2022-10-20

Determining Maritime Cyber Security Dynamics and Development of Maritime Cyber Risk Check List for Ships

Kayisoglu, Gizem

22nd Annual General Assembly

IAMU AGA22

International Association of Maritime Universities

The 22nd Annual General Assembly

19th - 21st October 2022

BATUMI, GEORGIA

The International Association of Maritime Universities (IAMU) Student Session Proceedings

www.aga22-batumi.com

IAMU International Association of Maritime Universities

THE NIPPON FOUNDATION

Batumi State Maritime Academy

The International Association of Maritime Universities (IAMU) Student Session

Proceedings

Poti, Georgia
20th of October, 2022

22nd Annual General Assembly

IAMU AGA 22

19th – 21st October 2022

Program Editor

Associate Professor Nino Kurshubadze
Batumi State Maritime Academy, Georgia

"A publication of the International Association of Maritime Universities"

Determining Maritime Cyber Security Dynamics and Development of Maritime Cyber Risk Check List for Ships

Gizem Kayisoglu [1, *], Pelin Bolat [1] and Kimberly Tam [2]

[1] *Istanbul Technical University, Türkiye*
[2] *The University of Plymouth, United Kingdom*
[*] *Corresponding author: yukselg@itu.edu.tr; Tel.:* +90 531 454 93 03.

Abstract: The digitalization in maritime industry rises integration of the information and operational technologies on the vessels. The high level of connectivity and the rising of digitalization in maritime sector increase the cyber security issue. The systems of vessels can be exposed to errors of digital world and encounter some malicious attacks. At this point, cyber security in maritime sector is an important topic in terms of not only securing the systems, preventing the accidents, loss of life, and damage to the environment but also national security, and global economy. Accordingly, in the context of IAMU 2022 Research Project for Young Academic Staff, it is aimed to determine maritime cyber security dynamics based on informational technology (IT) and operational technology (OT) for ships, dynamics affecting any breaches in the scope of maritime cyber security in marine insurance, and liabilities, responsibilities, rules and enforcements in the scope of maritime law. Thus, it is aimed to develop maritime cyber risk check list for ships by performing maritime cyber risk management with the help of these dynamics in the project. In this context, in this paper, the issues of maritime cyber security on the perspective of maritime cyber risk and maritime cyber insurance and suggestions on solutions of them is only tried to be emerged for creating an infrastructure of the project.

Keywords: maritime cyber security; maritime cyber risk; maritime cyber insurance

1. Introduction

The high level of digitalization and connectivity in maritime sector make the cyber security issue come to the force. In particular, ships became connected to universal networks, incorporated complex digital industrial systems, and integrated with the information and operational technologies. The systems of vessels can be subject to errors of digital world and faced with some malicious attacks [1]. At this point, cyber security in maritime sector is an important topic not only with respect to the particular of securing the systems, preventing the accidents, loss of life, and damage to the environment but also with respect to national security, and global economy. Furthermore, a cyber-breach gives rise to financial loss, disruption in the business procedures, and damage to reputation. Against all of these dangers, a company wants to get rid of the incident quickly and secure itself to work normally again. For this purpose to be achieved, both the issue of ship protection systems against physical attack, the design of the systems and supporting process should be taken into consideration at first.

The cyber environment of ships contain interconnected networks of both Information Technology (IT) such as the computer-based systems, personal computers, tablet devices, laptops, routers, servers and switches, etc. and operational technology (OT) such as, control systems, actuators, sensors, radar, etc. The cyber space onboard provide services, information, business and social functions. Besides, personnel security, the insider threat from shore-based or shipboard, ship-owners, operators, stakeholders, procedures, process, and physical aspects are important assets for cyber security responsibility in maritime. Appropriate measures should be taken in the framework of these assets.

