Department of Informatics and Computer Engineering

Cybersecurity

Thesis title:

Cybersecurity in Maritime

Zacharias Michalakis

Supervisor Professor: Konstantinos Mavrommatis

Athens, January 2023

Πανεπιστήμιο Δυτικής Αττικής
Σχολή Μηχανικών
Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών
Πρόγραμμα Μεταπτυχιακών Σπουδών: ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Cybersecurity in Maritime

Ζαχαρίας Μιχαλάκης

A.M. cscyb2020

Η μεταπτυχιακή διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι Εξεταστική Επιτροπή συμπεριλαμβανομένου και του Εισηγητή:

Konstantinos Mavrommatis Digitally signed by Konstantinos Mavrommatis Date: 2023.02.10 12:52:33 +02'00'	Panagiotis Giannakopoulos Digitally signed by Panagiotis Giannakopoulos Date: 2023.03.09 12:37:07 +02'00'	STEFANOS GKRITZALIS 12.02.2023 21:37
Κωνσταντίνος Μαυρομμάτης	Παναγιώτης Γιαννακόπουλος	Στέφανος Γκρίτζαλης
Επιβλέπων Καθηγητής	Καθηγητής	Καθηγητής

Ημερομηνία εξέτασης: 21/1/2023

ABSTRACT

The dangers in cyberspace are a new reality that during the last years is threatening the shipping sector as well. In earlier times, cyberspace was not considered at all by the shipping industry as there were other priorities that had to be addressed. Cyber risk management refers to the process of identifying, analyzing, evaluating and reporting a cyber threat. In the light of the unprecedented situation that the shipping industry is experiencing with the ever-increasing trend of cyber attacks, the international shipping community is in constant vigilance for the issuance of guidelines, recommendations and instructions, which will be the basis for future international treaties governing the issue of cyber security. It is therefore appropriate to note the first impacts of the legislation on this new problem and, if necessary, at any appropriate time to make any new legislative interventions and to be able to correct incorrect texts in a timely manner. It is important that every ship owner to be prepared for a cyber attack because it is not a science fiction scenario. Only by having this mentality, but also securing the cooperation of all stakeholders of the supply chain, the shipping industry will at least limit this issue to a significant degree. It is recommended that a shipping company first conduct a potential threat assessment that may occur. This should be followed by an evaluation of the systems and on - board procedures for mapping robustness and addressing the current threat level. The result of the company Risk Assessment and the subsequent strategy for cyber security should be the reduction of cyber threats.

Table of Content

LIST OF FIGURES

INTRODUCTION

Until recently there was no legislation that mentions concerns regarding cybersecurity in the shipping industry. In 2017 the International Maritime Organization (IMO) of the Maritime Safety Committee (MSC) proposed a management plan for marine cyber threats due to the increased number of cyber attacks targeting the shipping industry.[1]

The IMO is an international organization that was created to addressing international issues related to the shipping and shipbuilding industry. The guideline of this organization for addressing cyber security risks mention the following vulnerable elements:[2]

- shipping management

- cargo management

- passenger management

- engine and communications systems

The IMO plan adopts the effective management framework composed by NIST (National Institute of Standards and Technology) for cybersecurity with the operation of the five steps: recognition, protection, detection, response and recovery.[3]

The implementation of the GDPR in May 2018 had a significant impact on shipping companies, as they maintain a lot of personal data, such as email addresses, information of the crew or passengers. This data often needs to be transferred globally. As with other types of businesses, the GDPR obliges shipping companies to make an impact assessments on personal privacy at all times when there is an increased risk of breach, as well as to report within 72

[1] Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems.

[2] Mraković, I., & Vojinović, R. (2019). Maritime cyber security analysis–How to reduce threats?.

[3] Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems.

hours any incident of violation so that they can react promptly and effectively to a potential cyber attack.[4]

In the same period a lesser known European Union (EU) Directive emerged with equally significant consequences for the shipping industry. The European Network and Information Security Directive (NIS) requires that the "Large service providers", such as major ports and sea transport services in the EU, to prove that they have received adequate and necessary measures to manage cyber risks.[5]

Though challenges in today's cyber domain have led to denial of services and, thus, to a disruption in the supply chain, there are still no global guidelines regarding maritime security.[6] According to the survey by Jones Walker LLP (2018), the majority of small and medium-sized shipping companies do not have cybersecurity systems and are exposed to the dangers of cyberspace.[7] The biggest problem however (besides the incomplete of appropriate legislation) is the human factor. There is generally a difficulty in a deep understanding from behalf of the individuals within the shipping industry what exactly cyber attacks are and what their consequences are.[8]

Often, the fact that some crew members have minimal or even no knowledge of the subject, the mishandling of some system processes being results to exposure and vulnerability to cyber attacks. Thus, staff awareness plays a key role in the smooth running of the business.[9] According to the survey by Jones Walker LLP (2018), the companies that participated it was shown that all major shipping companies provide training programs for employees regarding the issue of cyber attacks.[10]

[4] Mraković, I., & Vojinović, R. (2019). Maritime cyber security analysis–How to reduce threats?.

[5] Hayes, C. R. (2016). *Maritime cybersecurity: the future of national security*

[6] Hayes, C. R. (2016). *Maritime cybersecurity: the future of national security*

[7] Lee, A. & Wogan, H. (2018). Jones Walker LLP Maritime Cybersecurity Survey.

[8] Miranda Silgado, D. (2018). Cyber-attacks: a digital threat reality affecting the maritime industry.

[9] Mraković, I., & Vojinović, R. (2019). Maritime cyber security analysis–How to reduce threats?.

[10] Lee, A. & Wogan, H. (2018). Jones Walker LLP Maritime Cybersecurity Survey.

This thesis is divided into seven Chapters. In the first Chapter some necessary definitions are provided. In the second Chapter, the issue of cyber security in shipping will be discussed. In the third Chapter, some recent cases of cyber attacks are given. In the fourth Chapter, the vulnerable systems on a ship are mentioned. In the fifth Chapter, cyber threats are discussed. In the sixth Chapter, there is an overview of ships network structure. In the seventh Chapter, the best cyber security practices are mentioned. After that, there are some conclusions based on the information that was provided. The thesis concludes with some recommendations and some areas for future research.

1. DEFINITIONS

It was deemed appropriate to provide some necessary definition on key terms that are going to be mentioned in this paper.

Maritime Cyber Risk is the case when a technological asset may be threatened and will possibly result in different kinds of malfunctions for the ship's or shipping company's safety, as a consequence of corruption, loss or breach of information or systems.[11]

Cyber risk management refers to the process of identifying, analyzing, evaluating and reporting a cyber threat. When this risk is accepted, or avoided, or its transferred or reduced to a level where it is considered acceptable, based on the costs and benefits of the actions taken by managers or ship owners.[12]

Malware falls under the category of cyber attacks and it comes in the form of software. Malware includes cryptominers, viruses, ransomware, worms and spyware. Its objective is to steal data, espionage and interruption of a service. Web Protocols and e-mail Protocols are the most common carriers used to spread malware software. However, by exploiting the vulnerabilities of a system, some malware are able to spread even further within a computer network.[13]

The maritime sector has not established a common ***"maritime cybersecurity"*** definition. This paper will utilize the definition found in the Merriam-Webster Dictionary: “measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.” (Merriam-Webster Dictionary). Therefore, cybersecurity can be understood as all the necessary measures that have to be taken in order to shield network and IT equipment on a ship, terminal, port, or electronic communication network.[14]

[11] www.imo.org

[12] www.imo.org

[13] Svilicic, B., Kamahara, J., Celic, J., & Bolmsten, J. (2019). Assessing ship cyber risks: A framework and case study of ECDIS security.

[14] Chang, C. H., Wenming, S., Wei, Z., Changki, P., & Kontovas, C. A. (2019, November). Evaluating cybersecurity risks in the maritime industry: a literature review.

A ***cyber attack*** refers to an effort or attempt to sabotage or obtain access into a certain computer or electronic system.[15] The targets of cyber attacks are the same that were described in above paragraph.

