Journal of *Marine Science and Engineering*

MDPI

Article

Qualitative Risk Assessment of Cybersecurity and Development of Vulnerability Enhancement Plans in Consideration of Digitalized Ship

Yunja Yoo and Han-Seon Park *

Maritime Safety Department, Korea Maritime Institute, Busan 49111, Korea; yjyoo@kmou.ac.kr
* Correspondence: hspark@kmi.re.kr

Abstract: The International Maritime Organization (IMO) published the Guidelines on Maritime Cyber Risk Management in 2017 to strengthen cybersecurity in consideration of digitalized ships. As part of these guidelines, the IMO recommends that each flag state should integrate and manage matters regarding cyber risk in the ship safety management system (SMS) according to the International Safety Management Code (ISM Code) before the first annual verification that takes place on or after 1 January 2021. The purpose of this paper is to identify cybersecurity risk components in the maritime sector that should be managed by the SMS in 2021 and to derive priorities for vulnerability improvement plans through itemized risk assessment. To this end, qualitative risk assessment (RA) was carried out for administrative, technical, and physical security risk components based on industry and international standards, which were additionally presented in the IMO guidelines. Based on the risk matrix from the RA analysis results, a survey on improving cybersecurity vulnerabilities in the maritime sector was conducted, and the analytic hierarchy process was used to analyze the results and derive improvement plan priority measures.

Keywords: cybersecurity; cyber threat; risk identification; risk matrix; risk assessment

Citation: Yoo, Y.; Park, H.-S. Qualitative Risk Assessment of Cybersecurity and Development of Vulnerability Enhancement Plans in Consideration of Digitalized Ship. *J. Mar. Sci. Eng.* **2021**, *9*, 565. https://doi.org/10.3390/jmse9060565

Received: 27 April 2021
Accepted: 19 May 2021
Published: 24 May 2021

1. Introduction

As technology advances, more and more ship systems rely on digitalization, integration, and automation and thus require cyber risk management [1–3]. Moreover, ships equipped with information technology (IT) and operational technology (OT) are connected to external networks, increasing the likelihood of cyberattacks in the form of unauthorized access to ship systems or malicious code infections [4–10]. Cyberattacks at sea can have adverse effects on the shipping lines supporting the safety operations of ships and vessels. For example, in February of 2017, the hacking of an 8250 TEU container ship's navigation system resulted in 10 h of the ship being controlled by cyber pirates, and other cases of offshore and shore cyberattacks also have been reported [11–18]. In June 2017, the port terminal IT system of Maersk Line, the world's largest shipping company, was also attacked by the NotPetya ransomware, which led Maersk's container ships and its 76 port terminals around the world to cease working, and the subsequent recovery process cost up to USD 300 million [19].

Based on a survey of key maritime stakeholders in more than 50 countries, the Global Maritime Issues Monitor 2018 report announced that "cyberattacks and data theft" would have the greatest impact on sea trade over the next 10 years (see Figure 1). In the global maritime issues map, cyberattacks and data theft are expected to have the second highest impact index of 3.61 over the next 10 years (1: minimal impact, 2: minor impact, 3: moderate impact, 4: major impact) [20,21]. The likelihood index for such an effect of cyberattacks and data theft over the next 10 years (1: very unlikely, 2: unlikely, 3: likely, 4: very likely) was the highest, at 3.67; conversely, the preparedness index for such issues (1: very unprepared, 2: unprepared, 3: neither prepared or unprepared, 4: prepared, 5:

very prepared) was the lowest, at 2.34. The high impact and likelihood index but low preparedness index for "cyberattacks and data theft" could cause serious economic damage. According to Cybersecurity Venture (2020), global cybercrime costs are expected to reach up to USD 6 trillion by 2021 and grow at an annual average rate of 15 percent to reach USD 10.5 trillion by 2025 [22].

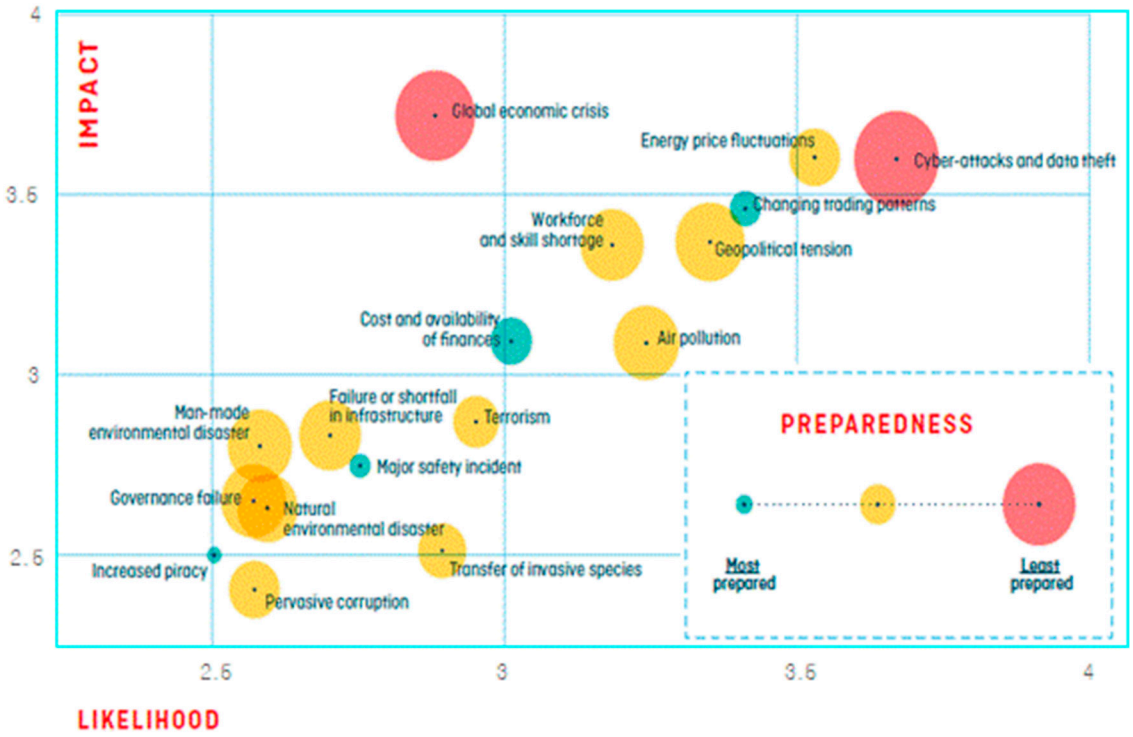

Figure 1. Global maritime issues map, adapted from [20].