When the historical developments of cyber security in maritime are evaluated, a hierarchical improvement is observed and it has been noticed that the above-mentioned framework is specified at every stage of this development. After the 2010 Strategic Defense and Security Review made publication about cyber security as a top threat for national security, in the maritime sector, it has become a prominent issue [2]. In 2011, ENISA highlighted the low cyber security awareness for maritime sector and suggested some titles about cyber security in maritime for raising the awareness [3]. In 2016, International Maritime Organization (IMO) has issued a circular about Guidelines on maritime cyber risk management. As per this circular, cyber risks are appropriately addressed in the International Safety Management (ISM) Code until 1st of January 2021. With these

amendments, various guidelines relating with cyber security on board ships were issued by BIMCO, DNV-GL, CLIA, INTERMANAGER, INTERCARGO, INTERTANKO, OCIMF etc… [4], [5]. When the researches on the cyber security in maritime in the literature are analyzed, it is observed that the level of cyber security awareness in maritime is visibly high in 2018 and the maritime sector has passed the operation level for cyber security [6]. Cyber security risk assessment and management studies have shown up as of years 2019, 2020 and 2021 [7]–[11].

On the perspective of maritime cyber insurance , the researches are still limited in the literature [12]–[14]. According to existing insurance policies, there are only restricted clauses about cyber security in maritime. For example, cyber related risks are excluded in the hull and machinery insurance (H&M) policies by adding relevant clauses, such as Cyber Attack Exclusion Clause (CL380) [15]. Cyber-attacks, which are not related with terrorist attack or war are covered in the pool of Protection and Indemnity Insurance (P&I) with a limit of $30 million USD per ship [1].

Maritime cyber risk indicates the level of threat on a digital asset due to potential attacks caused by a malicious event, person, situation, or malware, and the level of corruption and loss of information or operating systems due to ship-related safety, security or operation error. Cyber security has an impact on every aspect of a maritime organization such as, logistics, shipping, supply chain, company process, transportation, etc... Thus, maritime cyber risk must be integrated into organizational risk management and decision making structures to ensure high-level cyber security in a maritime organization. Maritime cyber risks include operational risk, financial risk, legal risk such as regulations, partnerships, contract etc…In this respect, cyber insurance must be improved by the way of cyber risk management in various insurer types such as P&I club, hull & machinery insurance, transportation insurance or in a separate insurance policy.

At this point, the significance of this paper is to emerge with the issues of maritime cyber security on the perspective of maritime cyber risk and maritime cyber insurance and suggestions on solutions of them. Accordingly, in the context of IAMU 2022 Research Project for Young Academic Staff, it is aimed to determine maritime cyber security dynamics based on informational technology (IT) and operational technology (OT) for ships, dynamics affecting any breaches in the scope of maritime cyber security in marine insurance, and liabilities, responsibilities, rules and enforcements in the scope of maritime law. Thus, it is aimed to develop maritime cyber risk check list for ships by performing maritime cyber risk management with the help of these dynamics in the project.

2. Maritime Cyber Risk Management

2.1 Maritime Cyber Risks

In maritime transportation, cyber incidents have impact on cargo control, navigation, and other industrial and business processes by threating lives, property, and environment, and interrupting with business activity. For instance, control of emergency systems and temperature for refrigerated containers can be impacted by cyber attacks. On the other hand, maritime cyber disruptions can have impact on port operations such as, controlling traffic lights, raising a drawbridge, scheduling trucks, and controlling, valves, pumps and pipelines for transfer of liquid cargo and fuel to ships. A dynamic positioning system used in the offshore oil sector for impeccable navigation control is infected with a malware according to a cyber incident report [16]. In another example, a smart phone of a crew member, which is infected with malware, is plugged into ECDIS and it has deleted all charts, therefore a two-day delay has occurred. In another incident, cyber attack is performed for drug smuggling through infiltrating to a European container terminal's tracking system by organized crime [12].

