2021-11-23

Maritime Cyber Security: A Global Challenge Tackled through Distinct Regional Approaches

Karamperidis, Stavros

10.3390/jmse9121323
Journal of Marine Science and Engineering
MDPI

Journal of *Marine Science and Engineering*

MDPI

Article

Maritime Cyber Security: A Global Challenge Tackled through Distinct Regional Approaches

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

[1] Department of International Shipping, Logistics and Operations, University of Plymouth, Plymouth PL4 8AA, UK
[2] Warwick Manufacturing Group, University of Warwick, Coventry CV4 7AL, UK; chronis.kapalidis.1@warwick.ac.uk (C.K.); tw@warwick.ac.uk (T.W.)
[3] Information Security Forum (ISF), London EC3M 1AJ, UK
* Correspondence: stavros.karamperidis@plymouth.ac.uk

Abstract: Maritime cyber security is an emerging issue that requires immediate attention, according to the International Maritime Organization (IMO). Feedback received from global shipping professionals indicate that a common threat to the industry, such as cyber security, is dealt with differently among industry practitioners around the globe. Data collected from two targeted focus groups (one in Europe and the second in Asia, two leading groups in the maritime transport sector) demonstrated that, based on technology adoption maturity, cyber security is perceived differently between these groups. The COVID-19 pandemic has highlighted these differences. Our findings lead to useful intelligence that will inform key maritime decision makers, both in meeting the IMO requirements and preparing the organization to address cyber risks.

Keywords: maritime cyber security; cultural differences; maritime transport sector

Citation: Karamperidis, S.; Kapalidis, C.; Watson, T. Maritime Cyber Security: A Global Challenge Tackled through Distinct Regional Approaches. *J. Mar. Sci. Eng.* **2021**, *9*, 1323. https://doi.org/10.3390/jmse9121323

Academic Editor: Claudio Ferrari

Received: 10 July 2021
Accepted: 18 November 2021
Published: 23 November 2021

1. Introduction

Innovative technologies have found their way to the maritime transport sector as they minimize the costs and maximize the benefits in everyday operations. At the same time, these new technologies enhance the interconnectedness of core port and shipping operations to the whole supply chain. As such, any interruption to the core of these operations may have a consequent knock-on effect to the wider economy and industries related to the supply chain, as illustrated in the CyRiM Report [1].

Despite the increasing numbers of cyber incidents to corporate networks and data, the maritime transport sector is rather slow in addressing cyber risk [2]. Well-established regulations and guidelines have been implemented for decades on topics such as environmental and crew safety and, more recently, on ballast water management; these risks are tangible. However, cyber risks are different. Their intangible nature means that their consequences are not palpable; therefore, it is difficult for them to be initially identified and addressed. Infected applications, computers in the office, or operational technology (OT) systems on board may continue to operate without any noticeable performance issues. Unlike any other risk, when a cyber breach occurs, it can affect the entire infrastructure of an organization, including its fleet and offices around the world.

This threat landscape will only grow, as ships at sea increase their connectivity, exchanging data so they can increase supply chain visibility and performance. Unfortunately, while connectivity solutions have evolved, achieving greater resilience, a single specific vulnerability in one industry or organization can swiftly cascade to affect other industries and organizations due to the lack of appropriate security controls [1].

Maritime transport companies are part of a complex supply chain that, at present, is digitalized. Digitalization is taking place so that performance in the overall supply chain can be improved [3]. At the same time, shipping companies are providing remote access

to on-board systems to third party service providers and vendors for software updates, performance monitoring, and maintenance [4]. These two intertwined activities increase the cyber-attack surface. It is not a farfetched scenario in which a critical cloud service provider or even a satellite communications services provider could be interrupted or ceased altogether because of a cyber breach. Such incidents could cascade on a global scale and impact all economic activities. The most profound example is the NotPetya malware attack in July 2017, which had a huge impact on global economic activities, costing approximately $892.5 million [5]. Research institutes and regulatory authorities are struggling to model, let alone quantify, cyber risk, mainly due to the lack of relevant data. When the threats move at the speed of light, they can be hard to comprehend.

In other leading industries, such as banking, manufacturing, retail, and healthcare, boards of directors and executive leadership are gradually becoming more aware of the cyber threat to their businesses and the need to manage cyber security at the enterprise level. A 2020 survey conducted by the Information Systems Audit and Control Association (ISACA) [6] found that 82% of respondents understood the board of directors to be "concerned" or "very concerned" about cyber security. Similarly, in shipping, as our research identified and demonstrates in Figures 1 and 2, more than 90% of experts consider cyber security to be either very or somewhat important for their working environment. However, this concern does not always align with how board members allocate resources to tackle cyber risk. Hence, security professionals are tasked to address this emerging threat without the necessary tools in place [7].

Even though the industry is cognizant of the importance of cyber security, confusion persists about how serious the cyber threat actually is, the risks that it poses to their enterprises, and the prioritization it demands. Going beyond the technical interpretation of cyber security, this paper aims to tackle the following research aim: *Identify how cultural differences affect the level of understanding on maritime cyber security*.

It should be highlighted that the paper is constructed based on the data extracted during two high-profile industry workshops. Members of the research team were invited to present in these two workshops. As such, an opportunity arose to put together a set of questions to be shared with the participants to extract valuable data from experts with deep knowledge of the maritime transport sector. Due to that restriction, the research environment was not fully controlled by the research team. Research was not conducted in the typical academic way, but it was a great opportunity to extract raw data and present it to an academic audience seeking rare true insight knowledge. Therefore, the research team extracted, analyzed, and present the findings in this paper, so they could provide rare evidence for an issue of paramount importance for the maritime transport sector. This paper makes a valuable contribution to current literature by focusing on outcomes extracted from experts and links them with existing literature.

Following the introduction, the related literature review on the key stakeholders involved in the maritime transport sector and the illustration of maritime cyber-crime importance for the sector is presented in Section 2. Section 3 describes the theory that supports the work conducted from the research team and shows how the data was collected through a survey. Outcomes of the survey are thoroughly discussed and presented in Section 4. Section 5 presents a conclusion and proposal for future research.

2. Literature Review

The adoption of new technologies in the global shipping sector, such as office and shipboard information technology (IT) systems, advanced supervisory control and data acquisition (SCADA) systems, and industrial control systems (ICS) enhance maritime operations that support 90% of world trade [8]. At the same time, these technologies, despite their benefits, introduce new vulnerabilities and threats to day-to-daily maritime transport operations. The rapid growth of technology-intense solutions in most cases does not take security into consideration [9]. In order to deliver transportation services to their customers, maritime transport stakeholders are now required to take cyber security

into consideration, as their customers expect them to operate in a secure, digitalized environment. Hence, it is critical for maritime stakeholders to rise to the challenge of the newly introduced cyber threat landscape in the maritime transport sector.

2.1. Maritime Transport Sector

The maritime transport sector consists of three main components: (1) mobile assets, (2) infrastructure, and (3) financial activities. Specifically mobile assets include: ships and auxiliary platforms. Infrastructure often described as maritime critical infrastructure includes: port infrastructure, offshore energy infrastructure, safety and security controls, navigation aids, communication systems (onshore, offshore, satellite), underwater cables, and pipelines. Finally, financial activities include: insurance agencies and vendors, booking/charter agencies, and banking-economic transactions [10].

Raising awareness is a challenge in the maritime transport sector, as senior maritime transport stakeholders are struggling to understand the changing risk environment. Identifying how cyber threats are affecting their organizations and allocating the necessary resources to address this is not straightforward. Staff engaged with cyber security are struggling to provide concrete evidence regarding the return on investment (ROI) for cyber security measures. This is becoming more difficult due to the abstract nature of cyber threats. Unlike piracy or extreme weather conditions, the consequences of a cyber breach are not always visible.

Safety and security at sea has paramount importance for shipping, a sector with a good safety and security record of accomplishment. Cyber security has been identified as a key part for maintaining safety and security for ships and port operations. Managing cyber threats, according to the Maritime Security Strategy [11] and the related Action Plan of The European Union (EU), is integral to achieving maritime transport security. NATO acknowledged the importance of the maritime cyber security back in October 2016, when it organized the first dedicated maritime cyber conference at the NATO Maritime Interdiction Operations Training Centre (NMIOTC) in Crete [12]. A key initiative aiming to contribute to the better understanding of cyber risk is the International Maritime Organization (IMO) guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3) and the consequent IMO resolution MSC 428(98) (July 2017) on maritime cyber risk management in safety management systems [13,14]. The latter document suggests that, as of 1 January 2021, all stakeholders engaged in the industry should demonstrate cyber capability.