Maritime domain includes all sections, areas and parts that are close to or have anything to do with a sea or ocean. It also involves any activities or tasks, personnel, building and ships.[16]

Data breach is a form of a cyber security situation where information can be accessed without prior authorization, usually with malicious intent, resulting in possible loss or misuse of this information. It also includes "human error" that occurs often in the configuration and development of certain services and systems and can lead to unintentional data exposure. In many cases, companies or organizations are unaware that there is a data breach in their environment due to the complexity of the attack and sometimes due to lack of visibility and classification of system information. According to Literature, it takes about 206 days to detect a data breach in one organization. Thus, it takes a lot of time to restore and recover the data and return a system to normal operating level.[17]

Identity theft or identity fraud is the illegal use of the staff's Personal Identifiable Information (PII) by a fraud, in his attempt to imitate the person in question and obtain financial advantage and other benefits.[18]

2. CYBER SECURITY IN SHIPPING

2.1. Onboard cyber security

The "Guidelines on Maritime Cyber Risk Management" in section 4 refers users who are looking for additional and more detailed guidelines for

[15] Dictionary.com
[16] Guard, U. C. (2005). National Plan to achieve Maritime Domain Awareness.
[17] Trautman, L. J., & Ormerod, P. C. (2016). Corporate directors' and officers' cybersecurity standard of care: The Yahoo data breach.
[18] Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks.

cyber risk management, to additional manuals to delve deeper into that issue. A very useful guide is “The Guidelines on Cyber Security Onboard Ships”.[19]

The largest shipping organizations and institutions around the globe joined forces and reissued in 2017 the 3rd edition of “The Guidelines on Cyber Security Onboard Ships”, which always follows the instructions of the IMO. Its purpose is, by analyzing all the data and providing its readers with a complete picture of what exactly the danger are in cyberspace, to help companies develop more suitable cyber risk management. The “Guidelines on Cyber Security Onboard Ships”, which were warmly welcomed by the IMO, ship owners and experts mainly refers to the way cyber risks are managed on ships. The guidelines given in this text are of advisory nature and in no case is one obliged to embrace and comply with them.[20]

The whole guide is based on the proper development, implementation and maintenance of cyber risk management, which is the current issue that concerns companies. For this reason, in the first pages this guide outlines the phases that are needed in order to achieve more comprehensive cyber risk management. According to the guide the steps are the following:[21]

1) identification of risks

2) identification of vulnerabilities

3) assessment of exposure

4) creating protecting and supporting measures

5) creation of plans for minimizing cyber risk to a potential threat

6) planning a response and recovery from an event

[19] BIMCO. (2016). *The Guidelines on Cyber Security Onboard Ships*.
[20] BIMCO. (2016). *The Guidelines on Cyber Security Onboard Ships*.
[21] Chang, C. H., Wenming, S., Wei, Z., Changki, P., & Kontovas, C. A. (2019, November). Evaluating cybersecurity risks in the maritime industry: a literature review

What makes "The Guidelines on Cyber Security Onboard Ships" a really useful tool for anyone who wants to understand the complex issue of cyber attacks is that it identifies the following:[22]

- the types of cyber attacks

- the types of perpetrators and their motives

- the systems they can be easily breached by a cyber threat and finally,

- it names the goals of a cyber attack while identifying the damage and losses it can inflict

This information can also be very useful at sea insurance for proper risk assessment.[23]

Finally, "The Guidelines on Cyber Security Onboard Ships" has great value for another reason, it is the first text written by institutions representing those involved in shipping on a professional level. It therefore shows how a company of the shipping industry has to react in the face of these risks.

On October 2020 the International Chamber of Shipping (ICS) and BIMCO in collaboration with Witherby published the “Cyber Security Workbook for On Board Ship Use ”, as a more updated version of the previous manual. The digital revolution and the targeting of ships by hackers has called for the need for crews to deeply comprehend what the dangers in cyberspace are, but also how and at what point in time a cyber attack can take place. Therefore, this guide was designed as a support tool, to provide the master, the officers, the security officer and the other members of the crew, the practical skills for identifying hazards and protecting the vulnerable ship systems. It also shows what is the best way to detect, response and recover in case a cyber attack occurs. The "Cyber Security Workbook for On Board Ship Use” aims to be a

[22] Tusher, H. M., Munim, Z. H., Notteboom, T. E., Kim, T. E., & Nazir, S. (2022). Cyber security risk assessment in autonomous shipping.

[23] Mraković, I., & Vojinović, R. (2019). Maritime cyber security analysis–How to reduce threats?. *Transactions on maritime science*, *8*(01), 132-139.

useful, practical and an understandable guide for the entire shipping community.[24]

2.2. Legislation and guidelines

In the light of the unprecedented situation that the shipping industry is experiencing with the ever-increasing trend of cyber attacks, the international shipping community is in constant vigilance for the issuance of guidelines, recommendations and instructions, which will be the basis for future international treaties governing the issue of cyber security. After all, as expected, the current situation, the conditions that are constantly changing, the new data that emerge, the perpetual threat of cyber attacks and the questions that arise as to how address the need, call for an international and united front to deal with this problem.

2.2.1. IMO - MSC

The IMO has issued guidelines which are relevant to "The Guidelines on Cyber Security Onboard Ships" and are contained in MSCFAL.1 / Circ.3 for maritime management and cybersecurity. The guidelines provide high recommendations on cyberspace management in shipping in order to secure the shipping industry against new and existing cyber threats. These guidelines provide all the required means that allow effective cyberspace management. Recommendations can be incorporated into existing risk management procedures and complement practices of security management already established by the IMO.[25]

The Maritime Safety Committee approved on June 16, 2017 the MSC.428_ (98). The resolution states that a security management system (SMS) has to consider the goals and necessities of the ISM code. Thus, it promotes proper cyber threat management encourages on behalf of a

[24] Mraković, I., & Vojinović, R. (2020). Evaluation of Montenegrin Seafarer's Awareness of Cyber Security.

[25] Chang, C. H., Wenming, S., Wei, Z., Changki, P., & Kontovas, C. A. (2019, November). Evaluating cybersecurity risks in the maritime industry: a literature review

company's administration, before that company verifies its compliance document (DOC) after the 1st January 2021. Although it is not yet mandatory, companies should start developing policies in their ISM code to be ready to ensure security.[26]

The instructions specify the following actions which offer cyberspace effective management:[27]

- Identification of systems and data that, if attacked, pose risks to the ship's operations.

- Emergency contingency planning for cyber attacks to ensure the shipping companies' smooth operations.

- Development and implementation of processes and defense means that are necessary for the timely detection of a cyber attack.

- Development and implementation of strategies in order to establish resilience and restoration of a company's necessary systems.

- Make backups to restore systems which are important for the company that has been a cyber attack victim.

More specifically, the resolution MSC.428_ (98) which concerns security risk management in shipping systems, recognizes the necessity encourage shipping companies to be more aware of cyber threats. This resolution provides support shipping safety and security, and it is functionally resistant to cyber threats. It also recognizes that administrations, classification societies, ship owners and ships, manufacturers, service providers, ports and port facilities and all other interested shipping industries have to accelerate their efforts in order to secure the industry from cyber threats. All these stakeholders must take into account the MSC-FAL.1 / Circ.3 guidelines regarding sea shipping cyberspace management, which was approved by the Facilitation Committee during its 41st meeting (4-7 April 2017) and by the Maritime

[26] Svilicic, B., Kamahara, J., Celic, J., & Bolmsten, J. (2019). Assessing ship cyber risks: A framework and case study of ECDIS security.

[27] Mraković, I., & Vojinović, R. (2020). Evaluation of Montenegrin Seafarer's Awareness of Cyber Security.

Committee Security. More specifically, the 98th session (7 to 16 June 2017), which contains recommendations for cyberspace can be integrated into existing risk procedures and complement the risk management practices and security and safety practices already established.[28]

IMO Resolution MSC.428 (98) encourages IMO Member States to ensure that cyber threats are addressed by security management systems since January 1, 2021. Many companies have fallen victim to cybercrime where hackers have access to their suppliers' email accounts (fuel, spare parts) and have sent e-mail messages asking for payments to go into other bank accounts than usual. This type of scam is called "phishing" and has started since 2013 and will be further discussed in this paper.[29]

2.2.2. International Security Management (ISM) Code

Taking into account the Decision A.741 (18) by which the Assembly approved the International Management Code for the Safe Operation of Ships and Pollution Prevention (International Safety Management Code (ISM)), the IMO recognizes the need for proper management organization in order to allow efficient response to the passengers' need to maintain high standards of safety and environmental protection. The ISM Code's goals are the following:[30]

- provide of best practices for ship operations

- evaluate all identified risks to ships, the staff and the environment

- establish safeguards

- continuous development of staff's skills

Furthermore, the ISM:[31]

[28] Chang, C. H., Wenming, S., Wei, Z., Changki, P., & Kontovas, C. A. (2019, November). Evaluating cybersecurity risks in the maritime industry: a literature review

[29] Aboul-Dahab, K. M. A. (2020). Demonstrating the cyber vulnerabilities of significant maritime technologies to the port facilities and on board of vessels.