According to Fairplay and BIMCO cyber security survey [17], phishing, spear phishing, and malware are the most common attacks in maritime. The results of these type of attacks are specified in five different categories as business interruption and theft of financial assets, personal or commercial data theft, denial of service or failure to meet contractual commitments, bankruptcy, and third party liabilities, which means passing on the problem to the commercial counterparties. These risks bring along cost loss such as legal expenses, cost of Forensics, Ransom payment, data restoration, business interruption and additional operating costs. At this point, cyber resilience constitutes a critical issue. For providing cyber resilience, cyber security and cyber insurance should be guaranteed as specific to any field [12].

According to Tonn et al [14], there is cyber risk assessment, security measures, mitigations and insurance which have already being adopted to maritime transportation infrastructures at the various level, however, they are inadequate in general. There is not effective tools currently for infrastructure managers to evaluate and manage cyber risk rigorously.

Dadiani [18] presented a dissertation about exist attitudes of marine insurance related cyber security and conducted a comparative analysis between the cyber-risks and the traditional marine risks and to give opinion about how marine insurance can deal with the cyber-attacks. Tucci [19] organized a panel about legal necessaries for maritime crew and managers to report cyber incidents and counter pose certain cyber standards for information sharing, risk management practices, and need of maritime cyber insurance. Soyer [20] emphasized the particular that maritime stakeholders should understand the nature and scope of available cyber risks policies and the relavance between such policies and traditional insurance policies. Cooper [21] provided suggestions in the book about how inadequate cyber safety measures on board a ship or shore side might impact the civil liability of a vessel and its owners or operators in the event of an accident. Hong and Hoang [22] aimed to (i) explore traditional marine insurances at risk and liability perspectives, (ii) analyze the nature of cyber risk and liability, which should be covered by maritime cyber insurance, (iii) analyze the marine insurance law and traditional marine insurance clauses/rules to define the legal barriers/shortages/conflicts of maritime cyber insurance, (iv) analyze the necessary required conditions to implement maritime cyber insurance. According to these limited studies, the main output revealed is to assess existing studies about cyber insurance policy and to suggest the integration of them to maritime field.

Only, Farao et al [23] created a framework, called as SECONDO, to help institutions for deciding related to cyber-insurance and cyber security investments by applying and integrating a serial of software parts. SECONDO involves three different modes as: (i) cyber-physical risk assessment and continuous monitoring; (ii) investment-driven optimized cyber-physical risk control; and (iii) block chain-enabled cyber-insurance contract preparation and maintenance. SECONDO provide to insurers for attending to the active cyber-physical risk management of a maritime company in order to decreasing risk of their insured.

2.2 Method for Maritime Cyber Risk Management

While there is a several potential cyber losses, different approaches exist for mitigating these losses. The approaches involve two different methods in general. The first one is design method that is aimed to develop system activities and architecture. The other one is operational methods which include alterations regarding trade operations [24], [25]. There are also some approaches for managing cyber risks, such as security software and investments in the cyber workforce. On the other hand, for mitigating cyber risk, protective technical measures such as software encryption, firewalls, system separation, virus detection, can be also used as well as developed theoretical approaches. Organizational measures for cyber risk can be categorized as procedural measures involving operational and management systems, structural measures including hardware and software, and responsive measures which means damage and response management when an attack or incident is found out [26]. Institutions must recognize that mentioned measures cannot prevent cyber risk as whole and they must manage properly residual risks and should use cyber insurance for transferring the risks to third parties [27].

The risk management approach, which is stipulated in “The Guidelines on Cyber Security Onboard Ships”, is proposed for improving maritime cyber risk assessment and creating a background for maritime cyber insurance policy [4]. It is developed with the aim to explain why and how cyber risks should be managed in a shipping context. It includes pro-documents, process, components, and responsible parties for risk assessment. Besides, in searching for a standardized approach to compliance, it is seen that the ISO27000 family of standards are suitable for ship owners and other stakeholders in the maritime sectors [29]. They can be considered as a guideline to make high the perception for not only on-board but also on-shore, adopting compliance for cyber risk management in maritime and certifying an Information Security Management System (ISMS).