As cyber risk management is now a requirement of the IMO, it would be expected that all maritime transport stakeholders should take similar actions in meeting this requirement and, consequently, address cyber risk within their operating environment. This is not the case, though. Maritime transport stakeholders around the world adopt a different posture to the issue. One key reason for this is that the origin of each individual reflects their level of understanding of a specific topic, including cyber security, as demonstrated in Section 3. Specifically, the maritime transport sector is multinational in nature as several stakeholders from various countries are involved. Typically, a ship may be registered in a particular flag state but may have a crew of many nationalities, none of whom may be from that country. The owners may be from different countries and the vessel operator may be from yet another country.

2.2. Flag States

Flag states are national authorities representing the respective country responsible for establishing and overseeing the regulatory regime governing ship operations within that country's registry. Flag states operate their registries according to their domestic laws and regulations while complying with a set of international codes [15].

The predominant regulatory entity issuing such codes is the IMO. The IMO is a specialized agency of the United Nations with the authority to regulate maritime affairs, including international shipping, port safety, and security. Most flag states transpose the IMO-generated international requirements in their national legislation.

However, the most popular flag states are considered "open registries" or "flags of convenience" that do not require a meaningful economic or financial tie to the country of registry [16]. One of the attractions of open registries is their lower fee structure related to registering and complying with the flag state's requirements. They are also less stringent in their staffing requirements and allow for the hiring of cheaper labor. Ships registered under these schemes are, in general, considered "lightly regulated", although some of them are well managed and highly reputable.

In the wake of the IMO's decision to incorporate cyber risk management under the International Safety Management (ISM) Code, a very small number of flag states have started addressing cyber risk management requirements. An apt example is the USA, where the US Coast Guard [17] issued the Navigation and Vessel Inspection Circular No. 01-20 "Guidelines for addressing cyber risk at maritime transportation security act (MTSA) regulated facilities", providing specific guidance for the incorporation of cyber risks in safety management systems. Because cyber risks represent a current, clear, and persistent threat to the maritime transport sector, overall, shipping companies are strongly encouraged to go above and beyond the compliance requirements and lay the foundations for comprehensive cyber security strategy and plans as early as possible.

2.3. Classification Societies

Classification societies are private, not-for-profit organizations that provide quality assurance to the maritime transport sector. The International Association of Classification Societies (IACS) is the prominent organization where most classification societies are members. While these societies were historically based in and focused on certain countries and markets, they have gradually increased their global representation. Furthermore, those societies organically grow in countries by establishing offices there and have also followed the merger and acquisition approach in which two classification societies merge and grow. The most prominent example is the merge of Norwegian DNV (Det Norske Veritas) with the German classification society (Germanischer Lloyd) to form a multinational classification society [18]. There is a large number of additional classification societies that function similarly.

In line with the IMO resolution regarding cyber risk management, classification societies have started to introduce detailed guidelines, assessing the cyber security posture of ships and shipping companies. For example, DNV, ClassNK, and ABS have developed relevant cyber security guidelines [19–21]. At the same time, classification societies are responsible for auditing ISM code implementation, which now includes cyber security.

2.4. Maritime Cyber Crime

Having looked at the structure of the maritime transport sector and briefly examined its response to the IMO cyber regulation, it is important to understand how the sector's transition to the digital era can, at the same time, introduce cyber related risks. To illustrate, one cyber threat campaign, referred to by researchers as the Daily Show, began as a phishing attack against the shipmaster of a tanker operator [22]. Since the initial infection, which involved key logger malware, the campaign spread around the world, affecting more than 50% of the IMO member nations, and infected not only unknown numbers of vessels and port facilities but also oil/gas, manufacturing, customs agencies, logistics companies, and banks.

As stated previously, maritime transport companies are constantly adopting new systems, platforms, and technologies to achieve greater levels of capability and efficiency, which introduces new risks to their operations. These risks range from email and IT-office environments to OT systems. The latter is the most important in shipping operations as it affects ships' seaworthiness [10]. It can be argued that, in the maritime transport sector specifically, cyber threats are becoming more frequent and sophisticated, as individual hackers, well-funded and organized criminal networks, nation states, and others target ports, shipping companies, vessels, and shore-side facilities. Predominantly, during the

COVID-19 pandemic, according to MTS-ISAC [23], an increase in cyber attacks in shipping took place, with some additional reporting from the Nautical Institute, demonstrating that this increase may have reached up to 900% [24].

Due to its nature, the cyber domain knows no boundaries. Cyber threat actors are less constrained by geography than connectivity. As shipping is increasingly reliant on connected technologies, every vessel, shore-based facility, and office represents a potential target. Vessels are particularly vulnerable to cyber threats, since ship operators (including management and third-party vendors) regularly access the vessel's networks and related operational systems, both physically and remotely. Unpatched operating systems on vessels with poorly configured networks, open serial ports, and legacy applications represent a considerable asymmetrical risk to shipping and land-based operations (ports, offices, and supply chains) [10].

The maritime transport industry has been slow to respond to the growing cyber threat [2,25]. However, this belated response is not granular throughout. The reasons for this anomaly are identified and analyzed in this paper.

3. Methodology

3.1. Theory That Supports Our Work

One of the main findings of the analysis relates to the perception of the topic of cyber security. This is evident throughout the responses collected for the various questions of the survey, as presented in Section 4. As such, the research team tried to identify a conceptual framework that justifies this approach. The most apt piece of academic work that closely aligns with this observation is the book by Nisbett [26], entitled: "*The geography of thought: How Asians and Westerners think differently . . . and why*". According to Nisbett [26], different cultures perceive specific topics in a different way. Specifically, and related to the composition of participants of this research, East Asian thought is "holistic", while Westerners focus on specific subjects. To elaborate, East Asians interpret specific subjects as part of the whole, examining the relations between objects and events within that discipline. Applying this concept to maritime cyber security, East Asians perceive cyber security as another risk factor, part of the overall aggregated risk affecting maritime transport operations. This argument is reinforced as it is demonstrated from the findings of this research, presented in Section 4. In contrary, the West approach emphasizes notable subjects aiming to tackle any challenges related to this through specific attribution. With Nisbett in mind, applying this concept to maritime cyber security, Western managers perceive cyber security as a standalone risk element to be dealt with by IT professionals. That demonstrates a clear differentiation between the mindsets and approaches that the maritime transport practitioners who participated in the two workshops (Asia and Western representatives) undertake when dealing with cyber security in the maritime transport sector.

Shipping is a truly global industry, as Kumar and Hoffmann [27] (p. 36) state: "*A Greek owned vessel, built in Korea, may be chartered to a Danish operator, who employs Philippine seafarers via a Cypriot crewing agent, is registered in Panama, insured in the UK, and transports German made cargo in the name of a Swiss freight forwarder from a Dutch port to Argentina, through terminals that are concessioned to port operators from Hong Kong and Australia*". As such, maritime transport stakeholders, irrespective of their physical location or their racial decent, should develop a common, fundamental mindset that could grasp the risk factor called cyber security. That is something difficult to achieve as the sector needs time to develop and adopt that common mindset. The first step towards that direction is for regulatory bodies to introduce relevant documentation, either mandatory or advisory. An apt example is the IMO, with its guidelines and consequent resolution on cyber risk management [13,14], as analyzed above.

3.2. Data Collection

A unique opportunity was offered to test the theory presented above through direct engagement with industry experts from Asia and Europe. Data for this paper was collected

by the authors during two industry-focused workshops. The workshops were designed for tackling issues related to cyber security in shipping; they were not designed for collecting academic research data. This was a limiting factor when trying to conduct further statistical analysis of the collected data, as the research team had no control over participants' demographics. However, as several key industry experts participated, it was a great opportunity to collect data for such a contemporary issue as the challenges posed by cyber threats in the maritime transport sector. Both events took place in December 2020, virtually, allowing for stakeholders, from a large number of countries, to participate. Data were collected with the use of an online tool; it was anonymized and securely stored. Each participant was able to submit one or multiple responses, as indicated in each question.

