A bibliometric analysis of cyber security in maritime ports

Abstract:
Cyber security of ports constitutes a hot topic with increased vulnerabilities in digitalization. Surprisingly, the main focus in literature is on maritime transportation cyber attacks, and little is known about ports' cyber attacks from human and organizational perspectives. With a bibliometric analysis based on Web Of Science, we described the main themes developed by each cluster's top five cited papers. We completed the anaysis with a systematic literature review based on Web Of Science and Scopus databases.

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

1. Introduction

Brazil (7,491Km) and France (4,853Km) are both countries with large coasts with major ports that contribute to transport more than 80% of goods worldwide. In a context of increased digitalisation, ports' cyber attacks constitute a hot topic with potentially drastic economic losses and supply chain blockages. Ports are extremely important elements for a country's economy, as they are the main entry and exit points for foreign trade. Ports connect ocean-side or sea-side transport conducted by ships, to land-side movements connected by road, rail, and sometimes, air. Thus ports are facilities with a combination of multi-modal transfers and movements. A variety of commodities are transported in shipping containers, including non-perishables like apparel and cars as well as perishables such as produce and food items. To facilitate the movement of commodities from the port to other downstream destinations in the commodity supply chain, ports themselves contain multi-modal transportation terminals, storage terminals,

several container yards, storage areas, and a network of roads to facilitate movements within the port to external areas. Each of these assets inside the port is operated by various stakeholders. For example, a port itself is operated by the county or an owning company, its storage terminals are operated by contracting companies, the transportation terminals are operated by transportation companies or public organizations, and trucks to move containers are operated by drayage companies. All these organizations are stakeholders who have a keen interest in ensuring efficient port operations and minimizing the impact of disruptions.

Nowadays, ships and maritime infrastructure are becoming increasingly interconnected as the maritime industry is undergoing the Industry 4.0 revolution. The increased digitalisation, ports' cyber attacks constitute a hot topic with potentially drastic economic losses and supply chain blockages. This development is associated with novel risk types such as the increased potential for successful cyberattacks. Several review studies have investigated the regulatory framework concerning maritime cybersecurity, the vulnerabilities in maritime systems, potential cyberattack scenarios, and risk assessment techniques (Bolbot et al., 2022). At the same time, attackers have seen in these systems an opportunity to penetrate critical systems and affect their security. These attacks targeting digital systems, also known as cyberattacks, are more and more numerous. With the increased number of cyber-attacks and improved regulation, little is still known about the role of humans and how maritime organisations can better prevent and/or mitigate ports' cyber risks.

We develop the two following research questions: (RQ1) What do ports' cyber attacks represent and what are the main challenges in terms of cyber resilience highlighted by the most co-cited papers of the literature?; (RQ2) - What are the main challenges in terms of cyber resilience highlighted by the systematic literature review and what research agenda can we build on them?

2. Cybersecurity in maritime transportation

2.1 Statistics

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[1] (Jacq, 2021) 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.

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.

In this subsection, we analyse 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.

[1] Admiral database is available online on: https://gitlab.com/m-cert/admiral/ Accessed 20th January 2025.

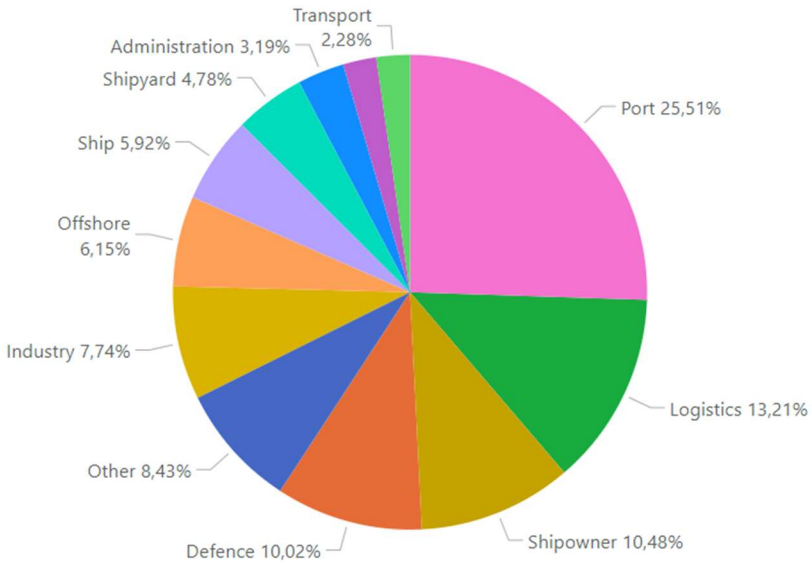

Figure 1: Type of cyberattacks in maritime sector per target types

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 allows seeing that cyberattacks targeting shipowners, ports and logistics represent nearly half of the total. If we only focus on ports and logistics organisations that are generally close to ports, they represent 38,72% of all maritime cyber-attacks. 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.