Accordingly, the steps of the proposed cyber risk management approach for maritime sector based on “The Guidelines on Cyber Security Onboard Ships” are as in Figure 1. According to Figure 1, the holistic and equational approach which is based on above-mentioned method is proposed. It includes the detail technique special for each step. Considering risk assessment methods, modelling, mitigations, and solutions in Figure 1,

residual risk can be calculated and the result constitutes a base for maritime cyber insurance [30].

Idendificatipn process	Threat	Vulnerability	Likelihood (1-5 Scale)	Impact Assessment(1-5 Scale)	Initial Risk (1-25 Scale)	Bow Tie (Mitigations)	Residual Risk
• identify the systems, assets, data, and capabilities that, if disrupted, could pose risks to the ship's operations in the scope of maritime cyber security • identify the roles and responsibilitie s of users, key personnel, and management both ashore and onboard in the scope of maritime cyber security	• Cyber incident scenarious for maritime are developed to understand the impact of emerging maritime cyber risks on marine company. • The scenarious are developed by examining the literature, assessing the real incidents, and consulting IT,OT experts and marine insurers	• The vulnerabilities of the determined cyber security incidents scenarios are idendified by examining the literature and consulting IT,OT experts and marine insurers	• Quantifying the likelihood would be substantiated by access to shipping-specific industry-wide threat intelligence based on incident reports • Quantifying the likelihood would be substantiated by looking to other sectors than shipping, as threat actors frequently repurpose techniques previously used to attack one sector to target another sector. • Quantifying the likelihood would be substantiated by examining the literature and consulting IT,OT experts and marine insurers	• The confidentiality , integrity, and availability (CIA) model provides a framework for assessing the impact of loss of confidentiality , integrity and availability. • The ranking scale can be used by assessing the the loss of confidentiality integrity, or availability could be expected to have a limited, substantial, and severe or catastrophic adverse effect on company and ship, organisationa assets, or individuals.	• Risk=Likeliho od*Impact	• idendify technical and procedural measures to protect against a cyber incident, timely detection of incidents and ensure continuity of operations • Consider defence in depht and in breadth • Consider detection, blocking and alert systems	• New likelihood or impact value is calculated according to mitigations. • Residual Risk=New Likelihood*N ew Impact

Figure 1. Maritime cyber risk management.

3. Maritime Cyber Insurance

Any business of any size, which relies on IT infrastructure to some extent, is subject to the risks of income loss, damage management, business interruption, damage repair, and potentially reputational damage when IT systems or equipment get interrupted. Cyber insurance enables organizations to make over some of the economic risk related with cyber incidents to an insurer. In this way, trade liability such as first-part costs as well as losses of damages, loss of data from networks and IT systems in the widest context take place in cyber insurance. It is considered as significant part of cyber risk management in institutions [31], [32]. Accordingly, many insurers work with technical assistance as part of an insurance policy for managing a breach and improving cyber security approaches within an organization. These assistance serves in the scope of initial evaluations of cyber security vulnerabilities and access to consultancies to improve their overall cyber security posture, to a range of services to support companies in the event of an incident [31].

As for insurance and infrastructure field in maritime, Tonn et al. [14] made an interview regarding cyber risk and cyber insurance for maritime transportation infrastructure with insurers and infrastructure managers. Infrastructure managers stated that there is uncertainty and unknown item in the cyber risk, therefore, they have some concern about cyber issue in maritime. Therefore, insurers are able to present cyber insurance policies with restricted contents and limits. As a result, insurers can be hard to improve an extensive scope cyber insurance, which is desired by managers, due to the unknown nature of cyber risk, lack of actuarial data, improving and changing continually technology [34, 35]