The first workshop was conducted by a large Chamber of Commerce based in East Asia. As aforementioned, data collection was conducted during the workshop and the questionnaire was designed and tested prior to that. However, the overall event was not purposely conducted for data collection; as such, data collected was a "by-product" of the workshop. Therefore, detailed statistics for the demographics of the respondents are missing. The research team only have information related to the overall number and country of origin of participants of the workshop. Additionally, during the workshop, a lively discussion with the participants took place, which indicated their willingness to share information with authors. During the workshop two authors were main speakers in the event.

The second workshop was conducted by a large shipping association based in Greece with representation throughout the EU. Unlike the previous workshop, one of the authors was the main speaker, presenting the same questionnaire during the session. Similar to the previous workshop, a lively discussion with the participants took place. Participants were willing to share additional information with us. Further information is demonstrated in the following section, where the survey is presented in detail.

Data from both workshops were analyzed instantly from the research team. The analysis was conducted on a regional level but also in combination, so that a better understanding of the overall responses of the maritime sector could be obtained. The findings are presented in Section 4. Prior to that, it is demonstrated in the following section how the survey was designed.

3.3. Survey

As was evident from the aforementioned literature review, cyber attacks in the maritime transport sector have increased substantially over the last decade. For that reason, the introductory question posed to participants of this survey aims at highlighting the importance of cyber security in daily operations for the maritime transport sector. Table 1 presents the list of questions used in the survey.

Apart from the initial question, which attempted to understand the importance of cyber security in the maritime transport sector, the questions composing the survey were grouped in two themes: (A) How the industry is coping with the new IMO 2021 regulation requirements; (B) how shipping companies experienced changes in daily operations due to COVID-19 from the spectrum of cyber security.

The survey was available for responses only during the presentations delivered by the research team, which helped the participants get a better understanding of each question. Additionally, clarification was provided, when needed, as a live Q + A session was available, assisting the submission of full questionnaires, as in some cases participants drop out from a survey or they leave some questions blank if they do not fully understand them.

This was a unique, impromptu, opportunity to examine experts, and as such, the survey did not collect participants demographics. Instead, an investigative lead approach was adopted. Participants represented the whole spectrum of the maritime transport sector (e.g., port operators, shipping companies, consultants, ship management companies, technology solution providers, and academics).

Table 1. Questions asked during the surveys.

	Questions
A	**How the industry is coping with the new IMO 2021 regulation requirements**
1	How important is information (cyber) security to your daily job and activities?
2	Which agency is more suitable to assist and guide the maritime transport sector in addressing cyber security?
3	Is the IMO 2021 Cyber regulation the answer to cyber security for shipping?
4	How prepared are shipping companies in meeting the IMO 2021 requirements and consequently addressing cyber security?(Difference in perception in what cyber security entails)
B	**How shipping companies experienced changes in daily operations due to COVID-19 from the spectrum of cyber security**
5	Has the COVID-19 pandemic affected the maritime cyber security landscape?
6	Have you experienced a surge in cyber attacks in your organization during the pandemic?
7	How effective have shipping companies been in adapting to the new norm due to the COVID-19 Pandemic?

Workshop 1: Up to 200 participants partially attended the event, while half of them (100) attended the entire event. Participants represented 30 countries.

Workshop 2: The total number of participants was 42, representing a total number of 15 European countries, whilst the majority of the participants were from Greece (a higher representation from Greece is considered as normal, due to the high representation of Greeks in the shipping sector).

The findings extracted during the two workshops are presented in the following section.

4. Findings and Discussion

This section presents the data collected, analyzes the findings, and discusses key points by linking them to the theoretical approach presented in Section 3.

Based on the responses of the introductory question, it became evident that there is a consensus between maritime professionals regarding the importance of cyber security in the maritime transport sector. Specifically, the research team examined the importance of information or cyber security in the daily maritime transport operations, both in Europe and in Asia, as demonstrated in Figure 1a,b. When European and Asian responses were combined, it was observed that more than 90% of experts considered cyber security to be either very or somewhat important for their working environment, as demonstrated in Figure 2. This evidence shows that cyber security is more relevant presently for the maritime transport sector.

As shipping is already a heavily regulated industry, where the compliance mindset remains predominant, the IMO introduced specific guidelines to address cyber security in shipping. The nature of these guidelines is at a rather high level without offering any specific insights on their implementation. As such, theme A of this survey aims to explore: How the industry is coping with the new IMO 2021 regulation requirements. Through this theme, a novel knowledge approach was introduced, which is needed for future policy guidance and clarifies any doubts in the long-run.

It was deemed necessary, for the first question, to identify the competent authority that could provide guidance and assistance on the implementation of the IMO requirements. As presented in the literature review, the maritime transport sector consists of several entities that play a specific role in its successful development over the last century. Classification societies, P&I clubs, governments, flag states, marine insurance, and regional and international organizations now have to understand their role in addressing cyber security in shipping. Unlike the consensus unveiled in the previous question, the responses collected from the two working groups for this question highlight a significant difference

regarding the competent authority for shipping. As demonstrated in Figure 3b, the majority of maritime transport professionals in Asia (53%) state that classification societies are the predominant authority, suitable to assist and guide the maritime transport sector in addressing cyber security, followed by governments with 27% and flag states with 10%. This perception is not shared with their colleagues in Europe, where the IMO, classification societies, and P&I clubs share equal representation (approximately 25%), as demonstrated in Figure 3a. At the same time, flag states seem to get similar percentages in both working groups. An aggregated response of both European and Asian is demonstrated in Figure 4. As both groups consider classification societies to be the authority to assist the maritime transport sector in tackling cyber security, it is therefore the highest scoring sector, with 40%, while the second most suitable organizations for tackling cyber security in maritime transport are governments, with 20%. Therefore, as demonstrated in Figure 4, classification societies have more "authority" than governments due to the multinational nature of shipping.

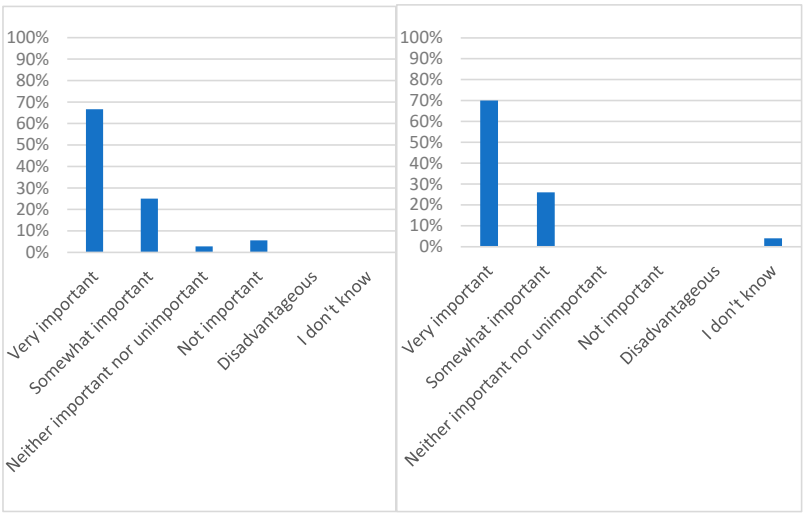


Figure 1. How important is information (cyber) security to your daily job and activities? (**a**) Europe; (**b**) Asia.