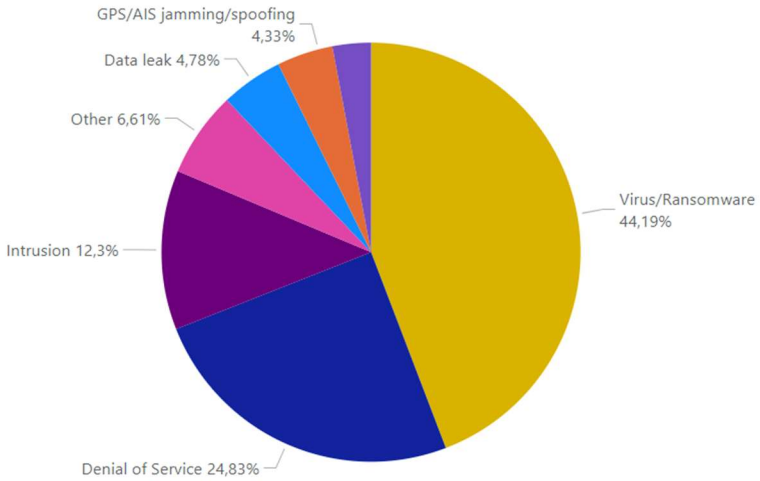

Figure 2: Type of cyber-attacks in maritime sector

Figure 3 presents the distribution of listed cyberattacks by type. The most common used attacks are Denial of Service (DoS) that compromise the availability of servers (70%). These types of attacks exploit different vulnerabilities to access and compromise IT and OT systems. Secondly, ports suffer from viruses and ransomwares (20,69%). In the case of ransomware, attackers demand a ransom to the organization to recover the normal functioning of their systems. Thirdly, ports have to face intrusion and data leak: attacks with similar objectives that are often related to economic or industrial spying interests. Finally, a growing stance of attacks even thought hey are still limited are spear phishing. These attacks play on human trust to access and/or damage the data of ports' information systems.

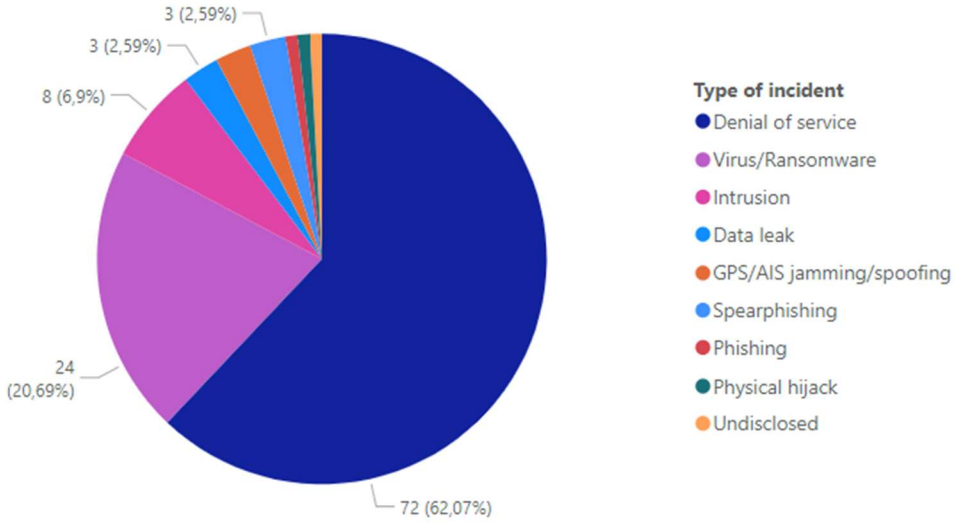

Figure 3: Type of cyber-attacks in ports

As we can appreciate in Figure 5, the number of cyberattacks the maritime sector is relatively low. This is due to the fact that all attacks are not publicly declared. Moreover, 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.