[30] http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cybersecurity.aspx

[31] Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems.

1. Confirms that it is very important to develop an approved cyber security management system that complies to the ISM's code.

2. Encourages the authorities to take measures against cyber threats.

3. Recognizes that some essential precautions have to be taken regarding cyberspace management.

4. Calls on the Member States to forward this resolution to all stakeholders.

In order to comply with IMO guidelines and to do what the resolution stipulates, each company should move in three directions and fulfill the following:[32]

1. Define roles and responsibilities for staff members, either being on land or on ships. In short, companies have to train its staff to be familiar with cyber threats and know exactly what to look for in order to act when faced with a cyber threat. As with specific procedures that are followed in cases of emergency, e.g. in the event of a collision or a fire, where all members of the company or the staff knows exactly what to do or avoid, so on in this case the crew must be properly prepared and trained to deal with a cyber attack. A research that was conducted in 2018 demonstrated the need to raise awareness of crew members, because, despite the fact that 47% of respondents answered that they were found at some point on a ship, which became the target of a cyber attack, only 15% of the respondents had received any form of security training regarding cyber space, which is a particularly small percentage. Therefore, it is necessary to understand that cybersecurity is not just a matter of a company's IT department, but it should be considered from the whole crew of the ship, and be an integral part of its operations. So it is absolutely important, both to inform and educate all stakeholders involved, which starts with the senior management and down to the crew of the ship. Furthermore, there is a need for an efficient design, which will ensure

[32] Karamperidis, S., Kapalidis, C., & Watson, T. (2021). Maritime Cyber Security: A Global Challenge Tackled through Distinct Regional Approaches.

preparedness to deal with and manage a crisis. These can be achieved through appropriate staff training and awareness programs.

2. Determine exactly which are the most sensitive systems of a ship, which if attacked by a cyber-threat, will disrupt its functions.

3. Be able to assess the magnitude of the risk and formulate an emergency plan (real time monitoring response) in order to minimize the impact of the attack. If a cyber attack takes place, the company must be organized in such a way that it does not "paralyze". It must apply such techniques and procedural measures, which will ensure the continuation of its operations in the event of an unexpected incident.

In general, the smooth integration of measures in the existing Security Management System is an important task that requires time and a lot of capital to complete efficiently.

2.2.3. ISO / IEC 27001 standard on Information technology

Another tool that IMO refers to through its instructions is "ISO / IEC 27001 standard on Information technology" which was published by the International Organization for Standardization (ISO) and International Electrotechnica Commission (IEC). The ISO / IEC27001 sets the prerequisites for a standard Information Security Management System (ISMS). ISMS is one way for companies to manage sensitive personal data such as the information of employees and confidential information provided to third parties, and at the same time guaranteeing their safety.[33]

These standards are important and useful for shipping companies and ships, since in this way they will be able to keep the information safe e.g. personal data of employees, crews and passengers.

[33] Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda.

2.2.4. The European Regulation on the Protection of Personal Data - General Data Protection Regulation (GDPR)

Within the borders of the European Union, companies are obliged, besides the above mentioned guidelines, to comply with one additional regulation, the much-discussed GDPR. The GDPR, the implementation of which was put in force for all Member States of the European Union on 25 May 2018, concerns the protection and processing of personal data. The GDPR also affects shipping, as ship owners are required to comply with this Regulation, which tightens the framework of legality of the processing of personnel data as defined in its articles, otherwise risk being penalized with particularly severe administrative fines. Therefore, it is mandatory to collect and keep the staff's personal data in certain files and pay special attention, without processing them and without sharing them with third parties without prior consent. The term personal data means any personal information which may accurately lead directly or indirectly, to the identification of a person.[34]

Greater responsibility for the GDPR lies with cruise shipping companies, which collect and store personal data of hundreds of passengers. These data, which are stored electronically in the database of each company, may include ID / passport number, date of birth, home address, medical history, and bank card numbers, all of which are required in order to complete a reservation. Therefore, storing this data makes them a potential cyber attack target. Hackers at any time may gain unauthorized access to the company's files and steal this data leading to bad publicity for the company, legal disputes over damages, seeking criminal liability, fines etc. From the above it appears that there is a clear connection between cybersecurity and GDPR, stressing once again the need for its integration into security systems.[35]

It should be added that harmonization with the European GDPR Regulation and the penalties imposed in case of non-compliance with it, concern every company, whether or not it is in the territory of an EU Member

[34] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies.

[35] Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means.

State, provided that the personal data collected concerns a European citizen. That means that there must not be any complacency and every company must be careful about safe custody and preservation of personal data in its files.[36]

However, the application and validity of the above directives has not yet brought any substantial solution. The problem of cyber threats still exists, because both the legislation and the legal regime governing maritime insurance, actually find it difficult to keep up with developments in technology that have a major impact on the shipping industry. So far there is no international treaty including cyber security and there is no mandatory insurance coverage for cyber attacks.

2.2.5. International Ship And Port Facility Security (ISPS) Code

The guidelines for the prevention of deliberate attacks and in general illegal acts on board ships and port facilities are set out in the ISPS Code which was approved by the IMO in 2002. The ISPS Code refers to all vessels doing international voyages, as well as passenger and cargo vessels of more than 500 gross tonnage. The ISPS does not involve warships or government vessels that are utilized for non-commercial vessel services.[37]

The ISPS Code consists o two parts. The first part (A) stipulates all mandatory provisions and the second one (B) stipulates all optional provisions at the discretion of the national authorities. The code was implemented in the European Union by Regulation 725/2004 confirming as mandatory the provisions of Part A and certain provisions of Part B.[38]

The objectives of the ISPS code are:[39]

[36] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies.

[37] Suppiah, R. (2009). International Ship and Port Facility Security (ISPS) code and crew welfare.

[38] Burmester, C. (2005). International Ship and Port Facility Security (ISPS) Code: the perceptions and reality of shore-based and sea-going staff.

[39] Suppiah, R. (2009). International Ship and Port Facility Security (ISPS) code and crew welfare.

1. The establishment of a global framework that encourages governments to work together with shipping companies and ports to identify security threats and take precautionary measures against incidents involving the safety of ships or port facilities.

2. The definition of the respective responsibilities of the governments, the governmental services, local administrations, shipping companies and ports. This will be applied on a national and international level to ensure cyber safety.

3. Ensuring efficient collection and exchange of data related to ship security.

4. The provision of methodology for security assessments, so that there are plans and procedures for responding to changing security levels.

5. Ensuring the certainty that adequate and proportionate maritime security measures are implemented.

2.2.6. Regulation 725/2004

In the field of shipping, the European Union considering the ISPS Code adopted by the IMO in 2002, developed Regulation (EC) 725/2004 of the European Parliament and the Commission on 31 March 2004 (Regulation (EC) 725/2004) on improving and enhancing the security against illegal acts towards ships and ports and port facilities. The main object and purpose of this regulation is the presentation and implementation of European Community measures aimed at improving security from illegal acts in relation to ships and to port facilities involved in trade both internationally and nationally. These measures are always associated with dealing with deliberate illegal activities.[40]

Following the adoption of Regulation 725/2004, some of the suggestions and advice of Part B of the ISPS Code became mandatory (instead of being

[40] Androjna, A., & Twrdy, E. (2020). Cyber threats to maritime critical infrastructure.

proposed) for EU Member States. These mandatory information concern the following:[41]

- Ship Security Assessment

- Ship Security Plan

- Port Facility Security Risk Assessment

- Port Facility Security Plan

[41] Ringsberg, A. H., & Cole, S. (2020). Maritime security guidelines: a study of Swedish ports' perceived barriers to compliance.

3. RECENT MARITIME CYBER ATTACKS

The following cyber attacks cases which took place were alarming in the world of shipping and urged the internationals shipping agencies and legislators to design and then to adopt legislation and general regulations concerning the protection of those involved in a cyber attack. It is important that every ship owner to be prepared for a cyber attack because it is not a science fiction scenario. Only by having this mentality, but also securing the cooperation of all stakeholders of the supply chain, the shipping industry will at least limit this issue to a significant degree.