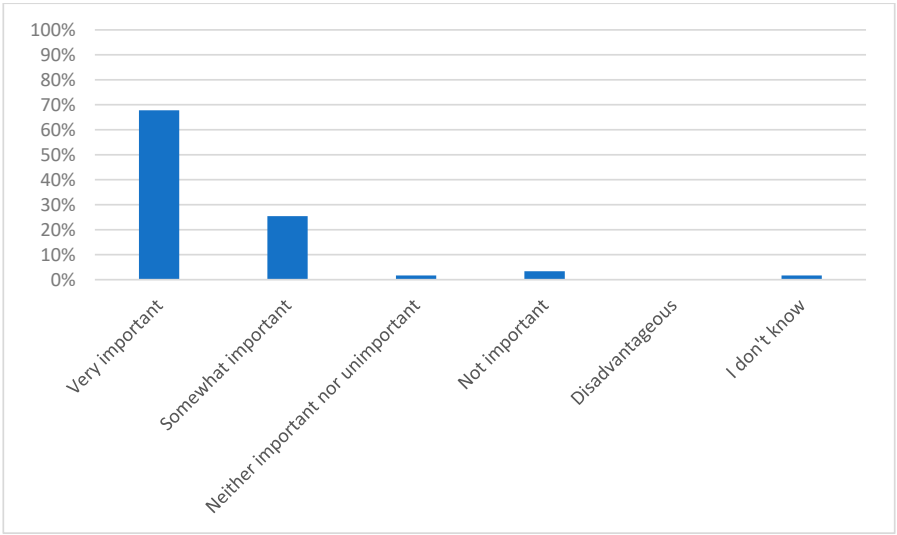
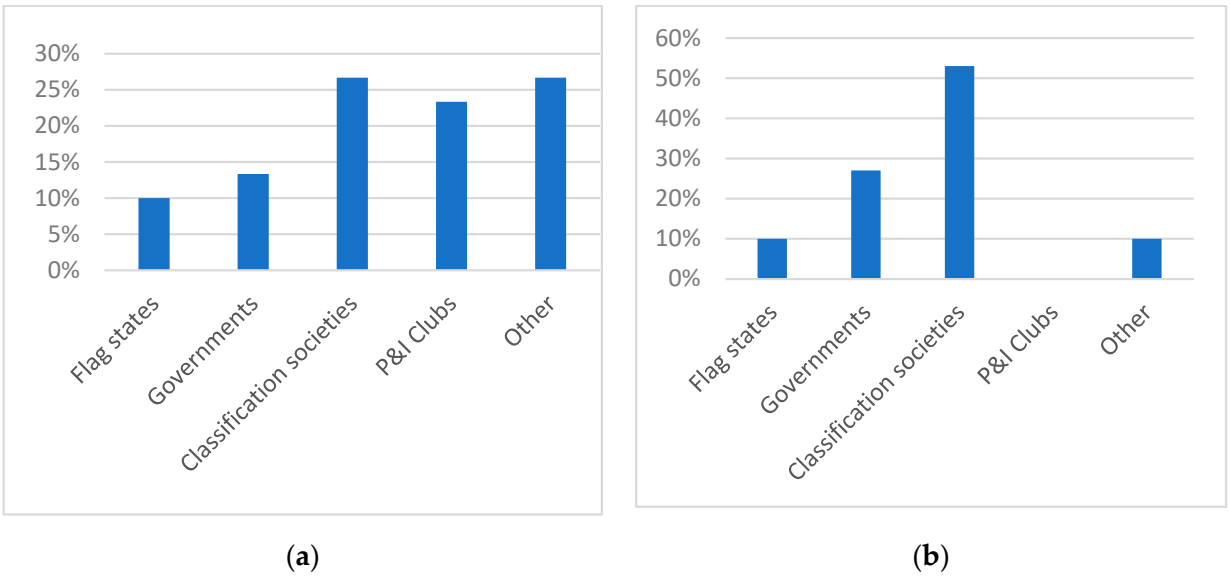


Figure 2. How important is information (cyber) security to your daily job and activities? (Asia and Europe).



(**a**) (**b**)

Figure 3. Which agency is more suitable to assist and guide the maritime transport sector in addressing cyber security? (**a**) Europe; (**b**) Asia.

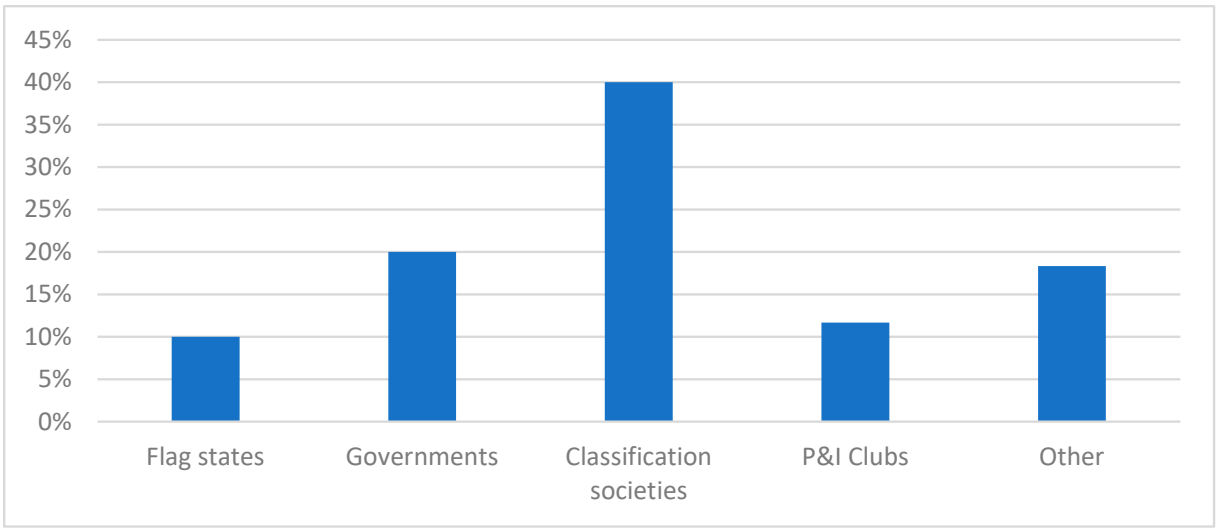


Figure 4. Which agency is more suitable to assist and guide the maritime transport sector in addressing cyber security? (Asia and Europe).

Aiming to understand the diversification between the responses in the two groups, examination of the broader picture should not be neglected. Going beyond cyber security, shipping professionals in Europe rely on the IMO's authority to regulate the industry. Similarly, P&I clubs, created by shipping professionals themselves, have a long-standing tradition in handling claims. On the contrary, classification societies are the de-facto entities that define responses to all, short of regulatory requirements in Asia. As such, cyber security would be no different.

Based on the findings of the previous questions, question 3 from Table 1 goes beyond the regulatory requirements and explores if the IMO resolution can effectively protect shipping from cyber breaches. As presented in the literature review, industry specific press has criticized the IMO cyber resolution as high level and not offering any tangible outcomes for its implementation, let alone specific steps for its inclusion in shipping companies' safety systems. Outcomes presented in Figure 5a,b are aggregated in Figure 6, and demonstrate findings regarding the IMO cyber resolution per region, Europe and Asia. The responses in Figure 6 are split, with half of the participants agreeing that the IMO 2021 cyber resolution

is the answer to cyber security for shipping and the other half either disagreeing or not being able to agree or disagree.

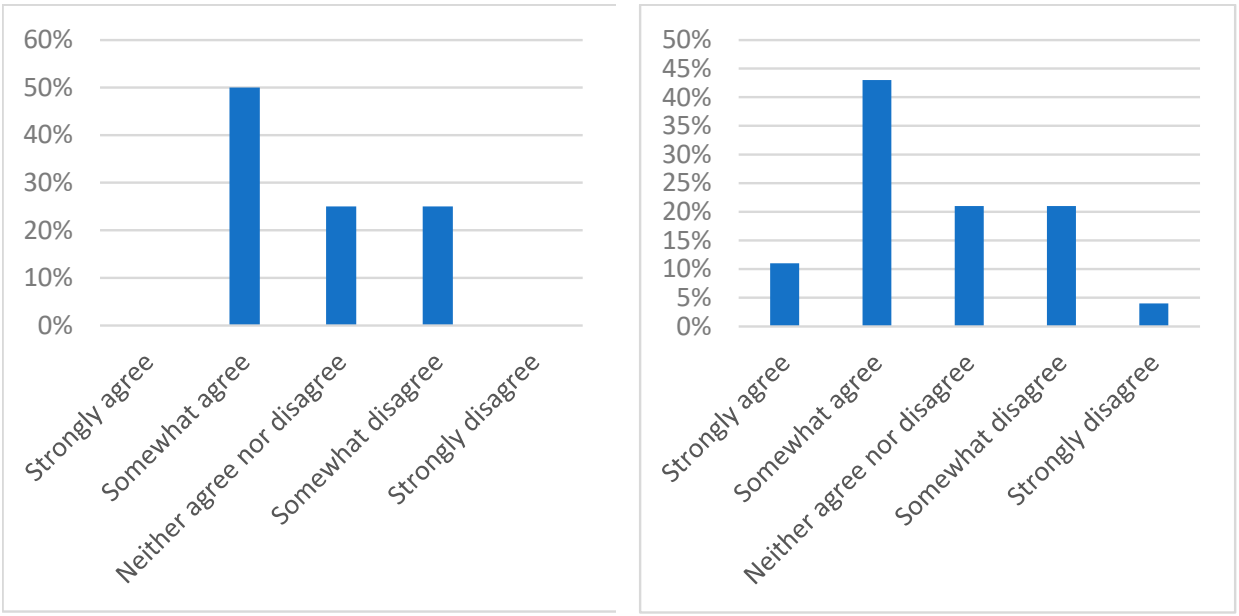


Figure 5. Is the IMO 2021 Cyber regulation the answer to cyber security for shipping? (**a**) Europe; (**b**) Asia.