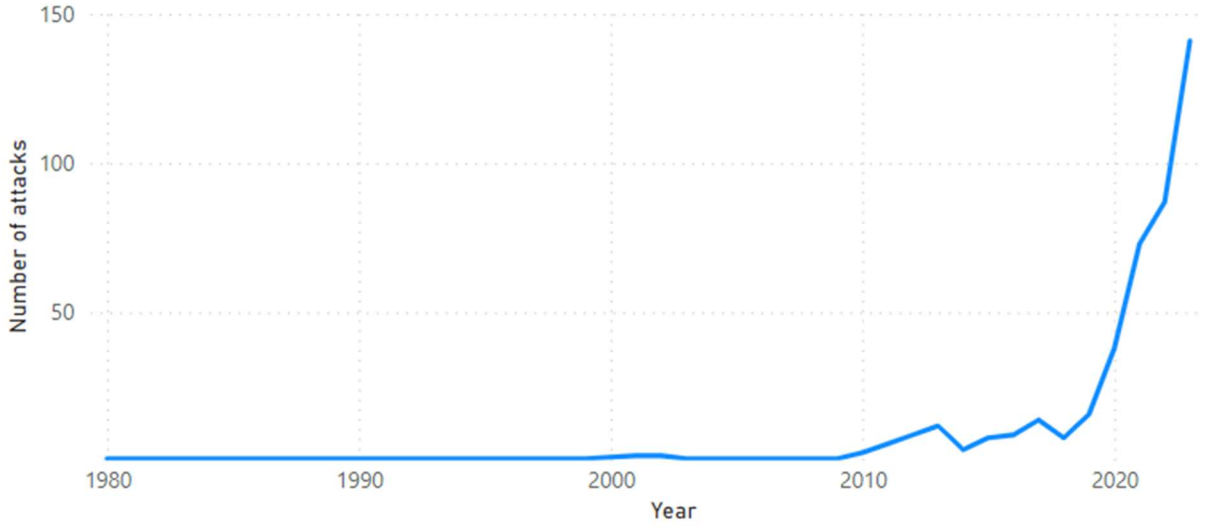

Figure 4: Number of cyberattacks in maritime sector per year

Each month ports are attacked. However, the information is not always publicly shared.

All this data and statistical analysis let us conclude that maritime cyberattacks have in general big economic consequences as major worldwide supply chain blockages including the ship fleet (Maersk, 2017) as well as the whole ecosystem of logistics organisations that are based close to ports. These attacks prove that cybersecurity is not only a technological challenge but also, they require new procedures for human organization and management.

2.2 Cyber risks and resilience on ports illustrarted by recent cases

Smart port 4.0 are characterised by their digitalisation which has drastically increased cyber risks. There are four main stakeholders that are directly concerned by cyber-attacks onshore and between ship-and-shore (Meland et al., 2020): (1) the port authorities and class (ship and crew certifications, class documents, arrival clearance); (2) the private operators (yard equipment, ship services, operators); (3) the public infrastructure (information to ships, Vessel Traffic Services, or VHF radio) and; (4) port operations (communication in port, port operation systems - POS, Cargo data systems and Port Community Systems, services to ship). A key point to further tackle cyber risks is related to the increasing information systems integration among these stakeholders which leads to augmented inter dependence and shared risks.

There are several types of cyber threats such as exposed IT systems of the different stakeholders based or in communication with ports such as sub-contractors, shipyards, on-shore installations,

services providers, regulators and research facilities. Ship companies nearly represent a quarter of targeted organisations. On port, exposed port IT systems, espionage on maritime operations. An interesting point is related to the increasing inter-dependency between ships and ports: by targeting for instance the headquarters of a shipping company, a whole fleet of ships can be disconnected from their communication capabilities.

Recent research on cybersecurity in ports highlights the increasing vulnerability of digitalized port operations to cyber threats. Studies have identified various dimensions of port cybersecurity hygiene, including human, infrastructure, and procedural factors (Chalermpong, 2021). Weaknesses in these areas can lead to different types of cyber attacks, such as hacktivism, cyber criminality, and cyber espionage. To address these risks, researchers propose integrated cyber risk assessment frameworks that consider both cyber and physical assets of ports (Gunes et al., 2021). These frameworks aim to evaluate and mitigate potential cyber threats through proactive measures. Additionally, advanced simulation tools are being developed to analyze security problems and identify gaps in marine port environments (Longo, 2012). The growing focus on security operations reflects the need to balance efficiency, cost-effectiveness, and security in transportation processes (Zhao et al., 2017).

Over the past five years, several notable cyberattacks have targeted port infrastructures worldwide. While specific details of each incident may be limited due to security and confidentiality concerns, the following cases have been documented in peer-reviewed scientific literature:

1. **Port of Barcelona Cyberattack (2018):** In September 2018, the Port of Barcelona experienced a cyberattack that affected several of its servers. Although specific details were not extensively disclosed, the port authority acknowledged the incident and warned of potential operational delays during the recovery process. (Bocayuva, 2021)
2. **Port of San Diego Ransomware Attack (2018):** Shortly after the Barcelona incident, the Port of San Diego suffered a ransomware attack that disrupted its IT systems. The port reported that the attack impacted its public services and business operations, leading to a temporary shutdown of certain systems to prevent further spread. (Bocayuva, 2021)
3. **APM Terminals Cyberattack (2017):** APM Terminals, a subsidiary of Maersk, was significantly impacted by the NotPetya malware in June 2017. The attack led to the shutdown of terminal operations across various locations, including major European

ports. The company estimated financial losses between $200 and $300 million due to the disruption. (Bocayuva, 2021)