3.1. Port of Antwerp

The port of Antwerp was a victim of a cyber attack, which began in 2011 and lasted for a period of more than two years. This cyber attack found a gap in the electronic container release system, known as ERS, which was first used in the port of Antwerp in 2005. The ERS operated as follows: some carriers, instead of freight forwarders, sent through emails some unique electronic numbers to the recipient, agent, and the terminal port (pin codes), which corresponded to specific containers, and were necessary for receiving the containers from the warehouses of the terminal. In 2011 a group of intruders managed to break this container system management and access data, which provided the perpetrators with information on their exact location and safety containers in the port. This allowed them to hide smuggled drugs and weapons and smuggle them into the country. The authorities realized what was going on, the way the whole scam was set up and the violation of the cyberspace, when the perpetrators (who were acting undisturbed for a long time) had overestimated their abilities and removed entire containers from the Antwerp terminal. Similar attacks took place during the year 2018 in the ports of Barcelona and San Diego. This case showed that the in the port's cyberspace security measures were inadequate and were creating a vulnerable

environment, and made it clear that there was a need for immediate cyber security measures.[42]

3.2. BW Group

Less than a month after the cyber attack in the Danish shipping company Maersk, another company, BW Group, fell victim by some hackers. More specifically, the computers in the company's offices were violated in Singapore, as a result of which the communication of the company with the outside world was interrupted and limited to recipient emails only and the ship's crew. It became known from the company representative that the attack was not due to any ransomware, however it was not specified if BW financial data or data were stolen. Then, as was expected, the time following the attack, the company tried to take appropriate measures to avoid any such situation in the future and fill the existing gaps in its cyber security system.[43]

3.3. Clarkson PLC

On November 29, 2017, the British shipping company Clarkson PLC with an official press release confirmed unauthorized access to its computer system in the United Kingdom. The violation was theft of clients' personal data, which included dates of birth, passport details, bank accounts, etc. and asking for ransom in order not to disclose this data. In fact, after an investigation by the authorities it was found that the breach of the systems came from a unique and isolated user account, which was then deactivated. The paradox is that the breach of systems with the corresponding interception of personnel data was detected on November 7, 2017 while this was happening for a period of 6 months, i.e. from 31 May 2017 until 4 November of the same year.[44]

[42] Caponi, S. L., & Belmont, K. B. (2015). Maritime cybersecurity: a growing threat goes unanswered.

[43] Tusher, H. M., Munim, Z. H., Notteboom, T. E., Kim, T. E., & Nazir, S. (2022). Cyber security risk assessment in autonomous shipping.

[44] Heering, D. (2020). Ensuring Cybersecurity in Shipping: Reference to Estonian Shipowners.

Following the cyber attack, Clarkson PLC made every effort on its part for the proper management of the attack, while trying not to affect its functions, but also to protect its customers. The company also took additional security measures to prevent similar incidents in the future and studied the attack in depth in order to enhance its cyber security.[45]

This incident shows that the issue of cyber attacks and cybersecurity is not just about ships, ports and shipping companies in the narrow sense, but it affects the whole range of shipping and maritime economy (ships, shipping companies, ports, brokers, insurers, suppliers and charterers), and it emphasizes that tackling cyber attacks and taking precautionary measures is more relevant and necessary than ever.

3.4. Cosco U.S.

On July 24, 2018, the perpetrators of the cyber attacks increased the list of victims by adding to it, Cosco Shipping Lines in the United States. The company with an announcement which was posted on its Facebook page the day after the attack, informed its customers that due to the consequent breakdown of the network, the telephone systems were inactive and email exchange was not operating smoothly in the wider area where the attack took place. In fact, for security reasons, the company cut off the connection to other areas, in order not to cause a general system breakdown.[46]

Another consequence of the attack was also an extensive malfunction of its terminal, Pier J, in the port of Long Beach. It was emphasized by the company that all its ships operate normally without them having been affected by the attack. The way the company came back after the incident proves that Cosco was on standby, had studied how cyber attacks work, which took place in Maersk a year ago, and tried taking the appropriate measures to minimize the risk. For this reason, the company managed to restore all its processes to normal and almost returned to normal one week after the event. Of course, the

[45] Heering, D. (2020). Ensuring Cybersecurity in Shipping: Reference to Estonian Shipowners.

[46] Lehto, M. (2021). Cyber security challenges in aviation and maritime.

fact that this particular attack was not as big, harmful and damaging as the one at Maersk, played an important role.

3.5. A.P. Møller - Mærsk

The most famous cyber attack in the history of shipping took place on June 27, 2017 when the Danish company Mærsk was "hit" by a malware called NotPetya12. The attack on the company was considered as collateral damage in the context of a generalized cyber attack, which further proved that the consequences of a cyber attack can be incalculable. In particular, the attack affected all Mærsk's global operations, as well as all terminals which total to 17. Two of them were breached in the port of Rotterdam and 15 in other ports around the world. The terminals, due to the problems of company's information system, some of the loads were not delivered to the correct destinations. Mærsk ships carry about 20% of world trade in containers, so it can be easily perceived the difficulty that a company as big as Maersk had to face, and the impact this cyber attack had on its activities. To restore the company to the previous state 4,000 new servers had to be reinstalled, 45,000 new computers and 2,500 applications. It is worth mentioning that the total reinstallation was completed within 10 days, while something similar under normal conditions takes about 6 months.[47]

Jim Hagemann Snabe, President of A.P. Møller - Mærsk, as one of the speakers at the 2017 World Economic Forum, shared his thoughts on cybersecurity and the conclusions he came to through experience with his company. Moreover, this cyber attack showed that all companies, regardless of their size and reputation, lag behind in cybersecurity. Therefore, the issue of cyber security, must not only be the first priority for every company, but it also is a competitive advantage for those who have it.[48]

[47] Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history.

[48] Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history.

From the first moment of the incident, Mærsk, without fear of the impact the incident might have had on its reputation, published through its twitter account the incident of the attack and informed everyone what steps were followed so that this event could be a source of knowledge for other companies. At this point, it is worth mentioning that shipping law does not make it necessary to disclose information of what occurs in the cyberspace, contrary to the legal framework of aviation, which makes it is mandatory to report such incidents as a precautionary measure in order to detect similar risks, capable of endangering their safety, as developed within the European Regulations Framework (Regulation (EU) 2018/1139 and Regulation (EU) No 376/2014).[49]

As pointed out by Mr. Jim Hagemann Snabe, the company, by going public with the attack, tried to pass on the experience in order for everyone to understand the magnitude of the problem, because no company should take this lightheartedly. As it turned out, prevention is even more important than an immediate reaction of a cyber attack. The attack on Mærsk demonstrated the need for companies to adapt to a new status, because, as William P. Doyle characteristically stated: "From the moment Mærsk fell victim to a cyber attack, something similar can happen to anyone." In fact, the publication of all the data of the attack by A.P. Møller - Mærsk was considered the first step in changing the mentality of companies in how they perceive the nature and impact of cyber risk. Today, all companies pay careful attention to the issue of cybersecurity and even in view of the Regulation - MSC.428 (98)[50], which was imposed by the IMO on January 1st, 2021, on all ships were the ISM is applied.[51]

[49] Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history.

[50] Companies need to prove that cyber security is an integral part of their security management system, no later than the first annual verification of the document of compliance (DOC) and specifically from 1 January 2021. The DOC certificate is issued for a company, after an initial inspection by the authorized body, in order to verify its full compliance with the ISM Code for the Safe Management System (SAD / SMA) which operates and is implemented for at least three months by both the company and from any type of company ship. The validity of the DOC is for five years and during its validity annual inspections are carried out every 12 months +03 months from the expiration date of the certificate. For the renewal of the DOC certificate after its expiration a new check is performed and ceases to be valid when one of the required statutory inspections has not been carried out or in the event that a significant deviation from the requirements of the ISM Code has been found. The Document of Compliance belongs to the final shipping documents (Svilicic et al., 2019).

[51] Lovell, K. N., & Heering, D. (2019, June). Exercise Neptune: MaritiMe cybersecurity training using the navigational siMulators.

In addition, this attack was the reason for the birth of a myriad of questions regarding the insurance coverage of such incidents and with what are the obligations of the stakeholders. To date, existing traditional insurance products do not cover the dangers posed by cyber attacks and therefore the current situation, made it necessary to create a new product of maritime insurance, which is becoming increasingly necessary for shipping companies.