The cyber environment on ships includes IT, comprising network components such as personal computers, laptops, tablets, and router switches, and OT, comprising control systems, sensors, actuators, and radars, and all of these can be the primary targets of cyber-attacks [3,8,23]. Tam and Jones [24] proposed some possible cyber vulnerabilities based on technical threats within their scope and suggested potential impacts; they also provided preventive policies. Rodseth and Burmeister [25] presented a risk assessment concept based on formal safety analysis (FSA) which suggested possible hazard scenarios of an unmanned ship. Chang et al. [26] tried to quantify the risk level of major hazard categories related to Maritime Autonomous Surface Ships (MASS) through a literature review. The risk level of cyber threats determined for a shipboard integrated navigational system (INS) was proposed by Svilicic et al. [27]. Vulnerabilities in digital components of an integrated bridge system (INS) were identified by Awan and Ghamdi [28]. In their study, Park et al. [12] performed a literature review to identify four cyber threats with risk control options in the maritime industry. In a similar vein, Kang [29] suggested some technical methods to enhance the cybersecurity of ship systems based on the industry guidelines [30]. In another study, Miron and Muita [31] provided recommendations on employing cybersecurity capability maturity models to support critical infrastructure providers, including ships and port facilities. Further, Kang et al. [32] suggested the development of a national cyber capability assessment methodology according to the base capability, attack capability, and defense capability. Moreover, criteria for the national cybersecurity capability assessment were proposed by Bae et al. [33]. However, measures to strengthen cybersecurity that comprehensively reflect policies that consider relevant stakeholders' needs or adequately protect the technical and physical security aspects of ship onboard systems against cyber risks are lacking. Therefore, comprehensive enhancement plans are needed to identify cybersecurity

vulnerabilities in consideration of the introduction of digitalized ships such as MASS in the maritime sector including shippers, and to strengthen the relevant security systems.

The International Maritime Organization (IMO) began a full discussion regarding MASS, represented by the digitized ship, at the 99th meeting of the Maritime Safety Committee (MSC) [34]. The IMO defined the levels of autonomy (level 1: seafarer onboard and partial automation, level 2: seafarer onboard and remote control, level 3: seafarer off-board and remote control, level 4: fully automated) of MASS. The meeting also carried out a regulatory scoping exercise (RSE) for IMO jurisdiction agreements regarding MASS operation at each autonomy level [35].

Recognizing the need to respond to cyber threats on a digitalized ship, the IMO has been conducting discussions on maritime cybersecurity, ultimately adopting a resolution on maritime cyber risk management at the 98th MSC in 2017 [36]. In accordance with this resolution, the IMO recommends that each flag state should integrate matters concerning cyber risk management regulations into the ship safety management system (SMS) before the first annual verification of the company's Document of Compliance (DoC), which occurs after 1 January 2021 [36–39]. The IMO guidelines include functional elements to support cyber risk management and provide appropriate integration into the risk management framework (United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity: NIST's Risk Management Framework). Additionally, the IMO presents shipowners' group guidelines and the ISO/IEC 27001 international standards as best practices for implementing marine cyber risk management [30,38,40,41]. The IMO also includes cyber risk management in Section 2.10 of the Interim guidelines for MASS trials of MSC.1/Circ.1604 document, 2019 [42].

The purpose of this paper is to identify cyber risk factors based on the best practices proposed by IMO guidelines, such as the shipowners' group guidelines (BIMCO et al. guidelines), and the ISO/IEC 27001 international standards, and to derive improvement plan priorities for enhancing cybersecurity systems in the maritime sector. To do so, a qualitative risk assessment was performed to identify item-specific vulnerabilities. The analytic hierarchy process (AHP) was used to analyze the results of a questionnaire on improving cybersecurity vulnerabilities and determine improvement plan priorities. Section 2 of the paper presents the procedures used to identify cybersecurity vulnerabilities in the maritime sector and the risk assessment methodologies with regard to vulnerability considering digitalized ships. It also introduces the AHP analysis content and the methods used to derive improvement plan priorities for enhancing cybersecurity vulnerabilities. Section 3 presents the improvement plan priorities based on a qualitative risk assessment of vulnerabilities in each administrative, technical, and physical security area. Section 4 presents a review of the results and their limitations. Section 5 summarizes the mains results of the study.

2. Methodology

To derive improvement plan priorities addressing how to enhance cybersecurity vulnerabilities in digitalized ships in the maritime sector, 27 risk factors were identified based on the risk classification system presented in the ISO/IEC 27001 international standards and industry guidelines [30,40]. ISO/IEC 27001 specifies the security technique requirements for an information security management system, including control objectives to support information security. Failure to control objectives means failing to protect information systems; it is therefore classified as a risk in the information system and is described in Table 1. These are shown in Table 1 and fall into three main groups: administrative risks, technical risks, and physical security risks.

Table 1. Risk factors and identification codes by cybersecurity area.

Security Areas	Risk Factors * in Case of Control Failure	Identification Code (ID)
Administrative Security	1. Raise awareness on information protection and conduct education targeting staff on board as well as on land	A1
	2. Access limitation of visitors (port-related officials, technicians, agents, etc.)	A2
	3. Upgrade hardware (H/W) and software (S/W), and S/W maintenance	A3
	4. Update anti-virus and malware prevention S/W tools	A4
	5. System of regulating remote access	A5
	6. Access to information is only allowed to authorized staff	A6
	7. Control the use of portable media (USB, portable PC, etc.)	A7
	8. Policy for discarding equipment including data	A8
	9. Establish contingency plans for cyberattacks	A9
Technical Security	1. Limitation and control of network port, protocol, and service	T1
	2. Configure network equipment such as firewall, router, and switch	T2
	3. Detect, block, and warn of cyberattacks through the system	T3
	4. Data encryption by utilizing a virtual private network (VPN)	T4
	5. Wireless access control with encrypted keys	T5
	6. Install anti-malicious code software and regularly install patch files	T6
	7. Hardware and software security configuration (system access limit excluding administrator)	T7
	8. Protect emails and web browsers	T8
	9. Support data backup and recovery	T9
Physical Security	1. Set up physical security area and access control	P1
	2. Design and apply physical security for office, working space, and facility	P2
	3. Access control and information system isolation of unauthorized users	P3
	4. Secure continuous availability and confidentiality from the cut-off of power supply and support facilities	P4
	5. Protect power supply and communication cables supporting data transmission and information facilities from being damaged	P5
	6. Ban on carrying any equipment, information, and software outside without prior approval	P6
	7. In case of reuse and discarding of equipment including storage media, remove data and licensed S/W and confirm the removal	P7
	8. Protect user information and check the management of unused equipment	P8
	9. Desk organization policy for documents and portable storage media	P9

* Source: The guidelines on cybersecurity on board ships, adapted from [30], ISO/IEC 27001—Annex A. Reference control objectives and controls, adapted from [40].