4. **Port of Antwerp Cyberattack (2011-2013):** Between 2011 and 2013, the Port of Antwerp was targeted by hackers hired by a drug trafficking organization. The attackers infiltrated the port's IT systems to access secure data, facilitating the smuggling of illicit goods. The breach remained undetected for an extended period, highlighting vulnerabilities in port cybersecurity. (Bocayuva, 2021)
5. **Port of Lisbon Cyberattack (2022):** In 2022, the Port of Lisbon suffered a cyberattack claimed by the LockBit ransomware group. The attack affected the port's website and some internal systems, leading to temporary disruptions. The port authority worked to restore normal operations while investigating the breach. (Senarak, 2023)
6. **South African Ports Cyberattack (2021):** In July 2021, Transnet, the state-owned company operating South Africa's ports, experienced a significant cyberattack. The incident led to the declaration of a "force majeure" at major ports, causing substantial delays and operational challenges. The attack highlighted the critical importance of cybersecurity in port operations. (Senarak, 2023)
7. **Port of Nagoya Cyberattack (2023):** Japan's largest port, Nagoya, was hit by a suspected ransomware attack in 2023. The incident disrupted container operations, leading to delays in cargo handling and transportation. The port authority took measures to contain the attack and restore affected systems. (Senarak, 2023)
8. **Port of Houston Cybersecurity Breach (2021):** In 2021, the Port of Houston detected a cybersecurity breach attributed to a suspected nation-state actor. While the port reported that operations were not significantly impacted, the incident underscored the ongoing cyber threats facing critical maritime infrastructure. (Senarak, 2023)
9. **Port of Kennewick Cyberattack (2020):** The Port of Kennewick in Washington State confirmed a cyberattack in 2020 that affected its administrative systems. The port worked with cybersecurity experts to assess the breach and implement measures to prevent future incidents. (Senarak, 2023)
10. **Port of Shahid Rajaee Cyberattack (2020):** In 2020, Iran's Shahid Rajaee port experienced a cyberattack that disrupted its operations. Reports suggested that the attack caused significant delays in the port's activities, highlighting the vulnerabilities of maritime infrastructure to cyber threats. (Senarak, 2023)

These incidents illustrate the increasing frequency and sophistication of cyberattacks targeting port infrastructures globally. They underscore the critical need for robust cybersecurity countermeasures and continuous monitoring to protect maritime operations from evolving cyber threats.

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 3.

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

We developed a bibliometric review on ship cyber-attacks and threats with the software VosViewer (Van Eck, Waltman, 2010). A key benefit of bibliometric methods is their ability to help reduce reviewers' subjectivity and bias, which are inherent in conventional qualitative reviews (Zupic and Cater, 2015). We followed the four-step procedure as outlined by Kovacs et al. (2015). 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 » and "topics", with the key words "« cyber security » and « maritime ports » or "ports" cybersecurity OR cyber* OR "information security" and port* OR terminal* OR smartport* and maritime. We limited our search on "articles" or "review article" in terms of document types. which led to a set of 54 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 45 articles that constitute the historical main 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.

3.3 Systematic literature review:

The review methodology of this article was based on Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) (Liberati et al, 2009), which is a structured method for conducting a systematic literature review. There are numerous other literature review techniques (Booth et al., 2021), but we preferred PRISMA as it is a widely used, systematic, and easy-to-follow approach (Moher et al, 2009). The information flow based on the PRISMA methodology is provided in Fig. 1, and the steps are elaborated in the subsequent sections. In the same figure, we also present the number of identified and finally selected publications.

