency: the case of piracy. Journal of Transportation Security, 13(3), 179-201.

[33] Kessler, G. C. (2021). The can bus in the maritime environment–technical overview and cybersecurity

vulnerabilities. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 15.

[34] Koola, P. M. (2018). Cybersecurity: a deep dive into the abyss. Marine Technology Society Journal, 52(5), 31-43.

[35] Koshevyy, V., & Shishkin, O. (2019). Standardization of interface for VHF, MF/HF communication using DSC within Itsintegration with INS in the framework of e-navigation concept. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 13(3), 593-596.

[36] Kovacs, A., Van Looy, B., & Cassiman, B. (2015), « Exploring the scope of open innovation: a bibliometric review of a decade of research », Scientometrics, 104(3), 951-983.

[37] Kumar, P., Gupta, G. P., Tripathi, R., Garg, S., & Hassan, M. M. (2021). DLTIF: Deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems. IEEE Transactions on Intelligent Transportation Systems, 24(2), 2472-2481.

[38] Hu, J., Qi, L., Zhang, Z., Wang, H., Li, X., & Terry Yang, X. (2021). A Cyber-Attack Detection in Vehicle-to-Infrastructure Communication Based on LSTM Network. In CICTP 2021 (pp. 1200-1207).

[39] Li, X., Shang, S., Liu, S., Gu, K., Jan, M. A., Zhang, X., & Khan, F. (2022). An identity-based data integrity auditing scheme for cloud-based maritime transportation systems. *IEEE Transactions on Intelligent Transportation Systems*, 24(2), 2556-2567.

[40] Liu, R. W., Nie, J., Garg, S., Xiong, Z., Zhang, Y., & Hossain, M. S. (2020). Data-driven trajectory quality improvement for promoting intelligent vessel traffic services in 6G-enabled maritime IoT systems. IEEE Internet of Things Journal, 8(7), 5374-5385.

[41] Liu, W., Xu, X., Wu, L., Qi, L., Jolfaei, A., Ding, W., & Khosravi, M. R. (2022). Intrusion detection for maritime transportation systems with batch federated aggregation. IEEE Transactions on Intelligent Transportation Systems, 24(2), 2503-2514.

[42] Mahmood, K., Ferzund, J., Saleem, M. A., Shamshad, S., Das, A. K., & Park, Y. (2022). A provably secure mobile user authentication scheme for big data collection in IoT-enabled maritime intelligent transportation system. IEEE Transactions on Intelligent Transportation Systems, 24(2), 2411-2421.

[43] Martínez, F., Enrique Sànchez, L., Santos-Olmo A., Rosado D. G., Fernàndez-Medina E. (2024) "Maritime cybersecurity: protecting digital seas." International Journal of Information Security: 1-29.

[44] Melnyk, O., Onyshchenko, S., Onyschchenko, O., Lohinov, O., Ocherentna, V. (2023) "Integral approach to vulnerability assessment of ship's critical equipment and systems." Transactions on Maritime Science 12.01 (2023): 3-3.

[45] Munusamy, A., Adhikari, M., Khan, M. A., Menon, V. G., Srirama, S. N., Alex, L. T., & Khosravi, M. R. (2021). Edge-centric secure service provisioning in IoT-enabled maritime transportation systems. IEEE Transactions on Intelligent Transportation Systems.

[46] Oruc, A., Kavallieratos, G., Gkioulos, V., & Katsikas, S. (2024). Cyber Risk Assessment for SHips (CRASH).

[47] Park, J. (2008). The economic impacts of dirty bomb attacks on the Los Angeles and Long Beach ports: Applying the supply-driven NIEMO (National Interstate Economic Model). Journal of Homeland Security and Emergency Management, 5(1).

[48] Pirbhulal, S., Gkioulos, V., & Katsikas, S. (2021). A Systematic Literature Review on RAMS analysis for critical infrastructures protection. International Journal of Critical Infrastructure Protection, 33, 100427.

[49] Polatidis, N., Pavlidis, M., & Mouratidis, H. (2018). Cyber-attack path discovery in a dynamic supply chain maritime risk management system. Computer Standards & Interfaces, 56, 74-82.

[50] Pöyhönen, J., & Lehto, M. (2020). Cyber security: Trust based architecture in the management of an organization security. In ECCWS 2019: proceedings of the 18th European conference on cyber warfare and security (pp. 304-313).

[51] Pöyhönen, J., & Lehto, M. (2022, March). Assessment of cybersecurity risks-Maritime automated piloting process. In The proceedings of the 17th International Conference on Cyber Warfare and Security. State University of New York at Albany Albany, New York USA (pp. 262-271).

[52] Pöyhönen, J., & Lehto, M. (2023). Comprehensive cyber security for port and harbor ecosystems. Frontiers in Computer Science, 5.

[53] Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. Proceedings of the IEEE, 104(6), 1258-1270.

[54] Rohan, R. (2023, February). Identifying Commonalities of Cyberattacks Against the Maritime Transportation System. In International Conference on Cyber Warfare and Security (Vol. 18, No. 1, pp. 497-503).