There are some model clauses for limiting and specifying cyber associated with liability such as BIMCO's "Cyber Security Clause 2019", which can also support charter parties. The BIMCO clause constitutes liabilities about performing and monitoring systems, procedures, and plans both with regards to pre and post cyber attack, putting in reasonable efforts to be certain third parties offering services assorting with these procedure, plans, and systems, sharing information related with effects cyber incidents. The JCC "Cyber Attack Exclusion Clause

and Write-Back" can be given another example as model clauses that excludes liability caused by cyber incidents. According to this clause, the insured is required to show proof the purpose of the cyber attack which was to damage to the insured's property. Similarly, Electronic Data Endorsement C which is named as NMA2914 exclude the insurance of loss, destruction, damage, erasure , distortion, alteration or corruption of electronic data from any cause. Therefore, there is a gap regarding cyber insurance especially with regards to maritime sector [36].

The clauses, insurances, and endorsement, which cause a gap to occur in maritime cyber insurance area, are as following [30]: CL380 - Institute Cyber Attack Exclusion Clause, LMA5402 - Marine Cyber Exclusion Clause, LMA5403 - Marine Cyber Endorsement, Protection & Indemnity insurance.

In the context of insurance dynamics on maritime cyber security, analyzing enterprise risks of ship to shore interconnectivity, these can be divided into two parts as IT and OT. IT assets include IT networks, accounts, e-mail, admin, spares management and sourcing, planned maintenance, notices of readiness, bills of lading, charter parties, cargo booking systems and stowage plans. OT assets involve automatic information system (AIS), global positioning system (GPS), supervisory control and data acquisition (SCADA) system, ECDIS, remote support for machinery, cargo control and distributed control systems (DCSs). These industrial control systems are highly integrated each other and they communicate with each other via internet, wireless, and other media [34], [37]. While the impact of IT damages is on ability to perform, financials, and reputation, OT disservices affect life, property, and environment along with items of IT loss. There are various threats that are triggering these losses. For instance, ever greater integration shore to ship cause to converging OT and IT technologies. Besides, improvement of inter-connectivity leads to viruses being transmitted faster. Malware is so much easily programmed with improved technology. Therefore, the change in technology is fast and in some respect it is beneficial but also disruptive. Cyber attacks are performed by political or ideological activists, nation states, cyber terrorists and criminals, disgruntled or maliciously-minded employees, organized crime seeking to acquire and exploit stolen data [25]. These attacks can lead to damage equipment, loss of service that cause probably accidents [37].

For this reasons, maritime cyber insurance (MCI) is important for sharing risk and withdrawing the loss amount. MCI includes ship owners and operators, the entirety of their business on land and at sea, the financial losses suffered following a cyber or cybercrime attack, the necessary stretch from standard cyber cover to accommodate "cyber-enabled fraud", and access to responsive service in event of the discovery of an attack.

Table 1. Maritime cyber insurance.

The key loss for MCI	Cybercrime coverage of MCI	The headline cost coverage	MCI key features
Network Compromise– unauthorized access to or misuse of an insured's computer or communication system	Cyber Theft – transfer, corruption or loss of money or financial assets arising from a network compromise	Digital Assets – indemnification of costs associated with replacing or restoring digital assets to the state they were in prior to a network compromise or other trigger	Insured(s) – Ship owners or operators
System Failure – unintentional or unplanned outage of an insured's computer or communication system	Social Engineering – plausible instruction to deliver funds purporting to come from a legitimate source	Breach Response Costs – legal fees and costs associated with compliance with legislation, notification of effected individuals +P R expenses	Coverage granted for owned or chartered fleets, including in-house ship management companies
Data Breach – unauthorized acquisition of data by a third party, including by and employee that compromises confidentiality or integrity of personal data or business information		IT Security & Forensics – costs incurred in investigating the source, scope and impact of an insured peril: including tackling malware, restoration of data, impact of social engineering, remediation of a failure of computer security (Key: urgency in the delivery of external expertise and service, integrated with insured's own crisis management resource)	Maximum Policy Limit(s) for any one event and in the annual aggregate. For instance Cyber USD 25M "Cyber Crime" sub-limit USD 500K
Extortion Demand – threat to corrupt an insured's computer, etc, to introduce malware, or execute a denial of service attack		Extortion Demands – reimbursement, where permitted, of extortion payments	Policy Deductibles starting from such an amount of USD 2500 for the defined insureds