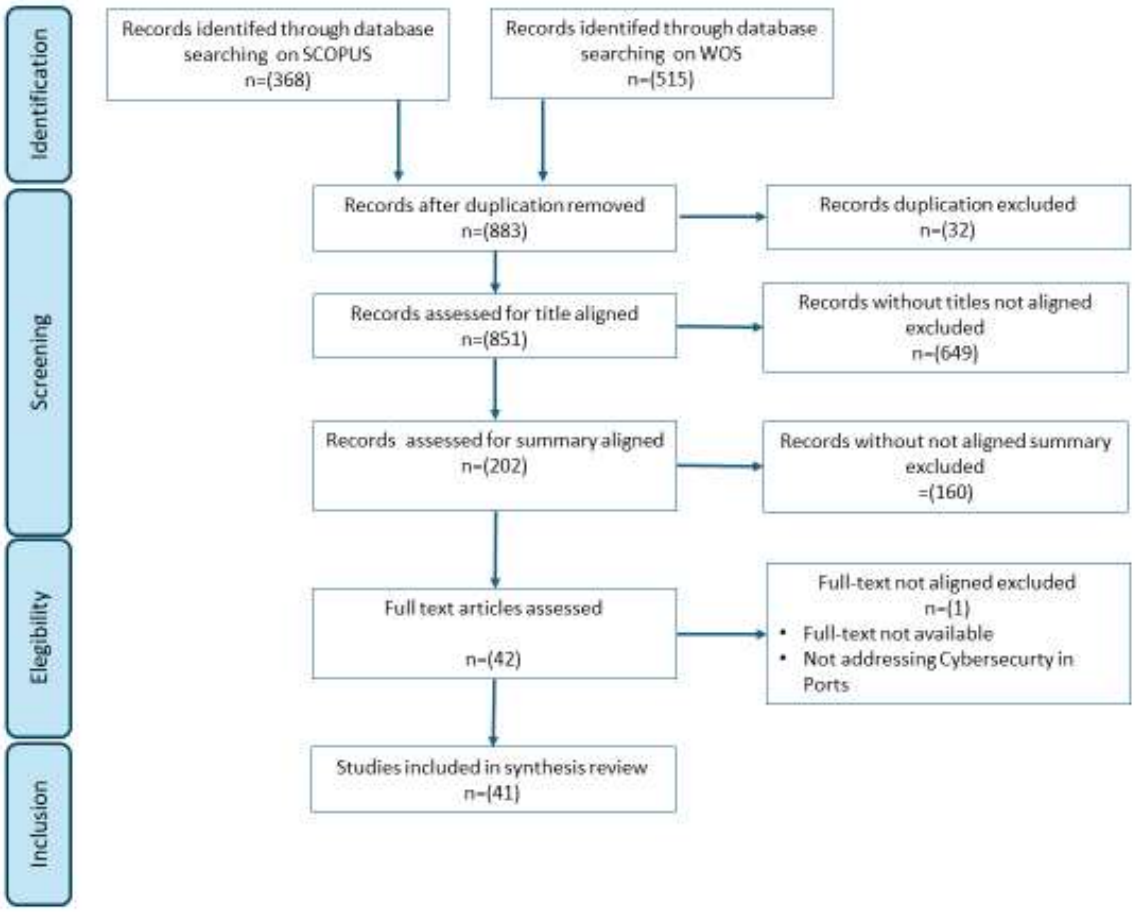

Fig.5 PRISMA process

We used three research axes for defining concept groups and using Boolean operators effectively, summarized in Table 1.

Portfolio Selection		
Theme: Cybersecurity in Ports		
Definitions of Axes and Key-words		
1. Cybersecurity	2. Ports	3. Maritime
Cybersecurity cyber security information security data security	Port seaport harbor smart port marine terminal container port	Maritime shipping marine naval Ship Vessel maritime logistics
Databases		
Scopus and Web of Science		
Search string		
("cybersecurity" OR "cyber security" OR "information security" OR "data security" OR "network security" OR "digital securit AND ("port" OR "seaport" OR "harbor" OR "terminal" OR "cargo" OR "smart port" OR "marine terminal" OR "container por ("maritime" OR "shipping" OR "marine" OR "naval" OR "ship" OR "vessel" OR "maritime logistics")		
Inclusion and Exclusion Criteria		
Inclusion:1) No time restrictions; 2) Selected "Journal Articles" and "Literature Reviews"; 3) Categories like Computer Scienc Studies, and Transportation; 4) English language only; 5) Selection based on title, abstract, and keywords; 6) No restriction o Articles not addressing Cybersecurity in Ports. **Exclusion**:1) Books, book chapters, conference papers; 2) Articles not published in peer-reviewed scientific journals; 3) Artic English;4) Selection not based on title, abstract, and keywords; 5) Articles not addressing Cybersecurity in Ports.		
Basis of Articles	Scopus	We
	383	
	883	

Table 2 Bibliography Portfolio Selection

4. Results:

4.1 The five main themes of the literature review presented with the bibliometric analysis

While the statistics are presented in 2.1, we firstly present the bibliometric analysis in 4.1 and then the systematic literature review and research agenda in 4.2.

Fig 6. shows the bibliographic map of five clusters based on CCA. We made the interpretation of these clusters based on the top-five 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-five most cited articles).

Cluster	*Label*	*Number of articles*	*Top 5 most-cited articles*
A (Red)	Cyber Resilience risks of smart port 4.0	13	Zarzuelo et al. (2020) ; Gunes (2021) ; Kalogeraki (2020) ; Aslam (2020) ; Boyes (2016)
B (Green)	Frameworks and methods to improve maritime cyber resilience	13	Tam and Jones (2019); Polatidis et al. (2018); Svilicic et al. (2019a); Jensen (2015); Svilicic et al. (2019b)
C (Blue)	Human role toward cyber critical infrastructure	8	Androjna (2020); Senarak (2021); Tam and Jones (2018); Zarzuelo (2021); Alcaide (2020)
D (Yellow)	Data-driven cyber security	8	Balduzzi et al. (2014); Alessandrini et al. (2016); Huang et al. (2018); Pallotta et al. (2013); Ray et al. (2015)
E (Purple)	Ship resilience and its relationships with ports	3	Hemminghaus et al. (2021); Apkan et al. (2022); Bolbot et al. (2020)

Table 3 Indicators of references output and citation impact cited by 54 articles included in the dataset; core of 45 articles that constitute the CCA with a threshold of 3 co-cited articles