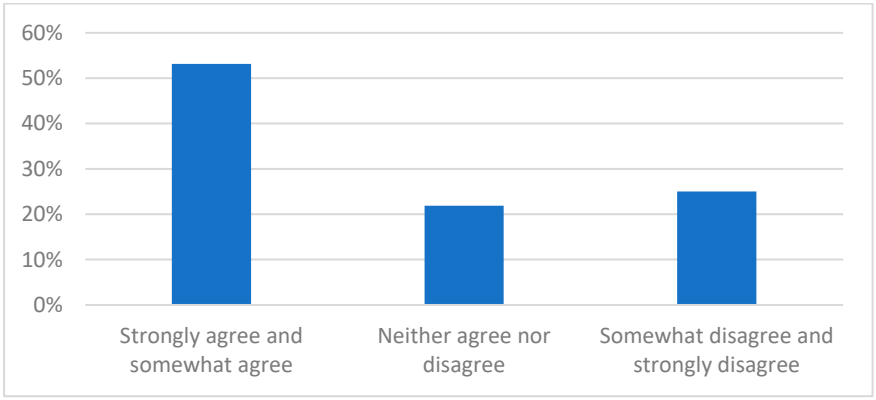


Figure 6. Is the IMO 2021 Cyber regulation the answer to cyber security for shipping? (Asia and Europe).

This split in the responses, which is similar for both the European and Asian participants of the survey, highlights the issue that the IMO 2021 cyber resolution, unlike other IMO guidelines, does not provide a clear answer to the sector's needs. For example, the ballast water management and sulfur cap regulations provide clear instructions on their applications, followed by technical specifications. As demonstrated from the findings of the survey, the IMO cyber resolution does not clearly pass the message required to the sector. The reason for that is because the IMO resolution is more descriptive rather than prescriptive.

Expanding on the previous question, the analysis explores the level of preparation for shipping companies when meeting the IMO 2021 resolution and, consequently, addressing cyber security. According to the practitioners who participated in the survey, and in contrast to the previous question, a difference between the responses in Europe and Asia was observed. While nearly half of the respondents in Europe believed that the sector is somewhat prepared (Figure 7a), a roughly similar percentage in Asia believed the opposite

(that the sector is somewhat unprepared, Figure 7b). This difference became evident when the results from Europe and Asia were combined, as demonstrated in Figure 8.

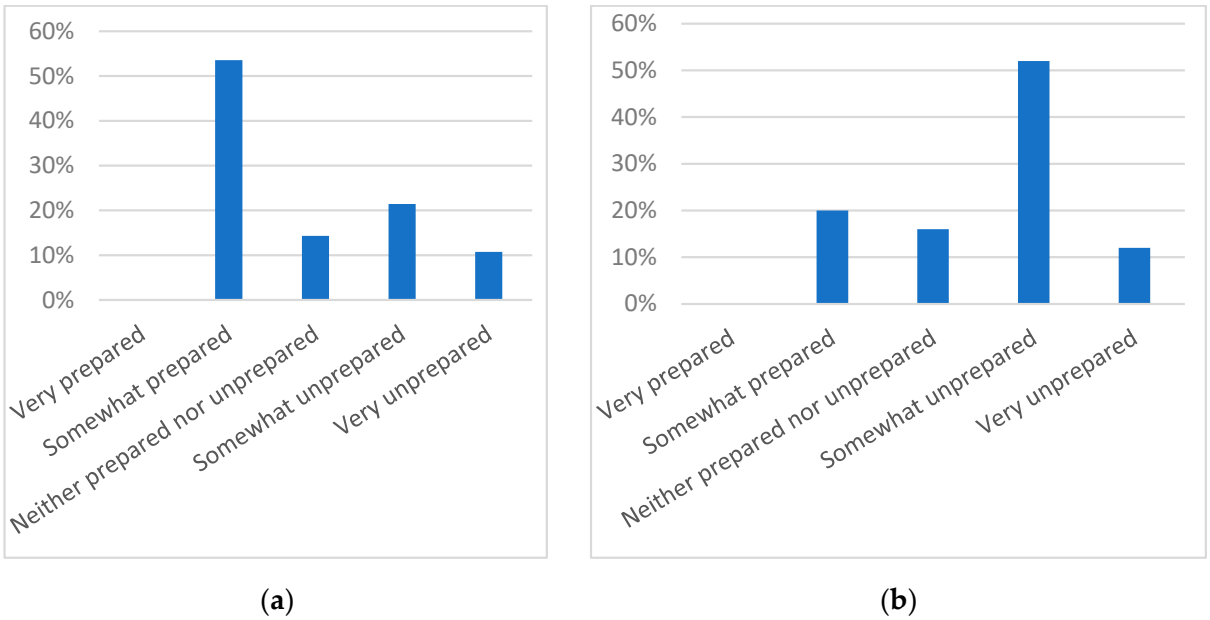


Figure 7. How prepared are shipping companies in meeting the IMO 2021 requirements and consequently addressing cyber security? (**a**) Europe; (**b**) Asia.

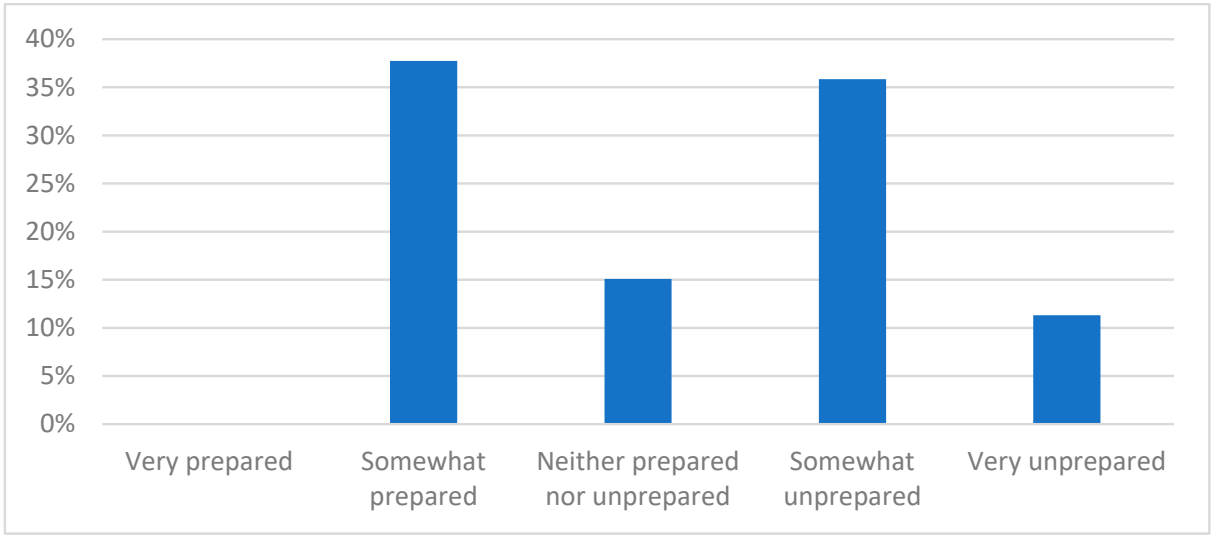


Figure 8. How prepared are shipping companies in meeting the IMO 2021 requirements and consequently addressing cyber security? (Asia and Europe).

The observed difference in perception on the level of preparedness for the IMO 2021 requirements is derived from two main attributes. The first attribute, as presented in the analysis of the findings of the previous questions, is that the IMO resolution does not offer clear guidance to the sector. Therefore, as it is demonstrated in Figure 7a,b that maritime transport stakeholders perceive differently what is required to meet the IMO resolution and address cyber security in the maritime transport sector. The second attribute is that there is a difference in perception in what cyber security entails. That perception derives from the increased technical savviness (as demonstrated in the literature review) compared to European counterparts, who are more "traditional" in operating the sector.