4. EQUIPMENT VULNERABILITIES IN SHIP SYSTEMS

4.1. ECDIS

The bridge systems of a vessel such as ECDIS can easily become targets of cyber attacks, just like any other computer system. The threat may come from viruses loaded with a USB stick, from clicking on a link which is in an e-mail or of course from an illegal intrusion by a hacker through some vulnerability. Although the ECDIS system works on computer systems, the necessary security measures required for systems protection are often overlooked as they are considered autonomous systems and therefore not treated as PCs. However, to the present day, it is considered unlikely that there will be a targeted attack on systems that perform ECDIS.[52]

4.2. GNSS

Ships rely on Global Navigation Satellite Systems (GNSS) to track navigation and required time (PNT). This means that security gaps can have a serious impact on general safety and the ship's navigation. Obstruction may occur by natural, accidental or intentional actions. The perpetrators can interfere with signals leading to incorrect data reporting in integrated systems of other ships.[53]

The impact of GNSS involvement has been demonstrated in many experiments conducted by the General Lighthouse Authority of the United Kingdom (GLA). These systems are based on providing basic on-board navigation as well as informing other ships of their coordinates and speed. This means that incorrect data could have a broader impact on the safety of both the ships themselves as well as others that sail nearby.[54]

Also, by transmitting signals to a target ship and increasing the signal strength and frequency, the ship begins to trust the signal it receives. Thus, the

[52] Svilicic, B., Kamahara, J., Celic, J., & Bolmsten, J. (2019). Assessing ship cyber risks: A framework and case study of ECDIS security.

[53] Geister, R. M., Buch, J. P., Niedermeier, D., Gamba, G., Canzian, L., & Pozzobon, O. (2018). Impact study on cyber threats to GNSS and FMS systems.

[54] Pelton, J. N. (2019). The Growth and Expansion of Precise Navigation and Timing.

attacker is allowed to provide fake info on board and remove the ship from service, while this displacement can be detected neither by the crew nor by offices.[55]

It is worth mentioning that the majority of vessels have more than just one GNSS module integrated into multiple systems. The way these modules are connected is not always clear, which means if there is an entanglement or falsification event, many alarms can be activated on the bridge. There are often limited contingency plans while the crew is often not trained enough to respond to failures regarding GNSS receivers.[56]

GLA recommendations include the use of Enhanced Loran (eLoran) systems. This is quite similar to GNSS and it is essentially a navigation system. ELoran maintains backup files in case of GNSS getting disrupted caused by natural disasters or by cyber attacks.[57]

4.3. AIS

Automatic Identification System (AIS) is used for ship monitoring, but also for safety at sea, awareness of the situation, businesses search and rescue. AIS messages are exchanged by radio frequency (VHF) and are based on GNSS coordinates for near reference stations via VHF. AIS is a two-way ship-to-ship and ship-to-shore that broadcasts system information.[58]

The main weaknesses of AIS result from the following:[59]

- Validity checks: AIS can be sent by anyone without carrying out geographical validity checks

[55] Geister, R. M., Buch, J. P., Niedermeier, D., Gamba, G., Canzian, L., & Pozzobon, O. (2018). Impact study on cyber threats to GNSS and FMS systems.

[56] Geister, R. M., Buch, J. P., Niedermeier, D., Gamba, G., Canzian, L., & Pozzobon, O. (2018). Impact study on cyber threats to GNSS and FMS systems.

[57] DiRenzo, J., Goward, D. A., & Roberts, F. S. (2015, July). The little-known challenge of maritime cyber security.

[58] Kessler, G. C., Craiger, J. P., & Haass, J. C. (2018). A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system.

[59] Kessler, G. C., Craiger, J. P., & Haass, J. C. (2018). A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system.

- Timing controls: Lack of timestamp means that it is possible to duplicate AIS data that is no longer valid

- Authentication: When transmitting AIS data there are no authentication protocols which allows the creation of harmful AIS packages to counterfeit another ship

- Integrity checks: AIS messages are encrypted, increasing the threat of messages being intercepted and modified without being noticed

As with GNSS, AIS is considered an easy target for cyber attacks, because they do not have a built-in signal encryption or authentication mechanism. This means that AIS is rather vulnerable to cyber attacks such as obstruction (locking a position) and blocking or forging (which feeds false information to the recipient).[60]

Attacks like these may cause serious damage. An AIS malfunction could lead to a possible collision with another ship. Radio transceivers defined by software for transmitting the AIS navigation system or VTS can be used. For instance, if there is not enough visibility, vessels rely on GNSS signals to locate and notify other vessels in the area.[61]

Even though there are many security gaps in AIS, it is not the primary target of cyber criminals.[62]

4.4. GPS

Nowadays, it is very easy and simple to find GPS interceptors on the market, since they are sold for a few thousand dollars. With this device it is possible to intercept GPS from distances up to about 500 meters. GPS is a basic device for the ship as it provides timing and reference data to a number of systems such as electronic maps, radar, compass etc. Such an interference

[60] Saravanan, K., Aswini, S., Kumar, R., & Son, L. H. (2019). How to prevent maritime border collision for fisheries?-A design of Real-Time Automatic Identification System.
[61] Androjna, A., & Twrdy, E. (2020). Cyber threats to maritime critical infrastructure.
[62] Saravanan, K., Aswini, S., Kumar, R., & Son, L. H. (2019). How to prevent maritime border collision for fisheries?-A design of Real-Time Automatic Identification System.

is sure to create significant problems in the operation of the ship and will make it significantly difficult its management especially in areas with high maritime traffic.[63]

Spoofing and jamming are a couple of methods utilized by perpetrators and can really wreak havoc on the maritime community, as long if it is done correctly. GPS spoofing is “an electronic attack involving signals being sent to a receiver to control navigation”, while on the other hand, GPS jamming involves an intentional blockage of GPS signals.[64]

The Office of Cyber and Infrastructure Analysis (OCIA), which is a branch of DHS, has realized that there are very substantial issues regarding GPS jamming and spoofing in the shipping industry, because a ship is very dependent on GPS systems. When a ship operates close to shoal water or in a narrow channel, there is an elevated risk for disasters resulting from incorrect navigation (e.g. colliding). If a vessel loses its navigational inputs, it becomes very difficult to steer, and or propulsion could have perilous consequences and inflict serious damage, cause delays and financial losses.[65]

4.5. Integrated bridge

Bridge integration started emerging in the late 60s. During that time, computers did not have the potential they possess today, and the interfacing between devices happened with analogue connections such as synchro transmitters and receivers, stepper transmitter and stepper receiver, pulses and analogue DC voltage. Nowadays, everything is connected with the usage of serial cables, in compliance with the Marine Industry Standard Serial Data Communication IEC61162. This allows compatibility between all equipment.[66]

[63] Manesh, M. R., Kenney, J., Hu, W. C., Devabhaktuni, V. K., & Kaabouch, N. (2019, January). Detection of GPS spoofing attacks on unmanned aerial systems.

[64] Manesh, M. R., Kenney, J., Hu, W. C., Devabhaktuni, V. K., & Kaabouch, N. (2019, January). Detection of GPS spoofing attacks on unmanned aerial systems.

[65] Hayes, C. R. (2016). *Maritime cybersecurity: the future of national security*

[66] Awan, M. S. K., & Al Ghamdi, M. A. (2019). Understanding the vulnerabilities in digital components of an integrated bridge system (IBS).

Because using digital navigation systems is becoming increasingly popular in the shipping industry, integrated bridge systems are very easy targets for cyber attacks. The systems that do not share a connection with other networks can also be easy targets, for the reason that removable media devices are more than often implemented to update these systems. An incident in cyberspace can be extended to denial or manipulation of a service. This means that navigation can be a hit as well.[67]

4.6. Autonomous vessels

The IMO states that the risk arises from vulnerabilities that are caused from mishandling, maintenance and design of cyber-enabled systems as well as from global cyber attacks. Many researchers and the International Electrotechnical Commission (IEC) have pointed out the need for proper security measures in the IT infrastructure of conventional and non-conventional ships. So, taking into account that autonomous vessels contain the above mentioned systems that are also found on a conventional ship, it is obvious that a correct and in-depth analysis is vital for remote controlled and autonomous vessels. The analysis risk is realized by comparing the probability of a possible occurrence attack with the consequences it will bring.[68]

Rolls-Royce is conducting studies in order to replace conventional ships with autonomous ships. This endeavor is supported by Tekes and also from various universities in Finland. Different aspects that include technology, security, law and finances are being currently studied in order for autonomous shipping to be possible in the near future. The company realizes that cyber risks can be detrimental and that it is possible to take over command of an autonomous ship via malware. In order to reduce these risks, Rolls-Royce proposes to eradicate a ship's vulnerabilities and to further invest in detecting and preventing intrusions.[69]

[67] Awan, M. S. K., & Al Ghamdi, M. A. (2019). Understanding the vulnerabilities in digital components of an integrated bridge system (IBS).
[68] Tam, K., & Jones, K. (2018, June). Cyber-risk assessment for autonomous ships.
[69] Katsikas, S. K. (2017, April). Cyber security of the autonomous ship.