Material Degradation – complete or partial interruption or degradation in service or failure of a computer or communication system	Business Interruption – reimbursement of enterprise-wide loss of profit and additional operational expenses suffered during the period of restoration following the operation of a material degradation or one of the key triggers (Cover provided without the need for PD to be demonstrated (Not Cyber Loss of Hire))	Business Interruption Time Retention such as minimum 8 hours
	Regulatory – reimbursement of defense costs and, where permitted, fines	Subject to the satisfactory completion of a short proposal form
	Third Party Liability – payment on behalf of the insured damages and defense costs for which the insured becomes legally liable to third parties. Typically for failure to protect information or to have negligently permitted the transmission of a virus to a third party. Excluding liabilities normally recoverable from a P&I Club.	The insurer
		Cyber Response Consultants
		Excluding claims categorized as property damage or death or bodily injury

To provide a very rough non-binding pricing indication in order to generate client interest all we need to know is the following:

•The client's fleet list to establish vessel particulars

•The company's annual turnover

Underwriting information are vessel type(s), number of vessels in the fleet, information submitted regarding the owner's self-assessment of their degree of readiness with regard to cyber security, including commentary regarding compliance with MSC.428(98) and TMSA3 if applicable.

On the other hand, in general, damage to any physical or tangible property, including hardware, satellite, electrical or mechanical failures, any actual or alleged breach of a third party's intellectual property right by an insured, including any patent or the misappropriation, theft copying, display or any publication of trade secrets, illegal programs, any trading losses resulting from the fluctuation of any stock, share, security or currency on any financial markets or exchanges and the monetary value of any electronically fund transfers, transactions by or on behalf of the insured, which are lost and not being a direct result of a network security breach of the insured are covered by maritime cyber insurance policy.

4. Conclusion

Cyber security is a critical problem comprising all stakeholders in the maritime sector. It is significant for business to review and to adopt the systems of cyber space and their measures when considering the insurers offer restricted insurance policy coverage for the loss that derived from a cyberattack. Hence, they can ensure to detect, reduce and prevent the cyber risks, count suitable clauses in insurance policy, and transfer their responsibilities. There are some encouragement and recommendation of important organizations in maritime sector, specifically, IMO 2021 and its published guideline create a standard path for reviewing and setting their safety management system focusing on cyber security. At this point, the term of cyber-seaworthiness comes out for vessels. For managing cyber-seaworthiness, a safety management system, an information technology asset, data, a data controller system should be integrated with each other and managed effectively.

In this context, firstly, the above mentioned sophisticate cyber risk assessment, mitigation, management, and insurance for maritime transportation system are needed to achieve cyber incident data and to develop cyber incident models. For developing systematic risk assessment tool and global practical marine cyber insurance policy, historic cyber incident data should be recorded and cyber information sharing system should be developed. Hence, managers can practice the cyber risk models which can be developed with data availability and records and they can understand the target of the risks. Accordingly, insurers can calculate the cyber risks

thanks to these availabilities and develops global marine cyber insurance policy. Understanding perceived probabilities and impacts of cyber-attacks along with experiences and perceptions of mitigation measures and insurance needs can facilitate the design of strategies to overcome these biases and improve the preparedness of infrastructure organizations for cyber-attacks. Lastly, research is needed on cyber insurance for maritime transportation infrastructure systems, to support new and more robust cyber insurance products that meet the evolving needs and demands of infrastructure systems. This research should draw from the previously mentioned research needs on metrics and modeling of cyber risk for insurance rating purposes and on cognitive biases and risk perceptions. Research can lead to creative insurance solutions to encourage the purchase of cyber insurance and the adoption of technically effective and cost effective cyber risk mitigation strategies by transportation infrastructure managers