Over the years, Asian maritime transport stakeholders are amongst the first to apply technology solutions that improve operations (e.g., minimize costs, etc.) [28,29].

Following the preliminary analysis regarding the industry's response to cyber security, predominantly concerning the IMO 2021 resolution, the second part of the questionnaire examined the industry's perception of the impact of the COVID-19 pandemic in day-to-day maritime transport operations.

The first question of theme B explores if the COVID-19 pandemic affected the maritime cyber security landscape. Even though this is not a binary question, for matters of simplicity, the question was structured as such (yes or no). Responses collected from both focus groups in Europe and Asia, as illustrated in Figure 9a,b and summarized in Figure 10, concur that the cyber security of the maritime transport sector was affected by the COVID-19 pandemic.

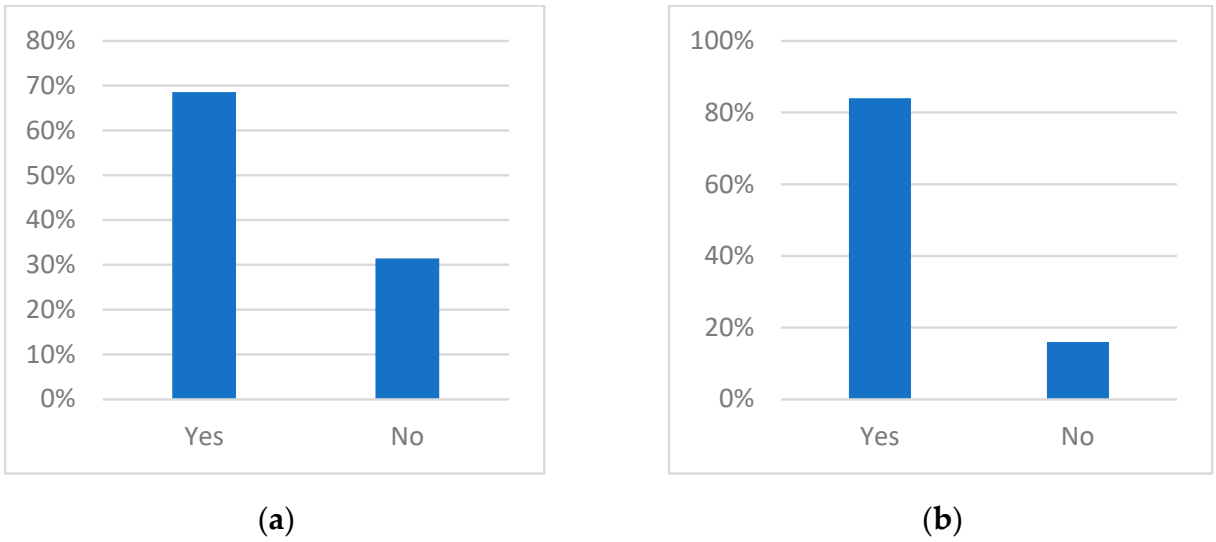


Figure 9. Has the COVID-19 pandemic affected the maritime cyber security landscape? (**a**) Europe; (**b**) Asia.

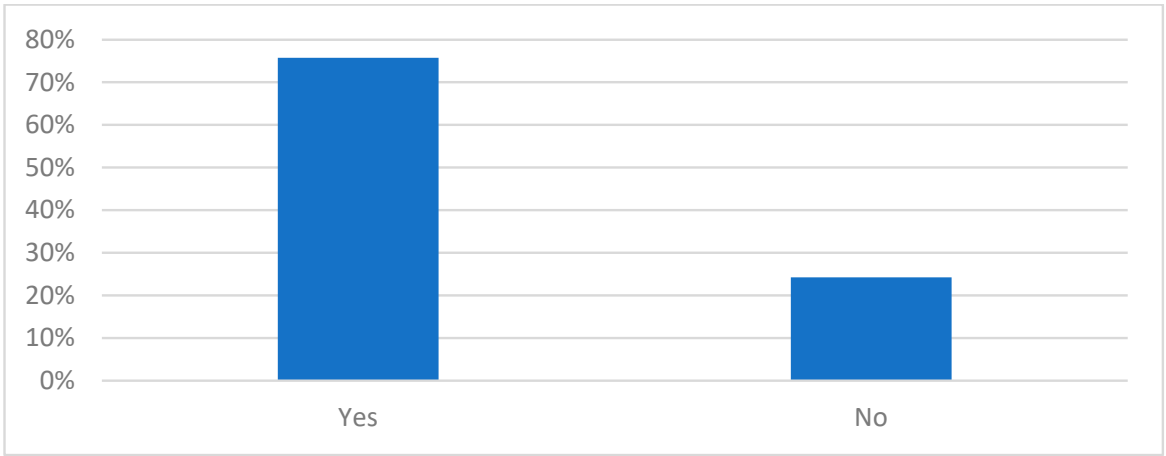


Figure 10. Has the COVID-19 pandemic affected the maritime cyber security landscape? (Asia and Europe).

This comes as no surprise, since, as noted previously, the number of cyberattacks since the appearance of the pandemic has globally, remarkably increased [23,24,29]. However, when trying to identify the effect of the pandemic on the maritime cyber security landscape, it became evident that respondents from Europe who believed that the industry's cyber security landscape was not affected, were twice as many as those from Asia, enhancing the points discussed in Figure 7a,b regarding the misconceptions about cyber security. As aforementioned, this originated from the fact that Asian maritime transport stakeholders

were amongst the first to apply technology solutions. Therefore, they were agnostic to the benefits of digital transformation in the maritime transport sector, along with the consequent potential cyber risks that they may face.

The next question of the survey examined whether the participants experienced a surge in cyberattacks in their organizations during the pandemic. This question aimed to narrow down the analysis, drawing from participants' direct engagement within their organizations. While in Europe the responses were split (with 53% mentioning that they did not experience a surge in cyber attacks in their organization and 47% mentioning the opposite), in Asia, two thirds of the respondents mentioned that they did not experience any surge in cyber attacks in their organizations during the pandemic. Figure 11a,b results are aggregated in Figure 12, demonstrate that there was an increase by 40% in cyber attacks in maritime transport organizations during the pandemic, reinforcing the argument that there is a need to increase cyber resilience in the maritime transport sector.

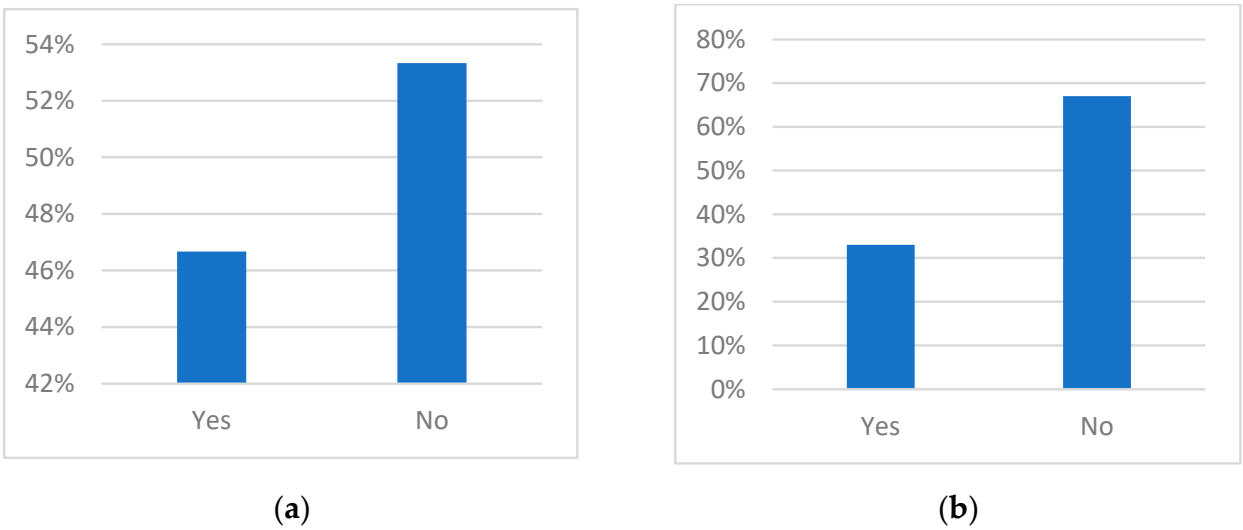


Figure 11. Have you experienced a surge in cyber attacks in your organization during the pandemic? (**a**) Europe; (**b**) Asia.