The importance of each of these 27 risks, based on risk assessment (RA, expressed as likelihood × severity), was assessed by six security experts from classification societies. The priorities for mitigating the 12 most important risks were then assessed using a questionnaire survey of 127 people working in related fields (response rate 28%) and the analytic hierarchy process [43–46]. The survey contains questions that allow respondents to check multiple choice in a single question. This causes the number of survey respondents (117)

and the figures (127) for the results of the survey items to differ. The overall methodology process for the risk assessment and the derivation of vulnerability improvement plans are shown in Figure 2 and Table 2.

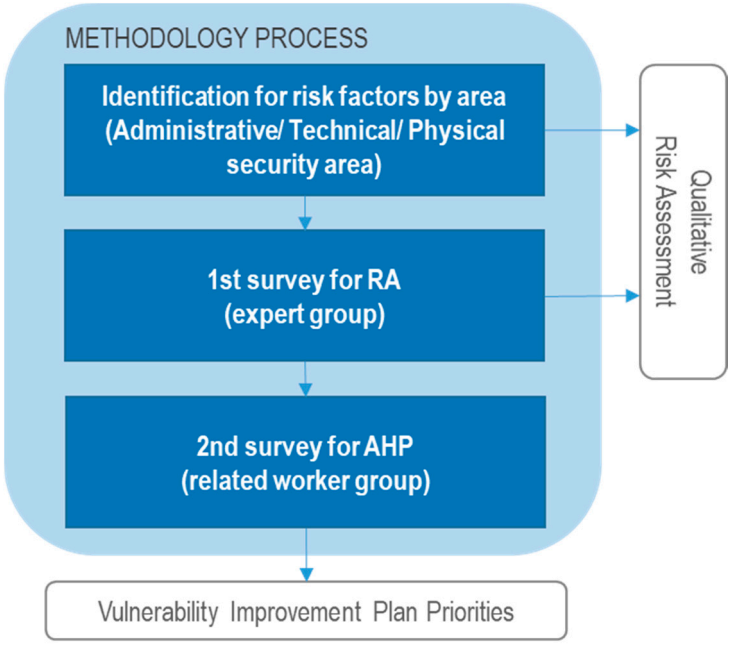

Figure 2. Methodology process for risk assessment and AHP.

Table 2. An overview of the survey respondents (first survey for RA and second survey for cybersecurity vulnerability improvement prioritization).

Survey	Working Area	Respondents (No.)	Percentage (%)
1st Survey for RA (Expert Group)	Cybersecurity Certification	6	-
2nd Survey for AHP (Workers in Related Agencies)	Policy	15	11.8
	Shipping	20	15.7
	Maritime Affairs	33	26.0
	Information and Communication	24	18.9
	Security Management	6	4.7
	Etc.	29	22.8
	Total	127 * (Online: 41, Field: 76)	100.0 (** Effective Response Rate: 28.2)

* actual no.: 117 (multiple choice for working area), ** less than 0.066 consistency ratio.

2.1. Risk Factors and Risk Assessment

In addition to the IMO guidelines, industry guidelines (e.g., BIMCO) are divided into technical protection measures and procedural protective measures, including physical security as a measure to protect the ship's key systems and data. Annex A of the ISO/IEC 27001 IT international standard, one of the IMO guidelines' best practices, presents control items for cyber hazards, and failure to control these items may lead to cybersecurity vulnerabilities. Therefore, the risk factors applicable to the maritime sector were identified through an expert review based on the BIMCO industry guidelines and the cyber risk management measures and control items of the ISO/IEC 27001 standard, and the potential cyber risk hazards in ship systems were identified according to the administrative, technical, or physical security area. Table 1 shows the risk factors for each security area based on the BIMCO industry guidelines and ISO/IEC 27001 standards, which are further outlined in the IMO guidelines [38]. The 27 risk factors listed in Table 1 include items involving

procedural protection measures and technical protection measures (including physical protection measures in the BIMCO industry guidelines) and items involving second-level reference control objectives and controls in Annex A of the ISO/IEC 27001 standard [30,40].

The qualitative RA of cybersecurity risk assessment was carried out for each security area in the maritime sector. Based on expert surveys, qualitative risk levels can be expressed as the frequency of occurrence (or likelihood) of control failures for each hazard and the severity (impact) resulting from failure of control on a scale from 1 to 5, producing the risk matrix shown in Figure 3 and the risk level indices by component shown in Table 3. The risk can be expressed by multiplying the likelihood and severity in Equation (1) [47–51].

$$Risk_{phase} = Likelihood_{A,T,P} \times Severity_{A,T,P} \quad (1)$$

where $Risk_{phase}$ is the risk by phase of administrative (A), technical (T), and physical (P) security areas, $Likelihood_{A,T,P}$ is the likelihood of cybersecurity control failure, and $Severity_{A,T,P}$ is the severity or impact as a result of cybersecurity control failure.