In all this context, the main learning objectives of this paper are (i) to present the importance and essence of maritime cyber security as part of a holistic approach; (ii) to show the potential impact of cyber-attacks on board a vessel and risk assessment; (iii) to demonstrate the significant impacts of a cyber incident on the maritime environment; (iv) to identify the dynamics affecting any breaches in the scope of maritime cyber security in marine insurance. These dynamics will emerge an infrastructure for developing maritime cyber check list for ships in the IAMU 2022 Research Project for Young Academic Staff.

5. Cover Letter

Authors confirm that this paper is original and being submitted for publication in the 22nd IAMUC Proceedings.

Acknowledgements

This study is supported and funding by IAMU 2022 Research Project for Young Academic Staff [REF: Young Academic Staff in FY2022]. The materials and data in this publication have been obtained through the support of the International Association of Maritime Universities (IAMU) and The Nippon Foundation in Japan.

References

[1] Lagouvardou S (2018) Maritime cyber security: concepts, problems and models.

[2] Fitton O, Prince D, Germond B et al (2015) The future of maritime cyber security.

[3] ENISA (2011) Analysis of cyber security aspects in the maritime sector.

[4] ICS and other organizations (2016) The guidelines on cyber security onboard ships.

[5] Standard Club (2020) Maritime cyber risk management guidelines. Standard Club. https://www.standard-club.com/fileadmin/uploads/standardclub/Documents/Import/publications/loss-prevention-industry-expertise-handouts/3365323-sc_ie_cyber_risks_20201117_final.pdf. Accessed 1 January 2022

[6] Bolat P and Kayisoglu G (2019) Antecedents and consequences of cybersecurity awareness: a case study for Turkish maritime sector. J. ETA Marit. Sci. 7 (4): 344–360. doi: 10.5505/jems.2019.85057.

[7] Jain A and President V (2017) Modelling cyber risk. 1–39.

[8] Svilicic B, Rudan I, Jugović A et al (2019) A study on cyber security threats in a shipboard integrated navigational system. J. Mar. Sci. Eng. 7 (10): 364. doi: 10.3390/jmse7100364.

[9] Svilicic B, Kamahara J, Celic J et al (2019) Assessing ship cyber risks: a framework and case study of ECDIS security. WMU J. Marit. Aff. 18 (3): 509–520. doi: 10.1007/s13437-019-00183-x.

[10] Svilicic B, Kamahara J, Rooks M et al (2019) Maritime cyber risk management: an experimental ship assessment. J. Navig. 72 (5): 1108–1120. doi: 10.1017/S0373463318001157.

[11] Tam K and Jones K (2019) Cyber-SHIP: Developing next generation maritime cyber research capabilities.

[12] Cromar Coverholder at Lloyds (2016) Maritime cyber insurance.

[13] ENISA (2016) Cyber insurance: recent advances, good practices and challenges.

[14] Tonn G, Kesan J, Zhang L et al (2019) Cyber risk and insurance for transportation infrastructure. Transp. Policy, 79: 103–114. doi: https://doi.org/10.1016/j.tranpol.2019.04.019.

[15] Cl.380 (2003) Specific cyber-attack exclusion clause.

[16] Cadet O and Rinnan A (2016) Who said that DP does not rhyme with cybersecurity?, Dynamic Positioning Conference, 1–22.

[17] IHS Market (2018) Maritime cyber survey 2018.

[18] Dadiani D (2018) The maritime commons : digital repository of the world cyber-security and marine insurance. World Maritime University.

[19] Tucci A. E (2017) Panel on legal and insurance issues in maritime cyber. Proceedings of the 2017 Maritime Risk Symposium: The Global Maritime Cybersecurity Challenge Tiffin University, 7–11.