5. CYBER THREATS

After conducting a literature review, it was found that there are mainly two types of cyber threats that may cause damage to a company and its ships:

- General threats or untargeted attacks

- Targeted threats or targeted attacks.

General threats refer to methods and means which one can locate online. These means and methods can be utilized to identify and exploit the extensive cyber security gaps a company or a vessel has. Some examples of these means and methods are the following:

- ***Malware (Malicious software):*** Malware which has been developed so that the perpetrator can gain access without the owner's authorization. Malware includes trojans, ransomware, spyware, viruses, and worms.[70]

- **Water holing:** This involves creating a fake website or putting at risk a real website for exploiting visitors. According to Panjunen,[71] when a perpetrator is using water holing, he/she wants to enter the user's network. It is worth mentioning that these cyber attacks are not common, however, they are a considerable threat because it is not easy to track them. Water holing is used by perpetrators in order to attack a company that has generally high-security standards, and therefore target the company's employees, business partners or an unsecured wireless network".[72]

- ***Spam messages:*** Spam messages are usually not a threat, but they can be used as a tool to gather classified information or install malicious software. Spamming is the act of sending unrequested e-mails in large quantities. They are considered a threat to cyber security if implemented by a perpetrator. Another noteworthy aspect is how spam can sometimes be

[70] Androjna, A., & Twrdy, E. (2020). Cyber threats to maritime critical infrastructure.
[71] Pajunen, N. (2017). Overview of maritime cybersecurity.

[72] Kettani, H., & Cannistra, R. M. (2018, October). On cyber threats to smart digital environments.

confused or can incorrectly be classified as phishing. They differ in the fact that phishing is a targeted action using social engineering tactics, designed to steal data while spam is a tactic for sending spam email to a bulk list. Cyber attacks may use junk mail tactics to deliver messages, while spam can link the user to a "dangerous" site for installing malware and stealing personal data.[73]

- ***Web-based attacks:*** This covers a wide range of attacks, for example facilitating a malware Uniform Resource Locator (URL) or malware to direct the user or the victim to the desired website or download malicious content for financial profit, theft of information or even ransomware. Cyber attacks can affect the availability of websites, applications and Application Program Interfaces (APIs), violating the confidentiality and integrity of the data.[74]

- ***Web application attacks:*** The increasing complexity of internet applications and their widely used services, poses challenges for insuring them against threats with a variety of motives, such as financial loss or theft of critical or personal information. Internet services and applications depend mainly on databases for storage or delivery of the required information. Cross-site Scripting attacks (XSS) is an example of such a threat. In this type of attack, the attacker uses techniques to extract access codes for accessing of online applications. So, these lead to malicious functions, such as redirecting to a malicious online location.[75]

Targeted threats are usually well planned and sophisticated than general threats. They implement means and methods which are developed specifically to target a company or a ship. Some examples of these are the following:

- ***Social engineering:*** Social engineering is a method implemented by cyber intruders to obtain confidential information and to break security

[73] Mraković, I., & Vojinović, R. (2020). Evaluation of Montenegrin Seafarer's Awareness of Cyber Security.

[74] Kettani, H., & Wainwright, P. (2019, March). On the top threats to cyber systems.

[75] Razzaq, A., Latif, K., Ahmad, H. F., Hur, A., Anwar, Z., & Bloodsworth, P. C. (2014). Semantic security against web application attacks.

procedures. It is usually done through social media networking. According to Walker,[76] "Social engineering involves a person's or a group's manipulation in giving information or a service which under other circumstances they would not give". For instance, the majority probably would not provide their password if someone asked them to do so. Unfortunately though, there are many who would if asked by someone who seemed trusting. Social engineering can be human-based or computer-based. The first one involves interacting with a company's employees through emails or other means to obtain data. Computer-based attacks are possible through the usage of a computer or another device capable of processing data. Social media is another tool implemented by hackers to collect the necessary data to make the false messages look more sophisticated and plausible.[77]

- ***Phishing:*** This involves sending emails to a large number of recipients requesting specific information. These emails can also trick an individual in visiting a fake website using one hyperlink contained in an email. Some cues that may indicate a fake e-mail are the following: Unknown sender, greeting (e.g. "dear member"), spelling and grammar mistakes, hyperlinks.[78]

- ***Spear phishing:*** This is more a more sophisticated and detrimental version of phishing. In this case, the perpetrator already possess data about the target. With spear phishing the perpetrator greets the person with his/her name. Because the perpetrator already has some information about the target, the recipient may not suspect a security breach attempt.[79]

- ***Brute force:*** An attack which, through a repetitive process, the attacker tries many passwords hoping to get the right one.[80]

[76] Walker, M. (2012). CEH certified ethical hacker exam one: all in one.
[77] Heering, D. (2020). Ensuring Cybersecurity in Shipping: Reference to Estonian Shipowners.
[78] Androjna, A., & Twrdy, E. (2020). Cyber threats to maritime critical infrastructure.
[79] Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks.
[80] Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks.

- ***Denial of service (DoS):*** This denies entry to all legal and authorized users so that they cannot have access to information, usually by "flooding" a data network.[81]

6. AN OVERVIEW OF SHIPS NETWORK STRUCTURE

6.1. Most common approaches

This section is going to cover the most common network structures seen in a vessel. For this reason, Ship A and Ship B are going to be used as examples.

6.1.1. Ship A

It is very common to compare the structure of a ship's network to the one of a company's. However, there are some minor differences, such as the fact that a ship relies on wireless network. The following figure illustrates the network found on Ship A.

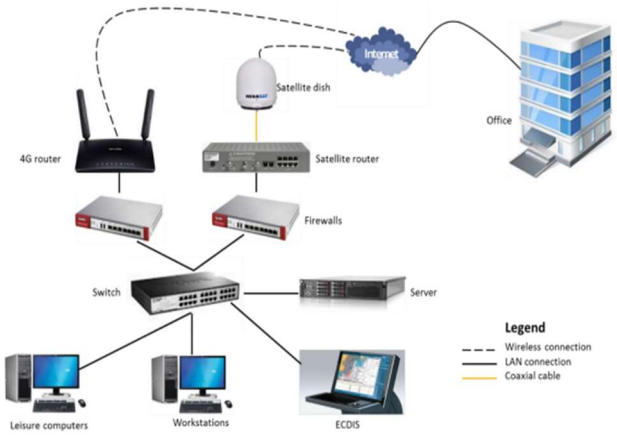

Figure 1. The network structure on Ship A[82]

[81] Tam, K., & Jones, K. (2018, June). Cyber-risk assessment for autonomous ships.
[82] Pajunen, N. (2017). Overview of maritime cybersecurity.

Access to internet was possible through a 5G network or a through satellite. On the ship, the 5G connection was used only when the vessel was within national waters, otherwise it would be very costly because of the data that would be needed. This is why satellite connection is preferable. Both types of connection run via the vessel's firewall in order to protect against unauthorized access.

A switch is used to connect all the network's devices on board. But, the vessel's network is a segment of the total company's network. For instance, the location of the e-mail server and a number of the databases is on the mainland. The vessel's IT systems are connected via VPN to the headquarters.

The server which is located on the vessel is handling directory. DHCP and backups. DHCP is set up in a manner, allowing only the vessel's own computer static IP addresses. Even in the case of someone plugging in his computer, access would not be granted by the server. The network's configuration also allows for prioritizing based on computer type. This means that the masters computer possess perhaps the highest priority.

Backups are performed on a daily basis which are saved on the server. Moreover, some officers possess external drives so that they can perform their own backup.

Every computer on the vessel can have AV software installed, They may also have a software that allows the company to connect via its own IT department.

In addition, leisure computers are connected to the company's domain. Of course, not all websites can be accessed, e.g. adult websites.