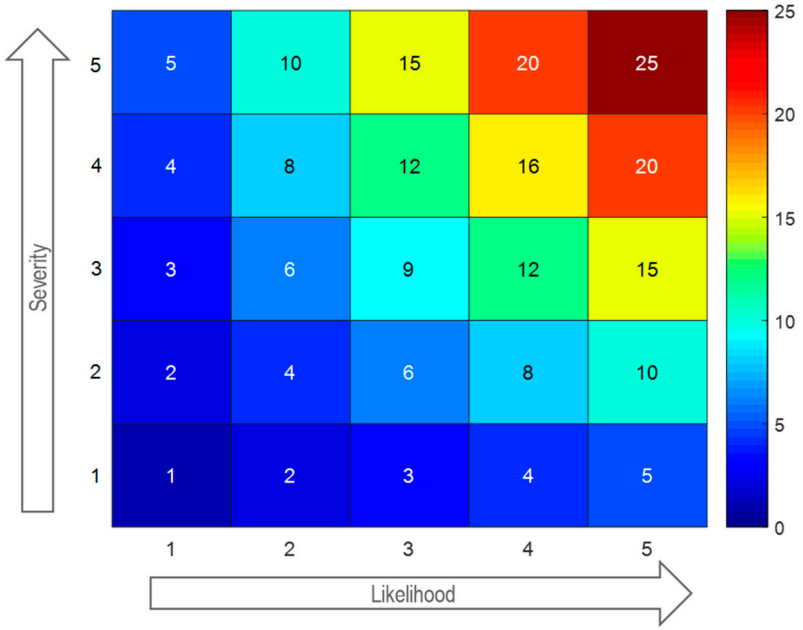

Figure 3. Risk matrix concept applied RA.

Table 3. Risk level with likelihood and severity indices.

Index	Likelihood	Severity	RA	Risk Level	Color
5	Very Likely	Very Severe	21–25	Very High Risk	
4	Likely	Severe	16–20	High Risk	
3	Moderate	Moderate	11–15	Medium Risk	
2	Unlikely	Not Severe	6–10	Low Risk	
1	Very Unlikely	Very not Severe	1–5	Very Low Risk	

2.2. Analytic Hierarchy Process Analysis

To derive improvement plan priorities for enhancing cybersecurity vulnerabilities in maritime areas, the first nine survey items in each security area were reviewed and configured based on the RA results by an expert group. Four items for each security area—that is, administrative, technical, and physical areas—were finally selected through a group of experts by reviewing the items with high risk as a result of RA.

In order to derive the priorities for cybersecurity risk factors, the survey method applied the AHP, a multi-attribute decision making technique that can group items that improve risk components within each security area. The questionnaire was structured as

independently as possible through expert review to ensure that the details of each security area were not duplicated, and the weight of each category (level-1) or group assessment item (level-2) was calculated by selecting four vulnerability improvement factors for each security area.

In the AHP, the data analysis procedure of a given dataset **A** (pair-wise comparison matrix) is as follows [43–46]:

$$\mathbf{A} = [a_{ij}] = \frac{w_i}{w_j} \text{ (for } i, j = 1, 2, \cdots, n) \quad (2)$$

$$\mathbf{A} \cdot \mathbf{w} = n \cdot \mathbf{w} = \lambda_{max} \cdot \mathbf{w} \ (\lambda_{max} \geq n, \ \ \mathbf{w} = w_1, w_2, \cdots, w_n) \quad (3)$$

where a_{ij} is numerical comparison between the values i and j, w_i and w_j are underlying subjective priority weights ($\sum w = 1$), **w** is the normalized weight vector, and λ_{max} is the maximum eigenvalue of matrix **A**.

The consistency index (CI), which is to validate the results of the AHP, is measured following the formula [46,52,53]

$$CI = \frac{\lambda_{max} - n}{n - 1} \quad (4)$$

The consistency ratio (CR), which is expressed as CI/RI using CI and the random consistency index (RI), is acceptable when the results are lower than 0.1 [46].

3. Analysis Results

3.1. Risk Assessment Results

In the maritime sector, a cybersecurity risk assessment was conducted on an expert group. The group of experts consisted of six people who have carried out cybersecurity certification tasks in the field of classification societies for ships, shipping companies, and shipyards for many years (average work experience: 11.3 years), and they reviewed 27 survey items for risk assessment and conducted the first survey (RA assessment). Table 2 shows the first survey, which performs an RA assessment for a group of experts, and an overview of the second questionnaire for deriving improvement plan priorities for determining the cybersecurity risk factors for employees in related agencies.

The results of the mean RA values from experts' surveys are shown in Figures 4 and 5 according to the risk matrix and risk component identification codes (A1–A9, T1–T9, P1–P9) of Table 1 items. In the administrative security area, A7 (Mobile media control policy, such as USB, mobile PC) had the highest RA at 17, followed by A3 (H/W, S/W upgrade, and S/W maintenance) at 14.17. In the technical security area, T6 (Installation of malicious code protection S/W and periodic patch files) had the highest RA at 16.5. In the physical security area, P1 (Physical security zone setting and access control) had the highest RA at 12, but most of the items lay below the medium risk level (11–15), relatively low compared to those in the administrative and technical security areas. The itemized RA average was the highest in the technical security area at 11.35, followed by the administrative security area at 11.28, and only 9.02 for the physical security area, indicating relatively low risk in that area. Of the 27 risk items, 2 (A7, T6) were shown to be high risk (RA 16–20), and 15 were shown to be medium risk with an RA range of 11–15 (T5, . . . , P9). Nine items appeared to be low risk with an RA range of 6–10, with the physical security area included the most frequently in Figure 5.