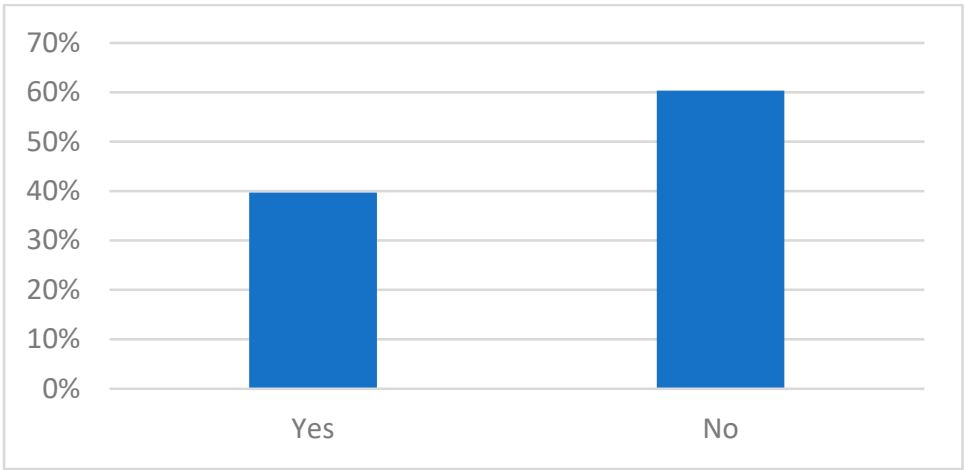


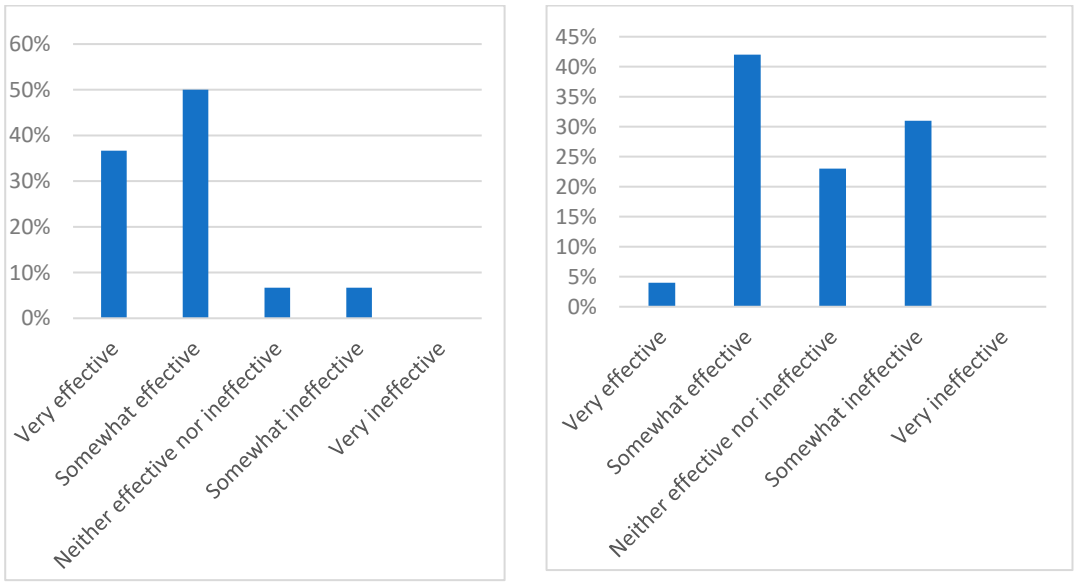
Figure 12. Have you experienced a surge in cyber attacks in your organization during the pandemic? (Asia and Europe).

Looking at the responses presented in Figure 11a,b, an interesting realization that reaffirms what has been previously mentioned was identified. Asian maritime experts were more advanced in terms of security-minded technology solutions applied within their maritime transport organizations, compared to their European counterparts. As such, they were able to mitigate incoming malicious content. Having the appropriate measures

in place and not allowing an increased number of attacks to penetrate their organizations ecosystem justified the responses presented in Figure 11b.

Similar to question 4, presented in Table 1 and analyzed above, the last question of the survey tried to identify the level of effectiveness of shipping companies in adapting to the new norm, due to the COVID-19 pandemic. This new norm entailed: (A) an increased number of employees working remotely (from home), (B) the adoption of digital solutions to facilitate this transition, and (C) uptake in number of cyber attacks affecting the industry.

As demonstrated in Figure 13a,b, 86% of European participants mentioned that shipping companies were either very or somewhat effective in adapting to the new norm. In comparison, opinions on the same matter from Asian participants were limited to almost half of the percentage demonstrated above (46% were either very or somewhat effective). Overall, Figure 14 illustrates that a strong majority of industry practitioners (68%) believed that the industry was effective in adapting to the new norm due to the COVID-19 pandemic.



(**a**) (**b**)

Figure 13. How effective have shipping companies been in adapting to the new norm due to the COVID-19 Pandemic? (**a**) Europe; (**b**) Asia.

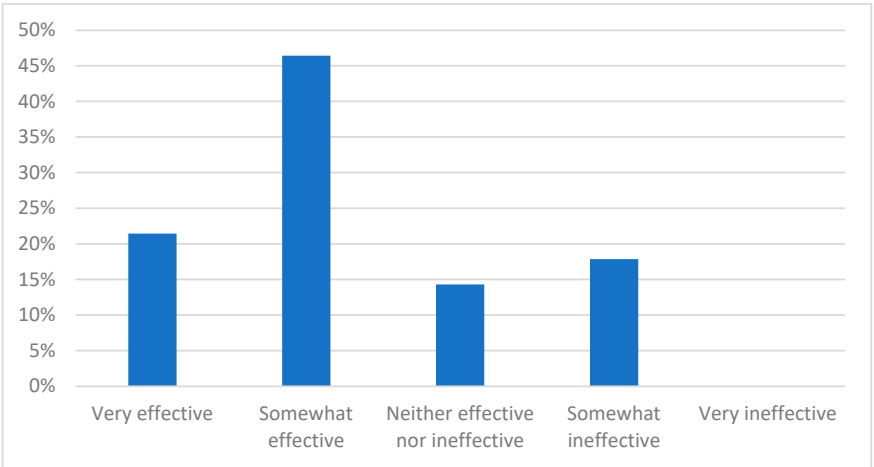


Figure 14. How effective have shipping companies been in adapting to the new norm due to the COVID-19 Pandemic? (Asia and Europe).

The difference in responses illustrated in Figure 13a,b reaffirms the trend identified throughout this survey regarding the level of maturity and understanding of what cyber security entails between the European and Asian participants. With reference to the findings of Figure 14, this comes as no surprise, as, unlike other industries, shipping, due to its nature, is used to having its most valuable assets operating remotely. Ships operating globally, thousand miles away from their shipping company's offices, have established procedures and technology solutions for decades.

In this section, the findings of the survey were demonstrated and discussed. Section 5 summarizes the key points of this research.

5. Conclusions

It became apparent throughout the paper that the increased adoption of digital solutions in the maritime transport sector introduces an insidious threat in cyber space. Ports and ships, being two of the most vital components of the supply chain, are vulnerable to cyber breaches, due to their complex operational environments. Both ships and ports have IT and OT systems composed by various third-party vendors, which, in most cases, require remote access, increasing cyber attacks to surface. Thus, maritime transport stakeholders have to take prompt actions in order to mitigate cyber risk. In order for this to happen, first and foremost, maritime transport stakeholders should understand what cyber security is; how it may affect their business; and the specific countermeasures that are suitable for their organization, and consequently adopt them to tackle these threats.

This research, unlike mainstream academic approaches, was initiated from the data collected during two targeted workshops, with the participation of more than 250 senior maritime transport practitioners. Due to the limitation of the research environment and the level of control available to the research team, it was decided not to over interpret the data with the use of quantitative statistical methods. The research team believes that its analysis will satisfy social scientists in terms of interpreting data collected in this activity by using a qualitative lens.