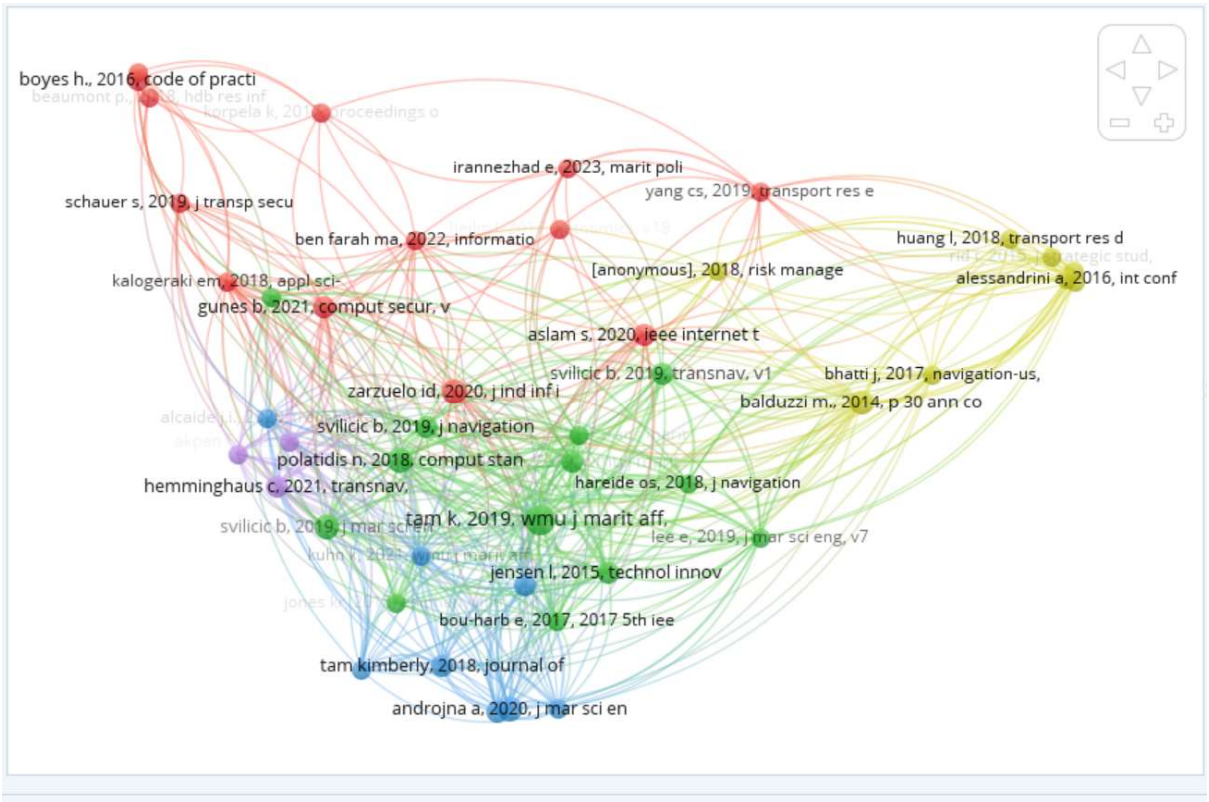

Fig.6 CCA of ports' cyber attacks and resilience

In the overall map of CCA, there are two central clusters that dominate the field (Clusters A and Cluster B) that set up the landscape of the new cyber risks in smart port 4.0 and then propose a few frameworks and methods to increase resilience. At the bottom, Clusters D and E propose mainly data-driven and mathematical methods to increase resilience. Conversely, Cluster C which little developed in the literature, highlights the main role of human in increasing the cyber resilience of critical infrastructure such as ports.

Cluster A (Red): Cyber risks and resilience in smart port 4.0

This cluster gathers the most cited papers of the whole CCA, historically the most influential papers in ports' cyber security and resilience, by order of importance: Zarzuelo et al. (2020) depicts the evolution of ports into four stages (loading and unloading port, indutrial ports, logistic ports, smart ports 4.0) and highlights the socio-technical challenges that ports are facing to move from isolated to integrated resolutions from the three main domains of ports (the seaside, the yard and transport systems and the landside and crane and gate optmisations). In the context of digitalisation the authors enhance more cooperatoin among all the stakeholders of ports. Gunes et al. (2020) and Kalogeraki et al. (2018) provide a complete model of cyber risk assessment to apply in each port. Among all information technologies, the Internet of Things (IoT) is highlighted as a powerful one to improve optimisation, safety and security

prevent owing to maritime data management and analytics. In response to this increased digitalisation, several papers provide guides and practical recommendations to professionals including a cyber security assessment and security plan (Boyes et al., 2020).