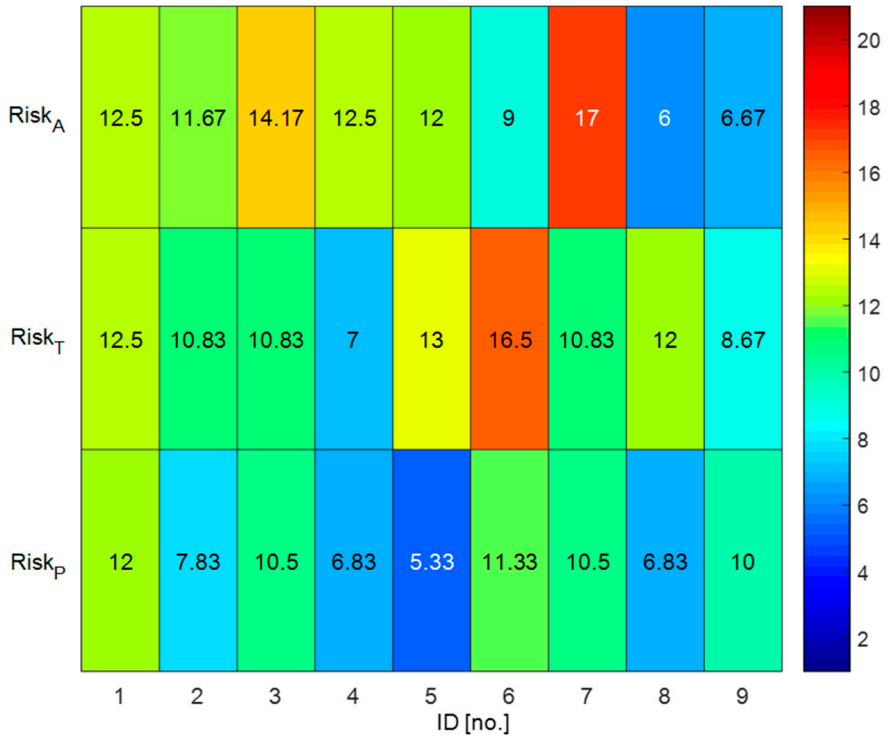

Figure 4. RA results by cybersecurity area with risk matrix.

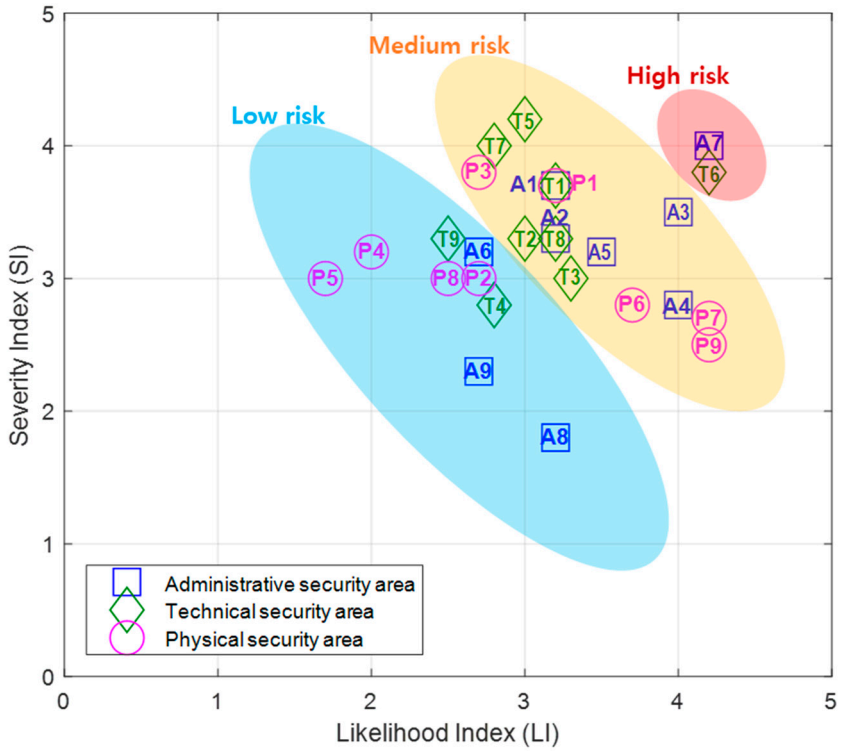

Figure 5. Risk level by cybersecurity area with LI and SI.

3.2. Vulnerability Improvement Priority

A second survey containing the 12 items from Table 4 was conducted among the 117 (online survey: 41, field survey: 76) maritime and security-related workers shown in Table 2 to determine priorities for improving cybersecurity vulnerabilities in the maritime sector. The IMO guidelines propose cyber risk management, including the NIST

cybersecurity framework (Identify-Protect-Detect-Respond-Recover) [38,41]. The Recover function should include plans for resilience and restoration of systems when a cybersecurity incident occurs. Therefore, although the RA results of A9 (Establish contingency plans for cyberattacks) were low at 6.67 (risk level: low risk), it was included in the final questionnaire regarding performing an AHP in the administrative security area with an expert group review.

Table 4. Relative importance assessment items for cybersecurity vulnerability improvement prioritization.

Security Areas (Level-1)		Assessment Items (Level-2)
I	Administrative Security	1. Raise awareness on information protection and conduct education targeting staff on board as well as on land 2. Control the use of portable media (USB, portable PC, etc.) 3. Upgrade H/W and S/W, and software maintenance 4. Establish contingency plans for cyberattacks
II	Technical Security	1. Limitation and control of network port, protocol, and service 2. Detect, block, and warn of cyberattacks through the system 3. Wireless access control with encrypted keys 4. Support data backup and recovery
III	Physical Security	1. Set up physical security area and access control 2. Ban on carrying any equipment, information, and software outside without prior approval 3. Secure continuous availability and confidentiality from the cut-off of power supply and support facilities 4. In case of reuse and discarding of equipment including storage media, remove data and licensed S/W and confirm the removal

The analysis of the results produced the itemized importance of the factors by security area with a consistency ratio of less than 0.066 (effective questionnaire response rate: 28.2%), as shown in Table 5. The weight of relative importance was the highest for technical security, with 0.377, followed by administrative security with 0.363. The weight of 0.281 for physical security indicates that it is relatively less important than the other areas.

Table 5. AHP analysis results for prioritizing cybersecurity vulnerability improvements.

Category (Weighting)	Security Area	Vulnerabilities	Score	Rank
I (0.363)	Administrative Security	I-1	0.128	1
		I-2	0.096	4
		I-3	0.081	6
		I-4	0.049	11
II (0.377)	Technical Security	II-1	0.122	2
		II-2	0.12	3
		II-3	0.066	10
		II-4	0.069	9
III (0.281)	Physical Security	III-1	0.088	5
		III-2	0.07	7
		III-3	0.069	8
		III-4	0.042	12

The highest priority among all 12 vulnerability improvement items was item I-1 (Awareness and education) in the administrative security area, with a score of 0.128, followed by the technical security items of II-1 (Network access control) with 0.122 and II-2 (Cyberattack detection and prevention) with 0.120.