ECDIS can be given by Furuno's server. An example of how ECDIS can be updated is shown in the figure below. At the moment UKHO gives out new chart updates, Furuno's server can proceed to downloading and sending them through a satellite connection to the vessel's Gate-1 unit. From that point, the navigation officer can install all necessary updates to ECDIS. A fact that is troublesome is that ECDIS is connected to Gate-1 through an Ethernet cable.

Figure 2. Furuno's ECDIS chart update system[83]

6.1.2. Ship B

The figure below demonstrated that the structure of the network on ship B has a lot of similarities to the structure of ship A. However, there are some small differences.

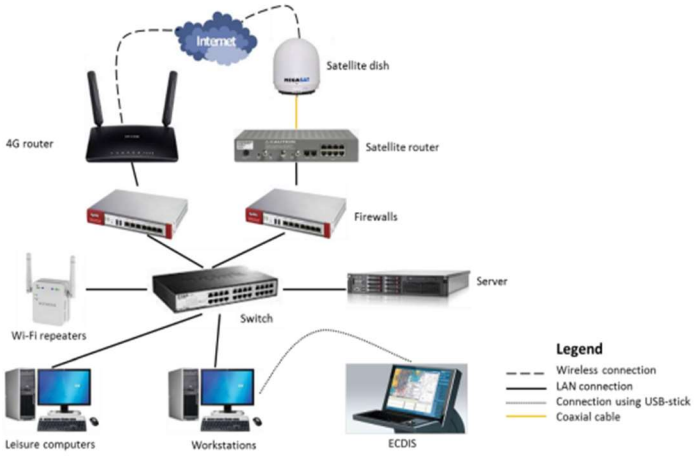

Figure 3. The structure of the Ship B network[84]

[83] Furuno http://www.furuno.com/en/merchant/ecdis/gate-1/
[84] Pajunen, N. (2017). Overview of maritime cybersecurity.

Internet access is provided as in Ship A. The difference is that the company allowed a 5G connection when not on national waters. Today, the majority of the vessels are connected via satellite, because the exchange of e-mails is very important in shipping.

Now proceeding to the differences, Ship B acts independently since there is no connection to the network of the company. All services are installed on the server which is on the vessel.

The configuration of the switch was such in order to allow two VLANs. One VLAN would be for be for the vessel's computers and the other for the staff's PCs. Both VLANs were in a good state since they were operating on Windows 8 and there was AV software as well.

Maintenance is provided by a third party and has the responsibility for administering devices, the network and providing support in general. The computers on the vessel had a software that allowed remote control.

Wi-Fi extenders can be found on each deck of the vessel. Because the vessel's structure is very strong, the extenders did not have adequate range, making it impossible accessing the network even if the vessel is at berth. A WPA key is protecting the network but there is an important issue: the password key is written on every extender, something that allows unauthorized access.

Updating ECDIS was performed when downloading them and then transferring them with a certain USB stick. The USB is scanned for viruses every time before usage.

6.2. Attack scenario

It is useful at this point to consider a possible scenario on how to exploit the network on Ship A. The perpetrator begins by searching for possible targets on LinkedIn. The perpetrator locates John Smith, who recently graduated from a maritime school and had found a job on Ship A. The perpetrator then starts collecting information about John from other social media, such as Instagram. He then crafts a spear phishing e-mail especially for John.

A week later, John accesses his e-mails on a ship's computer and sees that a very famous cruise company has approached him. The company knows John's name, compliments him on what he has achieved and offers him a job on their newly built ship. What John has to do is simply fill out a form that is provided as an attachment and send it. John gets very excited and without any second thought opens the attached file. The file though contained malware that starts running upon opening the file. This allowed the perpetrator to gain access to John's computer.

What the perpetrator had to do next is figure out what kind of network he was dealing with. He also knows that a ship's network is not secure enough and that probably there is no IT expert on board. He then begins scanning for open ports, operating systems and running applications. He can also locate different user accounts and their passwords. While doing all this, the perpetrator realizes that there is an ECDIS software. He exploits the vulnerabilities and he wants to have some fun by altering the course of the vessel.

7. BEST CYBER SECURITY PRACTICES

7.1. Recognizing a threat

Threats in cyberspace concern the company, the ship, the operation and trading. When assessing a threat, companies need to consider certain issues regarding their activities that could increase their vulnerability to cyber attacks. Experiences not only from the shipping industry but from other business sectors as well, indicate if a cyber attack succeeds, there can be serious damages and a halt in the provided services. The following table provide examples of threats and the possible consequences for the companies and ships they manage.[85]

[85] Androjna, A., & Twrdy, E. (2020). Cyber threats to maritime critical infrastructure.

Table 1. Examples of threats and the possible consequences

Threat groups	Motives	Aims
Activists	- Damaging a company's image - Ceasing operations	- Destruction of data - Going public with sensitive data - Attracting media attention
Criminals	- Financial gains - Corporate espionage - Industrial espionage	- Selling stolen data - Ransom for stolen data - Ransom for allowing operations to continue - Organizing an illegal transportation of goods - Gathering information
Opportunists	- The thrill of the challenge	- Breaching the system - Financial gains
- Terrorists - States	- Political gains - Espionage	- Acquiring information about new technologies - Disturbing the economy

The above groups of threats are capable of threatening the safety of ships and entrepreneurship of a company. Moreover, it is likely that the staff, either on board or on land, will endanger the company's systems. Normally, the company knows that this is probably not intended and be the result of human error in the operation and management of Information Technology Systems or by non-compliance to technical and procedural protection measures. It is also

possible though that the actions are malicious and that an employee deliberately attempts to damage the company and the ship.[86]

7.2. Cyber attack stages

The breach can go unnoticed even for years. This number was reduced to 205 days in 2015 and continues to go down as the detection technologically is being improved. In 2018, it took an average of 140 days to discover a cyber security breach. The time period for preparation of a cyber attack can be determined by its motives and goals as well as the robustness of technical and procedural controls in the cyberspace applied by the company, including those that are applied to its ships.[87] The general stages of a cyber attack are the following:

- Survey-reconnaissance. The perpetrators use public information so they can gather data about the target. Various tools can be used for this, such as social media. Using public sources can be supplemented by "sniffing" the actual data coming from and going to a company or a ship.[88]

- Delivery. The perpetrators may attempt to gain access to company and ship systems and data. This can be achieved within the company or the ship or remotely through as long as there is an online connection.[89]

- Breach. It is important to mention that when a system is compromised, the changes on the equipment may not be obvious or noticed at first. After breaching the system, the perpetrator can do the following: 1) Affect the system's functioning. 2) Access confidential data (e.g. consignment or guest lists. 3) Gain complete control of a system.

- Pivot. This is the phase where the perpetrator utilizes a virus that already has been installed on the system in order to "move" and perform other

[86] Rana, A. (2019). Commercial maritime and cyber risk management.
[87] Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems.
[88] Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2020). A novel cyber-risk assessment method for ship systems.
[89] Rana, A. (2019). Commercial maritime and cyber risk management.

activities. This method allows the attacker to utilize the system that has been compromised to attack systems that are not accessible. The perpetrator will most probably identify the weakest system part. When he/she obtains access, then the intruder will try to gain control over the whole system.

The motivations and goals of the perpetrator will determine the impact on the company's or on the ship's system and data. The perpetrator can:[90]

- Gain access to confidential data regarding cargo, crew and guests

- Falsify lists, cargo declarations or loading boards. This may allow transportation of illegal shipment of goods or theft of cargo

- Cause the impossibility of a service

- Assist piracy or seafaring

- Disrupt the smooth functioning of the company's and the ship's systems, for example by causing its network to crash.