*Cluster B (Green):*Frameworks and methods to improve maritime cyber resilience

All the papers of Cluster B have in common to suggest frameworks and methods to improve cyber resilience. Jensen (2015) provided a visionary paper on the growing cyber risks in a maritime industry. This industry is composed of several stakeholders with different levels of maturity regarding cyber risks which are highly connected to other stakeholders but with limited – or no – control over more "remote" parts of the landscape. As building a standard in maritime cyber resilience will take years with the help of the IMO, he recommended a practical approach by adopting local guidelines for maritime companies, an increasing role of insurance policies with "cyber premiums" and the help of national goverments to identify maps of main cyber risks, methods or frameworks to increase resilience and recommendations.

The most co-cited papers developed methods applied to ships. For instance, Tam and Jones (2019) proposed the MaCRA framework which is a simulation to quantify and prioritise cyber risks in maritime. The MaCRA framework inputs data on system vulnerabilities, potential outcomes, as well as attacker abilities and target defences. It then outputs graphical or numerical risk profiles that can be customised to the analyst to answer specific or broad maritime-cyber risk queries. Connecting MaCRA to the proposed lab would increase the framework's risk profile details, and help prioritize threat-mitigation research when analysing Cyber-SHIP bridge configurations. Other data-driven methods have been developed such as Polatidis et al. (2018). They 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. Finally others methods used ship maritime simulators that could lately inspire ports. The most cited papers are Svilicic et al (2019a) who investigated ship integrated navigation systems (INS). This is a software platform for fusion of data from the major radar and ECDIS systems (Electronic Chart Display and Information Systems) that need to be protected from cyber threats according to the International Safety Management (ISM) code updated by the IMO. In the same path, Svilicic et al. (2019b) proposed an innovative simulation to test cyber resilience on the ship simulator of a maritime school by establishing both cyber security management systems with bridge IT systems. It provided an assessment process directly applicable to all ships.

*Cluster C (Blue):*Human role toward cyber critical infrastructure

Ports are on of the central critical infrastructure towards cyber risks. Zarzuelo (2021) provided a very interesting overview of these infrastructures by raising awareness due to the high level of integration of different devices, agents and activities, together with an increasing connectivity between different ports has created a new ecosystem in which new risks have appeared. NIST Standards defining a common framework for cybersecurity based on five pillars (Identify – Protect – Detect – Respond – Recover), some authors (BIMCO, 2017; Polemi, 2017; Beaumont, 2018) have identified the following requirements for the port industry: i) identify vulnerabilities, barriers and gaps in security standards at ports and in the entire supply chain, ii) identify port threat scenarios and analyze the potential cascading effects in their supply

chains, iii) assess risk exposure, iv) define self-protection and detection measures implementing preventive tools, v) carry out a periodic updating and auditing of the cyber-protection tools and vi) develop contingent and recovery plans from cybersecurity incidents. Zarzuelo (2021) is one of the few authors recalling the importance of the human factor in protecting these critical infrastructures. Androjna (2020) explored the cyber challenges in maritime navigation and the human role in preventing attacks by rising wareness in attacks such as jamming qnd spoofing. IN the same path, Senarak (2021 provided models for prevention and policy developments according to different cyber threat categories.

Cluster D (Yellow): Data-driven cyber security

All the papers of Cluster D have in common have in common to mobilise computer-science methods to propose a data-driven cyber security. For instance, Huang (2018) proposed a multi source maritime information model to estimate ship emissions. Morevover, based on the AIS data vessel pattern discovery framework and on anomaly detection and route prediction by following the data ship movements, Pallotta (2013) built a methodlogy called Thread (Traffic Route Extraction and Anomaly Detection).

Cluster E (Purple): Ship resilience and its relationships with ports

It can be surprising to see a cluster dedicated to ship cyber resilience. However, in a context of increased inter-dependencies between ships and the shore, a cyber attack on ships could directly damage the shore and vice versa. The high permeability among the IT and OT systems (Operating Technology, also called engine systems) on ships (well-illustrated on the Fig. 1 of Apkan (2022) and on Bolbot (2020)) and on shore explain that part of the core seminal co-cited papers were dedicated to ships. For instance, Hemminghaus et al. (2021) developed a bridge attack tool for cyber security assessment of maritime systems for integrated bridge systems.

4.2 Proposition of a research agenda based on the systematic literature review

To systematically address the critical challenges facing cybersecurity in ports, a research agenda has been developed based on a systematic literature review. The agenda is structured into nine thematic categories, each representing a key domain where further investigation is essential (Table 2). These categories include advanced risk assessment methodologies, enhanced threat detection systems, human factors and training, infrastructure protection, supply

chain cybersecurity, regulation and policy, incident response, cyber-physical security and the adoption of cyber security standards. For each category, specific research items have been identified and linked with relevant scholarly sources. Table 2 that follows provides a structured overview of these priority areas, offering a roadmap to strengthen port cyber security