4. Discussion

4.1. Considerations and Limitations of the Study

In this paper, the cybersecurity risk factors in the administrative, technical, and physical security areas of the maritime sector were identified based on the literature and expert opinion, and their relative significance was investigated using a survey and a subsequent analysis of the results to determine improvement plan priorities for enhancing cybersecurity vulnerabilities. Awareness and training with regard to information protection, an item in the administrative security area, was found to have the highest importance and priority. On average, however, the technical security area had the most significant weighting, indicating the significant importance of the items in this area as well as the administrative security one.

The cybersecurity risk assessment indicated that the risk factors in the administrative security area (A1–A5, A7) had a medium risk level (RA 11–15) or higher, indicating vulnerability. Likewise, three items in the technical security area (T1, T5–T6) had a medium risk level or higher. In contrast, only one element in the physical security area (P1) had a medium risk level, indicating that this area features the lowest risk. The risk was the highest in the technical security area (RA index on average: 11.35), followed closely by administrative security (RA index on average: 11.2), whereas physical security was found to have relatively low risk (RA index on average: 9.2).

The AHP analysis aimed at determining improvement plan priorities found that the technical security area had the highest importance weight (0.377), followed closely by administrative security (0.363). Individually, the most important items were I-1 (Awareness and education) in the administrative security area, followed by II-1 (Network access control) and II-2 (Cyberattack detection and blocking) in the technical security area.

In the expert group, the average RA value was 11.35, indicating that technical security was the most important, while the related worker group also judged the importance of the technical security area as 0.363. The RA results of A7 (Control the use of portable media such as USB, portable PC) for the expert group were the highest at 17 (first of 27 items), while the AHP results of the related worker group for the same item were ranked fourth out of 12 items. In addition, A1 (Raise awareness on information protection and conduction targeting staff on board as well as on land), with a mid-level risk of 12.5 in the expert group, was ranked the highest in the related worker group AHP result, indicating that there was a difference in consciousness between the two groups.

The limitation of this qualitative RA is that it does not yield quantitative risk levels for all vulnerable elements of a ship's IT/OT systems. Additional studies using quantitative assessment methods referring to industry standards used to assess security vulnerabilities in computer systems are required to calculate quantitative risks.

The Korean government started the Korea Autonomous Surface Ship (KASS) project in 2020 to develop four core technologies with 13 detailed element technologies by 2025. Cybersecurity technology development is also included in the detailed tasks [54]. Development will be carried out on autonomous ships by developing security gateways and integrated security management systems, while its performance will be evaluated through verification such as penetration testing. As the KASS project progresses, quantitative assessments of actual MASS ships should be carried out at the practical level on behalf of cyber risk qualitative assessments in the future.

4.2. Recommendations for Improvement Plans

The IMO's guidelines on maritime cyber risk management recommend that matters concerning administrative security for cyber risk management should be reflected in the

safety management systems (SMSs) of the International Safety Management Code (ISM Code) [39] before the first annual verification can be conducted after January 2021 [38].

The Korean government has established standards for the ISM Code in Article 46 of the Maritime Safety Act (establishment of safety management systems for vessels), Article 15 of the Enforcement Decree of the same act (vessels subject to establishing and implementing safety management systems), and Article 16 (qualification standards for designated persons and safety management personnel) [55,56].

However, there is no basis for forcing matters concerning cybersecurity under the current law, and as the IMO recommends revising the ISM Code to include matters concerning cyber risk management, domestic laws should consider preparing legal procedures to include matters related to cyber risk management. The IMO has discussed including matters concerning the protection of physical cyber assets in the Ship Security Plan (SSP) of the International Ship and Port Facility Security Code (ISPS Code) [57,58].

The Korean government has a legal basis for covering physical security measures for ships and port facilities (as required by the ISPS Code) in its International Ship and Port Facility Security Act and the Enforcement Decree of the International Ship and Port Facility Security Act [59,60]. The ISPS Codes focus on physical security areas, and they must be expanded and reviewed to cover both administrative and technical security areas of the ISM Code as one legislation.

It is also necessary to consider the improvement plan priorities from the AHP results, which are the top four priorities: I-1 (Awareness and education) and I-2 (Control the use of portable media) in the administrative security area, and II-1 (Network access control) and II-2 (Cyberattack detection and blocking) in the technical security area, when reviewing and discussing the current law for modification. For the I-1 and I-2 items, regular security training needs to be mandatory for workers handling information security systems, and measures should be taken to ensure that they are used only for authorized mobile media. For items II-1 and II-2, there should be a plan in place to apply control techniques that enable network access only to authorized systems through authentication (or certification by a classification society), and to apply detection–blocking techniques against cyberattacks and threats.

5. Conclusions

As part of its aim of strengthening cybersecurity systems in the maritime sector, the IMO published the "Guidelines on Maritime Cyber Risk Management" in 2017, adding to the ISO international standard, the U.S. National Institute of Standards and Technology's standards, and industry guidelines for shipowners' organizations. Under the IMO's guidelines, each flag state is to integrate and manage matters concerning cyber risk in the ship SMS of the ISM Code before the first annual audit due on or after 1 January 2021.

In this paper, in order to derive cybersecurity improvement plan priorities in consideration of digitalized ships, cybersecurity vulnerability items in the maritime sector were divided into the three areas of administrative, technical, and physical security based on industry guidelines and international standards. The goal was to identify cyber issues and perform a vulnerability analysis regarding factors that should be integrated into and managed by the ship SMS in 2021.

A risk matrix for maritime cybersecurity vulnerability analysis was used to perform a qualitative risk assessment (RA) based on the risk factors for each security area, comprising a frequency of occurrence index and a severity index. Furthermore, to derive improvement plan priority survey items for cybersecurity risk factors in the maritime sector, the high-risk items from the RA results of the risk matrix were reflected in the final survey items for the AHP analysis after an expert review.

Any assessment of cyber risks should cover administrative and technical risks, as well as physical security, as the RA in the first (expert) survey showed that the first two areas represent the largest risks, whilst the second (AHP) survey suggested that members of the

maritime community would give them higher priority for risk mitigation. The top three priorities for mitigating maritime cybersecurity risks are as follows:

- Increasing awareness of risks and educating staff about mitigation measures;
- Controlling access to cyber networks;
- Improving threat detection and blocking systems.

Several recommendations for improvement plans have been proposed in connection with cybersecurity in the maritime sector under the current domestic legal system constraints and in accordance with the AHP results.

Further studies relying on quantitative assessment methods, such as industry standards used to assess security vulnerabilities in computer systems, are required to assess the cybersecurity factors in the future of IT/OT systems.