[55] Rose, A., & Wei, D. (2013). Estimating the economic consequences of a port shutdown: the special role of resilience. Economic Systems Research, 25(2), 212-232.

[56] Schauer, S., Polemi, N., & Mouratidis, H. (2019). MITIGATE: a dynamic supply chain cyber risk assessment methodology. Journal of Transportation Security, 12(1), 1-35.

[57] Shipunov, I. S., Nyrkov, A. P., Ryabenkov, M. U., Morozova, E. V., & Goloskokov, K. P. (2021, January). Investigation of computer incidents as an important component in the security of maritime transportation. In 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus) (pp. 657-660). IEEE.

[58] Svilicic, B., Rudan, I., Jugović, A., & Zec, D. (2019). A study on cyber security threats in a shipboard integrated navigational system. Journal of marine science and engineering, 7(10), 364.

[59] Svilicic, B., Kristić, M., Žuškin, S., & Brčić, D. (2020). Paperless ship navigation: cyber security weaknesses. Journal of Transportation Security, 13, 203-214.

[60] Simola, J., Pöyhönen, J., & Martti, L. (2023). Cyber Threat Analysis in Smart Terminal Systems. In The Proceedings of the... International Conference on Cyber Warfare and Security. Academic Conferences International Ltd.

[61] Tam, K., & Jones, K. (2019a). MaCRA: A model-based framework for maritime cyber-risk assessment. WMU Journal of Maritime Affairs, 18, 129-163.

[62] Tam, K., & Jones, K. (2019b). Factors affecting cyber risk in maritime. In 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA) (pp. 1-8). IEEE.

[63] Tam, K., Hopcraft, R., Moara-Nkwe, K., Misas, J. P., Andrews, W., Harish, A. V., Giménez, P., Crichton, T., Jones, K. (2021). Case study of a cyber-physical attack affecting port and ship operational safety, Journal of Transportation Technologies, 2022, 12, 1-27.

[64] Thai, V. V., & Grewal, D. (2007). The maritime security management system: Perceptions of the international shipping community. Maritime Economics & Logistics, 9, 119-137.

[65] Uflaz, E., Sezer, S. I., Tunçel, A. L., Aydin, M., Akyuz, E., & Arslan, O. (2024). Quantifying potential

cyber-attack risks in maritime transportation under Dempster–Shafer theory FMECA and rule-based Bayesian network modelling. Reliability Engineering & System Safety, 243, 109825.

[66] Van Eck, N., Waltman, L. (2010), « Software survey: VOSviewer, a computer program for bibliometric mapping », Scientometrics, 84(2), 523–538.

[67] Watson, R. T., Haraldson, S., Lind, M., Rygh, T., Singh, S., Thomas, D., ... & Ward, R. (2021). FOUNDATIONS OF MARITIME INFORMATICS. In *2021 World of Shipping Portugal. An International Research Conference on Maritime Affairs 28-29 January 2021, Online Conference, from Portugal to the World*.

[68] Weaver, G. A., & Marla, L. (2018). Cyber-physical simulation and optimal mitigation for shipping port operations. In 2018 Winter Simulation Conference (WSC) (pp. 2747-2758). IEEE.

[69] Weaver, G. A., Feddersen, B., Marla, L., Wei, D., Rose, A., & Van Moer, M. (2022). Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach. Transportation Research Part C: Emerging Technologies, 137, 103423.

[70] Yu, Hongchu, et al. (2023), "Literature review on maritime cybersecurity: state-of-the-art." The Journal of Navigation (2023): 1-14.

[71] Xiao, Z., Fu, X., Zhang, L., & Goh, R. S. M. (2019). Traffic pattern mining and forecasting technologies in maritime traffic service networks: A comprehensive survey. IEEE Transactions on Intelligent Transportation Systems, 21(5), 1796-1825.

[72] Zăgan, R., Raicu, G., Hanzu-Pazara, R., & Enache, S. (2018, June). Realities in maritime domain regarding cyber security concept. In Advanced Engineering Forum (Vol. 27, pp. 221-228). Trans Tech Publications Ltd.

[73] Zhao, R., Yang, L. T., Liu, D., Deng, X., Tang, X., & Garg, S. (2024). Tensor-Based Secure Truthful Incentive Mechanism for Mobile Crowdsourcing in IoT-Enabled Maritime Transportation Systems. IEEE Transactions on Intelligent Transportation Systems.

[74] Zhao, Y., Liu, Z., & Wong, W. S. (2021). Resilient platoon control of vehicular cyber physical systems under DoS attacks and multiple disturbances. IEEE Transactions on Intelligent Transportation Systems, 23(8), 10945-10956.

[75] Zhang, Q., Li, S., Wu, B., & Wang, J. (2020). Passive maritime surveillance based on low earth orbit satellite constellations. IEEE Wireless Communications, 27(6), 61-67.

[76] Zhou, X. Y., Liu, Z. J., Wang, F. W., & Wu, Z. L. (2021). A system-theoretic approach to safety and security co-analysis of autonomous ships. Ocean Engineering, 222, 108569.

[77] Zupic, I., Cater, T. (2015) "Bibliometric methods in management and organization." Organizational Research Methods 18.3 (2015): 429–472.