category	item	references
1. Advanced Risk Assessment and Management	Develop and refine risk assessment methodologies specifically designed to handle the inherent uncertainty in cybersecurity data within the maritime domain.	Mohsendokht et al., 2024
	Research the adaptation and improvement of conventional risk analysis techniques (e.g., HAZOP, FMEA) to better address cyber threats.	Mohsendokht et al., 2024
	Develop holistic risk assessment frameworks that comprehensively account for the interdependencies between IT and OT systems in ports.	Weaver et al., 2022; Gunes et al., 2021
	Investigate quantitative methods for describing and assessing port vulnerability, particularly from a maritime supply chain perspective, and explore standardization across different ports.	Mohsendokht et al., 2024; Jiang et al., 2021
	Create dynamic risk analysis frameworks that can adapt to evolving threat landscapes and technological advancements.	Harish et al., 2025
	Explore the application of advanced techniques like data-driven Bayesian Networks (BNs) integrated with real-time data and machine learning for enhanced risk prediction and analysis in maritime infrastructures, including ports.	Mohsendokht et al., 2024
	Develop methodologies for assessing the economic losses resulting from cyberattacks on ports, considering operational effects on transportation networks.	Weaver et al., 2022
	Research the integration of cyber risk assessment with existing port facility security assessments under the ISPS Code.	Gunes et al., 2021
2. Enhanced Threat Detection and Prevention	Investigate and implement advanced threat detection systems utilizing AI and machine learning for real-time monitoring of network activities and identification of unusual behavior indicative of cyberattacks.	Mohsendokht et al., 2024; Peng et al., 2025; Dimakopoulou & Rantos, 2024

Table 4 Nine main themes from the systematic literature review and items for a research agenda

Conclusion

This paper provides an overview of the statistics regarding ports' cyberattacks and an analysis of the literature review through two stages: firstly a few statistics that are quite sensitive to find and secondly a bibliometric analysis based on the most cited papers of WoS core collection database.

In terms of research methodology for data collection, finding empirical data regarding ports' 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 recognised as one of the most complete by the IMO); secondly, many maritime organisations 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 ports 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. 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 ports per se but also all the stakeholders in the maritime ecosystem with whom the port 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, ships).

To complete this literature review, we present a ssytematic literature review baed on PRISMA methodology that provide the nine main future challenges on which we build our research agenda.

References

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

Alessandrini, A., Alvarez, M., Greidanus, H., Gammieri, V., Arguedas, V. F., Mazzarella, F., ... & Vespe, M. (2016, December). Mining vessel tracking data for maritime domain applications. In 2016 IEEE 16th International Conference on Data Mining Workshops (ICDMW) (pp. 361-367). IEEE.

Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. Journal of Marine Science and Engineering, 8(10), 776.

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. Network, 2(1), 123-138.

Aslam, S., Michaelides, M. P., & Herodotou, H. (2020). Internet of ships: A survey on architectures, emerging applications, and challenges. IEEE Internet of Things journal, 7(10), 9714-9727.

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

Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems. Safety science, 131, 104908.

Boyes H., Isbell R., Luck A. (2020), Cyber security for ports and port systems – good practice guide, The Institution of Engineering and Technology, Department of transport, UK.

De la Peña Zarzuelo, I., Soeane, M. J. F., & Bermúdez, B. L. (2020). Industry 4.0 in the port and maritime industry: A literature review. Journal of Industrial Information Integration, 20, 100173.

De la Peña Zarzuelo, I. (2021). Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue. Transport Policy, 100, 1-4.

Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. Computers & Security, 103, 102196.

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.

Huang, L., Wen, Y., Geng, X., Zhou, C., & Xiao, C. (2018). Integrating multi-source maritime information to estimate ship exhaust emissions under wind, wave and current conditions. Transportation Research Part D: Transport and Environment, 59, 148-159.

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).

Jensen, L. (2015). Challenges in maritime cyber-resilience. Technology Innovation Management Review, 5(4), 35.

Kalogeraki, E. M., Papastergiou, S., Mouratidis, H., & Polemi, N. (2018). A novel risk assessment methodology for SCADA maritime logistics environments. Applied Sciences, 8(9), 1477.

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.

Meland, P. H., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents.

Pallotta, G., Vespe, M., & Bryan, K. (2013). Vessel pattern knowledge discovery from AIS data: A framework for anomaly detection and route prediction. Entropy, 15(6), 2218-2245.

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.

Ray, C., Gallen, R., Iphar, C., Napoli, A., & Bouju, A. (2015, May). DeAIS project: Detection of AIS spoofing and resulting risks. In OCEANS 2015-Genova (pp. 1-6). IEEE.

Senarak, C. (2021). Port cybersecurity and threat: A structural model for prevention and policy development. The Asian Journal of Shipping and Logistics, 37(1), 20-36.

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

Svilicic, B., Kamahara, J., Rooks, M., & Yano, Y. (2019b). Maritime cyber risk management: An experimental ship assessment. The Journal of Navigation, 72(5), 1108-1120.

Tam, K., & Jones, K. D. (2018). Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. Journal of Cyber Policy, 3(2), 147-164.

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