Author Contributions: Conceptualization and methodology, Y.Y.; survey and analysis, Y.Y.; writing—original draft preparation, Y.Y.; writing—review and editing, Y.Y.; supervision and project administration, H.-S.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by "A study on strengthening cybersecurity systems in the maritime sector (KMI201916)" funded by the Korea Maritime Institute; and "Development of Autonomous Ship Technology (20200615)" funded by the Ministry of Oceans and Fisheries (MOF, Korea).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Request to corresponding author of this article.

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

References

1. Kessler, G.C.; Craiger, J.P.; Haass, J.C. A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system. *J. Trans. Nav.* **2018**, *12*, 429–437. [CrossRef]
2. Oikonomou, S. Maritime Cybersecurity Practices Scheme (Block Box). Master's Thesis, School of Science Informatics and Computational Biomedicine, University of Thessaly, San Jose, CA, USA, 2019.
3. You, B.; Zhang, Y.; Cheng, L.C. Review on cybersecurity risk assessment and evaluation and their approaches on maritime transportation. In Proceedings of the 30th Annual Conference of International Chinese Transportation Professionals Association, Houston, TX, USA, 19–21 May 2017; pp. 429–437.
4. AON. *2018 Cybersecurity Predictions: A Shift to Managing Cyber as an Enterprise Risk*, 2018 ed.; Aon Cyber Solutions: London, UK, 2018.
5. CISCO. *2018 Annual Cybersecurity Report*, 2018 ed.; CISCO: San Jose, CA, USA, 2018.
6. COMODO. *Comodo cybersecurity Q1 2018 Report*, 2018 ed.; COMODO Threat Research Labs: Clifton, NJ, USA, 2018.
7. FIRE-EYE. *M-Trends 2018*, 2018 ed.; FireEye: Milpitas, CA, USA, 2018.
8. Kessler, G.C. Cybersecurity in the maritime domain. In Proceedings of the Marine Safety & Security Council; US Department of Homeland Security: Washington, DC, USA; US Coast Guard: Arlington, VA, USA, 2019; Volume 76, pp. 34–39.
9. PWC. *Revitalizing Privacy and Trust in a Data-Driven World: Key Findings from The Global State of Information Security Survey 2018*, 2018 ed.; PwC: London, UK, 2018.
10. WIPRO. *State of Cybersecurity Report 2018: Foresight for the Global Cybersecurity Community*, 2018 ed.; WIPRO: Bengaluru, India, 2018.
11. G-CAPTAIN. Clarkson Plc Reveals Details of 2017 Cybersecurity Incident. Available online: https://gcaptain.com/clarkson-plc-reveals-details-of-2017-cyber-security-incident/ (accessed on 19 June 2019).
12. Park, C.; Shi, W.; Zhang, W.; Kontovas, C.; Chang, C.H. Cybersecurity in the maritime industry: A literature review. In Proceedings of the International Association of Maritime Universities (IAMU) Conference, Tokyo, Japan, 30 October–1 November 2019.
13. SAFETY-AT-SEA. Shipping Must Confront Onboard Systems' Cyber Vulnerabilities. Available online: https://safetyatsea.net/news/2017/shipping-must-confront-onboard-systems-cyber-vulnerabilities/ (accessed on 19 June 2019).
14. SAFETY-AT-SEA. Cyber Attack Hits COSCO Shipping. Available online: https://safetyatsea.net/news/2018/cyber-attack-hits-cosco-shipping/ (accessed on 19 June 2019).
15. SAFETY4SEA. Lessons to be Learned from Recent Cyber Incidents. Available online: https://safety4sea.com/cm-lessons-to-be-learned-from-recent-cyber-incidents/ (accessed on 19 June 2019).