This impromptu engagement was commonly themed in order to address one key industry concern: whether cultural differences affect the level of understanding of maritime cyber security. As the two workshops were conducted virtually in Asia and Europe, it was realized that the predominant perception for cyber risk differs in these two geographical areas. The main analysis has reiterated that each group had a different understanding. A similar observation was conducted by Nisbett [26], who mentions that different cultures perceive specific topics in a different view. As stated by Nisbett and reaffirmed by our findings, East Asians think "holistically", while Westerners focus on specific subjects. This differentiation can also be attributed to the level of maturity regarding cyber security, as presented in the findings section. As such, Asians understand cyber security challenges better and consequently incorporate them in their aggregated business risk management. In contrast, the less mature Western maritime transport stakeholders perceive cyber security as an impartial risk factor to be dealt in isolation.

Findings presented in this research highlight that many maritime transport stakeholders are not aware of what cyber security entails and do not fully realize the degree of dependence of their businesses on software-enabled systems, platforms, and services. While they might acknowledge the existence of cyber threats in general terms, as apparent in Section 4, they miss important details; understanding how these cyber threats can affect their organizations' daily operations. A holistic approach to cyber risk management begins at the senior management level and extends downwards to the entire organization.

Future Research

Acknowledging that this paper was elaborated based on an opportunity that arose from the authors' engagement with the industry, we believe that further, targeted, academic research is to be conducted, with statistical tools, such as ANOVA, in mind. To achieve that, the research outline should include details of targeted audience profiles, along with a

questionnaire, which will be designed to collect information related to participants and their demographics. Such an approach would facilitate the implementation of aforementioned statistical tools and thus present a statistical analysis of the results. Specifically, future research should explore two main topics: (1) revalidate our findings as to how cultural differences affect the level of understanding of a specific topic, in this case maritime cyber security, with further research, such as longitudinal research, which could enhance our findings; (2) explore whether the surge in cyber attacks, partially due to pandemic, affected the sector's response to the IMO cyber requirements. This research should take place in a more academic style, where the theory should be tested against our main finding, that there is a different perception of cyber risk based on cultural background. To achieve this, enhanced collaboration between all key stakeholders (academics, cyber experts, maritime transport sector stakeholders) should take place. As we initiated this piece of research, due to our wide links with maritime transport stakeholders, we would happily participate in any future discussions, which we are sure will take place soon due to the urgent need to tackle such an important issue as maritime cyber risk management.

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

Funding: This research received no external funding.

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

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

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

Acknowledgments: The authors would like to thank the Greek Chamber of Commerce in Hong Kong and the International Propeller Club of Piraeus for organizing the events that led to this paper. Without their invaluable support, this piece of research would not have been possible.

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

References

1. CyRiM Report. Shen Attack Cyber Risk in Asia Pacific Ports. Available online: https://apps.cambridgeriskframework.com/erm/portal/publication/shen-attack (accessed on 31 October 2019).
2. Kuhn, K.; Kipkech, J.; Shaikh, S. Maritime Ports and Cybersecurity. In *Maritime Transport and ITS Solutions in Port Logistics*; Fiorini, M., Gupta, N., Eds.; IET: London, UK, 2021.
3. Polemi, N. *Port Cybersecurity: Securing Critical Information Infrastructures and Supply Chains*; Elsevier: Amsterdam, The Netherlands, 2017.
4. Peake, M. Cybersecurity Looks to the Cloud to Protect Data at Sea. Available online: https://www.wartsila.com/insights/article/cybersecurity-looks-to-the-cloud-to-protect-data-at-sea (accessed on 11 June 2021).
5. Greenberg, A. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*; Doubleday: New York, NY, USA, 2020.
6. ISACA State of Cybersecurity 2020. Available online: https://www.isaca.org/go/state-of-cybersecurity-2020 (accessed on 5 June 2021).
7. Fielder, A.; Panaousis, E.; Malacaria, P.; Hankin, C.; Smeraldi, F. Decision support approaches for cybersecurity investment. *Decis. Support Syst.* **2016**, *86*, 13–23. [CrossRef]
8. UNCTAD. *Review of Maritime Transport*; UNCTAD: Geneva, Switzerland, 2018.
9. Miller, C.; Stuart Wells, F. Balancing security and privacy in the digital workplace. *J. Chang. Manag.* **2007**, *7*, 315–328. [CrossRef]
10. Kapalidis, C. Cyber securityat Sea. In *Global Challenges in Maritime Security*; Otto, L., Ed.; Springer: Cham, Switzerland, 2020; pp. 127–143.
11. European Union. *EU Maritime Security Strategy*; European Commission: Brussels, Belgium, 2014.

12. NMIOTC. 1st NMIOTC Cybersecurity Conference in the Maritime Domain 2016 (04-05 OCT 2016), Chania Crete. Available online: https://nmiotc.nato.int/transformation/conferences/cyber-security-conference/ (accessed on 30 June 2021).
13. IMO. *Guidelines on Maritime Cyber Risk Management*; IMO: London, UK, 2017.
14. IMO. *Resolution MSC. Maritime Cyber Risk Management in Safety Management Systems*; IMO: London, UK, 2017.
15. UNCLOS (United Nations Convention on the Law of the Sea). United Nations Convention on the Law of the Sea of 10 December 1982 Overview and Full Text. Available online: https://www.un.org/depts/los/convention_agreements/convention_overview_convention.htm (accessed on 3 June 2021).
16. UNCTAD. *Review of Maritime Transport*; UNCTAD: Geneva, Switzerland, 2020.
17. US Coast Guard. *Navigation and Vessel Inspection Circular No. 01-20: Guidelines for Addressing Cyber Risks at Maritime Transportation Security Act (MTSA) Regulated Facilities*; US Coast Guard: Washington, DC, USA, 2020.
18. DNV. Our History. Available online: https://www.dnv.com/about/in-brief/our-history.html (accessed on 4 June 2021).
19. ABS Group. IMO Cyber Risk Management. Available online: https://www.abs-group.com/What-We-Do/Safety-Risk-and-Compliance/Cybersecurity/Maritime-Cybersecurity/IMO-Cyber-Risk-Management/ (accessed on 4 June 2021).
20. ClassNK Consulting Service, Cybersecurity Management System (CSMS) Construction Support. Available online: https://www.classnkcs.co.jp/en/cyber_security/index.html (accessed on 4 June 2021).
21. DNV. Maritime Cybersecurity. Available online: https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/index.html (accessed on 4 June 2021).
22. Hall, C. The Daily Show Agenda, 27st Annual Berlin First Conference, Wapack Labs. Available online: https://www.first.org/resources/papers/conf2015/first_2015_-_hall-_chris_-_daily_show_agenda_20150618_fw.pdf (accessed on 30 June 2021).
23. MTS-ISAC (Maritime Transportation System—Information Sharing and Analysis Center). 2020 Annual Report. Available online: https://www.mtsisac.org/post/2020-mts-isac-annual-report (accessed on 7 June 2021).
24. MarineLink, Maritime Cyber Attacks Increase 900%. Available online: https://www.marinelink.com/news/maritime-cyberattacks-increase-480311 (accessed on 30 June 2021).
25. Kapalidis, C. Maritime Cybersecurity: No Substitute for Testing, Chatham House. Available online: https://www.chathamhouse.org/expert/comment/maritime-cyber-security-no-substitute-testing (accessed on 11 June 2021).
26. Nisbett, R. *The Geography of Thought: How Asians and Westerners Think Differently... and Why*; Free Press: New York, NY, USA, 2003.
27. Kumar, S.; Hoffmann, J. Globalization: The maritime nexus. In *The Handbook of Maritime Economics and Business*; Grammenos, C., Ed.; Lloyd's: London, UK, 2002; pp. 35–62.
28. Watson, R.; Lind, M.; Haraldson, S. Physical and digital innovation in shipping: Seeding, standardizing, and sequencing. In Proceedings of the 50th Hawaii International Conference on System Sciences, Hilton Waikoloa Village, HI, USA, 4–7 January 2017.
29. Chan, H.K.; Dai, J.; Wang, X.; Lacka, E. Logistics and supply chain innovation in the context of the Belt and Road Initiative (BRI). *Transp. Res. Part E Logist. Transp. Rev.* **2019**, *132*, 51–56. [CrossRef]