[20] Soyer B (2020) Cyber risks insurance in the maritime sector: growing pains and legal problems in maritime law in motion. World Maritime University, 627–642.

[21] Cooper S (2018) Cyber risk, liabilities and insurance in the marine sector. Marketing and Managing Tourism Destinations, Informa Law from Routledge.

[22] Hong T and Hoang H (2020) Cyber security risks and liabilities in modern marine insurance. World Maritime University.

[23] Farao A et al (2020) SECONDO: a platform for cybersecurity investments and cyber insurance decisions. International Conference on Trust and Privacy in Digital Business, TrustBus 2020: Trust, Privacy and Security in Digital Business, 65–74.

[24] Gisladottir V, Ganin A. A, Keisler, J. M et al (2017) Resilience of cyber systems with over- and underregulation. Risk Anal., 37 (9): 1644–1651. doi: 10.1111/risa.12729.

[25] Nogal M and O'Connor A (2017) Cyber-transportation resilience. Context and methodological framework. Resilience and Risk, NATO Science for Peace and Security Series C: Environmental Security, 415–426.

[26] Paté-Cornell M. Elisabet, Kuypers M, Smith M et al (2018) Cyber risk management for critical infrastructure: a risk analysis model and three case studies. Risk Anal., 38 (2): 226–241. doi: 10.1111/risa.12844.

[27] Kesan J. P. and Zhang L (2020) Analysis of cyber incident categories based on losses. ACM Trans. Manag. Inf. Syst., 11 (4): 1–28. doi: 10.1145/3418288.

[28] Molisani E (2021) Insurance and cyber risk a focus on cyber. MR International Lawyers. https://slidetodoc.com/insurance-and-cyber-risk-a-focus-on-cyber/. Accessed 5 January 2022

[29] ISO27001 (2014) ISO 27001 Information security management system. International Certification and Auditing Co. Lmt. https://belgelendirme.ctr.com.tr/iso-27001.html. Accessed 7 January 2022

[30] Howden (2020) Marine cyber risk and insurance. Howden Insurance Brokers. https://www.howdengroup.com/ae-en/marine-cyber-risk-and-insurance-howden. Accessed 7 January 2022

[31] Gordon L. A, Loeb M. P, Sohail T (2003) A framework for using insurance for cyber-risk management. Commun. ACM, 46 (3): 81–85.

[32] ABI (2021) Cyber risk insurance. The Association of British Insurers. https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/business-insurance/cyber-risk-insurance/%0A%0A. Accessed 10 January 2022

[33] Kyriakides H (2021) Marine cyberattacks: analysis of liability and IMO 2021. The Legal 500, 2021. https://www.legal500.com/developments/thought-leadership/marine-cyberattacks-analysis-of-liability-and-imo-2021/. Accessed 10 January 2022

[34] Ezell B. C, Michael Robinson R, Foytik P et al (2013) Cyber risk to transportation, industrial control systems, and traffic signal controllers. Environ. Syst. Decis., 33 (4): 508–516. doi: 10.1007/s10669-013-9481-2.

[35] Toregas C and Zahn N (2014) Insurance for cyber-attacks: The issue of setting premiums in context.

[36] SANS (2016) Bridging the insurance/InfoSec gap: The SANS 2016 cyber insurance survey. The SANS Institute, 2016. https://www.advisenltd.com/2016/06/21/bridging-the-insuranceinfosec-gap-the-sans-2016-cyber-insurance-survey/. Accessed 12 January 2022

[37] Ralston P. A. S, Graham J. H, Hieb J. L (2007) Cyber security risk assessment for SCADA and DCS networks. ISA Trans., 46 (4): 583–594. doi: 10.1016/j.isatra.2007.04.003.

IAMU
International Association of Maritime Universities

www.aga22-batumi.com

BATUMI STATE MARITIME ACADEMY