16. THREAT-POST. Gold Galleon Hacking Group Plunders Shipping Industry. Available online: https://threatpost.com/gold-galleon-hacking-group-plunders-shipping-industry/131203/ (accessed on 19 June 2019).
17. WORLD-MARITIME-NEWS. Hackers Access BW Group's IT Systems. Available online: https://worldmaritimenews.com/archives/232434/hackers-access-bw-groups-it-systems-countermeasures-undertaken/ (accessed on 19 June 2019).
18. ZDNET. Port of San Diego Suffers Cyber-Attack. Available online: https://www.zdnet.com/article/port-of-san-diego-suffers-cyber-attack-second-port-in-a-week-after-barcelona/ (accessed on 19 June 2019).
19. SAFETY4SEA. Maersk Line: Surviving from a Cyber Attack. Available online: https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/ (accessed on 19 June 2019).
20. GMF; MARSH; IUMI. *Global Maritime Issues Monitor*, 2018 ed.; Global Maritime Forum Foundation: Copenhagen, Denmark, 2018.
21. ALLIANZ. *Safety and Shipping Review 2019: An Annual Review of Trends and Developments in Shipping Losses and Safety*, 2019 ed.; Allianz Global Corporate & Specialty: Munich, Germany, 2019.
22. CYBERCRIME-MAGAZINE. Cybercrime to Cost the World $10.5 Trillion Annually by 2025. Available online: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (accessed on 9 December 2020).
23. Kavallieratos, G.; Katsikas, S. Managing cyber security risks of the cyber-enabled ship. *J. Mar. Sci. Eng.* **2020**, *8*, 768. [CrossRef]
24. Tam, K.; Jones, K. Maritime cyber-security policy: The scope and impact of evolving technology on international shipping. *J. Cyber Policy* **2018**, *3*, 147–164. [CrossRef]
25. Rodseth, O.; Burmeister, H. Risk assessment for an unmanned merchant ship. *J. TransNav* **2015**, *9*, 147–164. [CrossRef]
26. Chang, C.; Kontovas, C.; Yu, Q.; Yang, Z. Risk assessment of the operations of maritime autonomous surface ships. *Reliab. Eng. Syst. Saf.* **2021**, *207*, 1–11. [CrossRef]
27. Svilicic, B.; Rudan, I.; Jugovic, A.; Zec, D. A study on cyber security threats in a shipboard Integrated Navigational System. *J. Mar. Sci. Eng.* **2019**, *7*, 364. [CrossRef]
28. Awan, M.; Ghamdi, M. Understanding the vulnerabilities in digital components of an Integrated Bridge System (IBS). *J. Mar. Sci. Eng.* **2019**, *7*, 350. [CrossRef]
29. Kang, N.S. Analysis of on-board ship cybersecurity. *J. Kor. Soc. Mar. Eng.* **2018**, *42*, 463–471. [CrossRef]
30. BIMCO; CLIA; ICS; INTERCARGO; INTERMANAGER; INTERTANKO; IUMI; OCIMF; WSC. *The Guidelines on Cyber Security Onboard Ships*, 3rd ed.; INTERCARGO: London, UK, 2018.
31. Miron, W.; Muita, K. Cybersecurity capability maturity models for providers for critical infrastructure. *Technol. Innov. Manag. Rev.* **2014**, *4*, 33–39. [CrossRef]
32. Kang, J.M.; Hwang, H.U.; Lee, J.M.; Yun, Y.T.; Bae, B.C.; Jung, S.Y. A study on national cyber capability assessment methodology. *J. Kor. Inst. Info. Secur. Cryptol.* **2012**, *22*, 1039–1055.
33. Bae, S.; Park, S.; Kim, S.J. A study on the development for the national cybersecurity capability assessment criteria. *J. Kor. Inst. Info. Secur. Cryptol.* **2015**, *25*, 1293–1314. [CrossRef]
34. IMO. *Provisional Agenda for the 99th Session of the Maritime Safety Committee to Be Held from 16–25 May 2018*; MSC.99/1; International Maritime Organization: London, UK, 2017.
35. IMO. *Regulatory Scoping Exercise for the use of Maritime Autonomous Surface Ships (MASS)*; MSC.99/5; International Maritime Organization: London, UK, 2017.
36. IMO. *Maritime Cyber Risk Management in Safety Management Systems*; MSC.428(98) Resolution; International Maritime Organization: London, UK, 2017.
37. Hopcraft, R.; Martin, K.M. Effective maritime cybersecurity regulation—The case for a cyber code. *J. Indian Ocean Reg.* **2018**, *14*, 354–366. [CrossRef]
38. IMO. *Guidelines on Maritime Cyber Risk Management*; MSC-FAL.1/Circ.3 Annex; International Maritime Organization: London, UK, 2017.
39. IMO. *International Safety Management (ISM) Code with Guidelines for Its Implementation*, 5th ed.; International Maritime Organization: London, UK, 2018.
40. ISO/IEC. *International Standard 27001: Information Technology—Security Techniques—Information Security Management Systems—Requirements*; 2013 Standard; International Organization for Standardization: Geneva, Switzerland, 2013.
41. NIST. *Framework for Improving Critical Infrastructure Cybersecurity, 1.1 version*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2018.
42. IMO. *Interim Guidelines for MASS Trials*; MSC.1/Circ.1604; International Maritime Organization: London, UK, 2019.
43. Bernasconi, M.; Choirat, C.; Seri, R. The analytic hierarchy process and the theory of measurement. *Manag. Sci.* **2010**, *56*, 699–711. [CrossRef]
44. Saaty, T.L. *The Analytic Hierarchy Process: Planning, Priority Setting, Resources Allocation*; McGraw-Hill: London, UK, 1980.
45. Saaty, T.L. How to make a decision: The analytic hierarchy process. *Eur. J. Oper. Res.* **1990**, *48*, 9–26. [CrossRef]
46. Taherdoost, H. Decision making using the analytic hierarchy process (AHP): A step by step approach. *Econ. Manag. Syst.* **2017**, *2*, 244–246.
47. BV. *Rules on Cybersecurity for the Classification of Marine Units*, 2018 ed.; Bureau Veritas: Paris, France, 2018.
48. DEUTSCHE-FLAGGE. ISM Cybersecurity. Available online: https://www.deutsche-flagge.de/de/redaktion/dokumente/ism-rundschreiben/circ2018_4_2.pdf (accessed on 19 June 2019).

49. IALA. *Risk Management, IALA Guideline 1018*, 3rd ed.; International Association of Marine Aids to Navigation and Lighthouse Authorities: Saint-Germain-en-Laye, France, 2013.
50. IEC. *Risk Management—Risk Assessment Techniques*; IEC 21010:2009 Standard; International Electrotechnical Commission: Geneva, Switzerland, 2009.
51. KR. *Guidelines of Maritime Cybersecurity, 1.0 version*; Korean Register: Busan, South Korea, 2017.
52. Han, S.H. A practical approaches to decrease the consistency index in AHP. In Proceedings of the 5th SCIS & ISIS 2014, Kitakyushu, Japan, 3–6 December 2014; pp. 867–872.
53. Lee, J.G. A Study on Decision Factor of Residential Environments of NEW STAY Using the AHP. Master's Thesis, Graduate School of Real Estate Studies, Konkuk University, Seoul, Korea, 2015.
54. KASS. Project Detail. KASS (Korea Autonomous Surface Ship) Project. Available online: http://kassproject.org/en/info/projectdetail.php (accessed on 12 May 2021).
55. MGL. Maritime Safety Act. MGL (Ministry of Government Legislation). Available online: https://elaw.klri.re.kr/kor_service/lawView.do?hseq=49260&lang=ENG/ (accessed on 9 December 2020).
56. MGL. Enforcement Decree of the Maritime Safety Act. MGL (Ministry of Government Legislation). Available online: https://elaw.klri.re.kr/kor_service/lawView.do?hseq=53293&lang=ENG/ (accessed on 9 December 2020).
57. IMO. *The International Ship and Port Facility Security (ISPS) Code*, 2003 ed.; International Maritime Organization: London, UK, 2003.
58. IMO. *Measures to Enhance Maritime Security—Cyber Risk Management in Safety Management Systems*; MSC 101/4/4; International Maritime Organization: London, UK, 2019.
59. MGL. International Ship and Port Facility Security Act. MGL (Ministry of Government Legislation). Available online: https://elaw.klri.re.kr/kor_service/lawView.do?hseq=51649&lang=ENG/ (accessed on 9 December 2020).
60. MGL. Enforcement Decree of the International Ship and Port Facility Security Act. MGL (Ministry of Government Legislation). Available online: https://elaw.klri.re.kr/kor_service/lawView.do?hseq=49955&lang=ENG/ (accessed on 9 December 2020).