7.3. Weakness Identification

It is recommended that a shipping company first conduct a potential threat assessment that may occur. After this, there has to be an assessment of the systems and on - board procedures for mapping robustness and addressing the significance of the threat. This can be done either by personnel that has knowledge over the matter or it can be done by external agents that possess knowledge of the shipping industry and its core procedures.[91]

An autonomous system is not as vulnerable to cyber attacks in comparison to those that are connected to local area networks. Attention should be given at understanding how critical systems connect to uncontrolled networks. In this way, the human factor has to be considered because a lot of

[90] Androjna, A., & Twrdy, E. (2020). Cyber threats to maritime critical infrastructure.
[91] Mraković, I., & Vojinović, R. (2020). Evaluation of Montenegrin Seafarer's Awareness of Cyber Security.

incidents are caused by staff actions. These onboard systems could include the following:

- Cargo management systems. These systems are used for loading, controlling and handling cargo, including dangerous cargo, and can be interconnected by various systems on land (e.g. ports and terminals). These systems can also include mission tracking tools. However, monitoring is normally done through the company's systems that are connected to the ship and not directly between the sender and the ship.[92]

- Propulsion and power management system. Digital systems which are used to monitor and control on board machines which are responsible for propulsion and navigation, are easy targets. These systems can become even easier targets if they are used in conjunction with remote monitoring (Remote access).[93]

- Access control systems. The systems used for supporting access control and ensuring the safety of a ship and of its cargo, including its (CCTV) monitoring, its security system of machines and auxiliaries as well as electronics systems are easy targets.[94]

- Passenger service and management systems. Smart devices (tablets, portable scanners, etc.) can be turned into, without the knowledge of their owners, means of access by the attacker, and ultimately the collected data is transmitted to other systems.[95]

- The public networks to which passengers are connected. The fixed or wireless networks that are installed on board for the benefit of the passengers should be considered insecure and should not be associated with any system that is vital to the ship's security.[96]

---

[92] Rana, A. (2019). Commercial maritime and cyber risk management.
[93] Mraković, I., & Vojinović, R. (2020). Evaluation of Montenegrin Seafarer's Awareness of Cyber Security.
[94] Mraković, I., & Vojinović, R. (2020). Evaluation of Montenegrin Seafarer's Awareness of Cyber Security.
[95] Mraković, I., & Vojinović, R. (2020). Evaluation of Montenegrin Seafarer's Awareness of Cyber Security.
[96] Mraković, I., & Vojinović, R. (2020). Evaluation of Montenegrin Seafarer's Awareness of Cyber Security.

- Crew management and welfare systems. On-board computer networks used to manage the ship are particularly vulnerable when users are online or when they access their mail. Perpetrators know this and they try to exploit it by gaining access to systems and data on board.[97]

- Communication systems. If a ship uses satellite or wireless devices for internet connection, its vulnerability is higher. The provider of satellite communications, provides programs (antivirus, malware) which provide internet security, but should not be solely dependent on these in terms of securing on-board systems and data. Authorities should strictly comply with applicable authentication requirements and access control management.[98]

7.4. Common Vulnerabilities

The following points, which exist in older ships, but also in some new ones are equally vulnerable to cyber attacks:[99]

- Outdated and unsupported operating systems.

- Outdated software or lack of anti-virus.

- Insufficient configuration, including inefficient network management and usage of default passwords.

- Network of computers on board which has no protection measures and network distribution.

- Safety equipment or systems permanently connected to land.

- Incomplete access controls, including manufacturers and service providers.

[97] Ringsberg, A. H., & Cole, S. (2020). Maritime security guidelines: a study of Swedish ports' perceived barriers to compliance.

[98] Pajunen, N. (2017). Overview of maritime cybersecurity.

[99] Miranda Silgado, D. (2018). Cyber-attacks: a digital threat reality affecting the maritime industry.

7.5. Developing protective measures

The purpose of a Risk Assessment is to develop a strategy for decreasing cyber threats. Technically, this means performing the necessary actions in order to establish and maintenance of cyber security. It is essential to determine how the security measures will be implemented in the cyberspace and on board.[100]

More specifically, protective measures include the following:

In-depth security: The company's policies and procedures have to seriously consider cyber security. Cyber threats may be complex, therefore, an "in-depth defense" approach must be reviewed. When there are multiple layers of security, systems are more resistant to cyber attacks.[101]

Technical Protection Measures: These measures are essentially a list of critical security controls (CSC) which are audited to make sure that they offer an efficient approach for companies to evaluate and better their defense against cyber threats.[102]

Procedural Protection Measures: Procedural controls focus on the way staff use the systems on board. Data containing valuable and sensitive information must be well protected and treated in accordingly. Examples of procedural actions can be crew training, visitor access, updating and maintaining software, updating antivirus, administrator protocols.[103]

Contingency planning: Losing Operating Technology Systems is considered a major issue regarding the safe functioning of a ship. In the event of an incident in cyberspace results in losing or the malfunction of Operating Systems Technological Systems, it will be important to take immediate action to guarantee all the stakeholders' safety.[104]

---

[100] Mraković, I., & Vojinović, R. (2020). Evaluation of Montenegrin Seafarer's Awareness of Cyber Security.

[101] Mraković, I., & Vojinović, R. (2020). Evaluation of Montenegrin Seafarer's Awareness of Cyber Security.

[102] Rana, A. (2019). Commercial maritime and cyber risk management.

[103] Androjna, A., & Twrdy, E. (2020). Cyber threats to maritime critical infrastructure.

[104] Chang, C. H., Wenming, S., Wei, Z., Changki, P., & Kontovas, C. A. (2019, November). Evaluating cybersecurity risks in the maritime industry: a literature review.

Efficient response: A team should be set up, which may include a combination of the ship's staff and onshore staff and / or external experts to obtain the appropriate measures for the restoration of Information and Operational Technologies Systems, and the ship to be able to continue its normal operations. The team must be able to prevent and counter a cyber attack. In order for a response to be effective, at least the following steps must be followed: Initial assessment, system and data recovery, incident analysis, deterring a similar attack.[105]

Recovery plan: A company must have recovery plans for the crew to find on board and at land. These plans can recover systems and data that are essential for the restoration of Information and Operational Technological Systems in operating condition. To ensure on board safety, operation and navigation of the ship should be a priority. The crew that is responsible for cyber security must have deep knowledge of these plans.[106]

[105] Pajunen, N. (2017). Overview of maritime cybersecurity.

[106] Mraković, I., & Vojinović, R. (2020). Evaluation of Montenegrin Seafarer's Awareness of Cyber Security.

CONCLUSIONS

The dangers in cyberspace are a new reality that during the last years is threatening the shipping sector as well. In earlier times, cyberspace was not considered at all by the shipping industry as there were other priorities that had to be addressed. At the same time cyber attackers had not yet gazed upon the shipping industry. After very serious and especially damaging hacker attacks either on shipping companies or on the ships of their fleets, IMO-based bodies have initiated the relevant procedures and legislated on the serious issue of cyber security. With the entry of 2021, when the implementation of the legislation was a fact, an expectation was born that the legislative framework will have a positive impact on addressing cyber risks.

It is therefore appropriate to note the first impacts of the legislation on this new problem and, if necessary, at any appropriate time to make any new legislative interventions and to be able to correct incorrect texts in a timely manner. During this process of continuous monitoring and timely readdressing, it is believed that gradually the issue of cyber threats will be under control so that the shipping industry can feel complete in this area.

Through the present study it was shown that the issues of legislation and best practices related to cyber security in the shipping industry are of vital importance. In this direction, after some basic definitions were provided, current legislation was provided at both global and European level.

In 2017, the IMO issued the MSC-FAL.1 / Circ.3 themed "Guidelines for the Management of Marine Cyber Risks". These guidelines provided high-level recommendations for the protection against current and emerging threats and vulnerabilities in cyberspace, including functional components to support effective cyber risk management. The IMO then approved these guidelines through Resolution MSC.428 (98) entitled "Maritime cyberspace risk management in security management systems". This resolution encouraged administrations to ensure that cyber threats were properly addressed.

Best practices are designed for developing an understanding and awareness of key aspects of security in cyberspace and are not intended to

provide technical guidance for the ship or the personnel on board. These practices, as guidelines, focus on separate issues on board and undertake a high level of commitment from the company ashore. In general, they provide guidance to ship owners and operators on how to evaluate their functions and how to develop the necessary procedures and actions to improve and maintain resilience and integrity of the systems on their ships. It has to be emphasized that best practices are non-binding proposals as the official IMO legislation is.

RECOMMENDATIONS

Focusing on IMO legislation, as the most basic tool that the ship industry possesses, it is worth pointing out that, as it is written, it is extremely abstract and general. This fact does not help those who they are going to comply with the law, move within specific and more "tangible" frames. It is normal therefore that ship owners and ship managers not knowing clearly and precisely, what actions they should take in order to effectively deal with the issue of cyber security.

It is therefore considered necessary to provide clear directives - from both states and legislators - that are specific and descriptive. This will help ship owners, as recipients of the legislation, to fully understand what they need to do to protect their fleet and company from the dangers dwelling in cyberspace.

There will definitely be more costs in terms of equipment and staff that is specialized or will acquire the necessary knowledge on the subject. There is also a bureaucratic issue in the sense of a Risk Assessment should be done to be able to deal with the new danger. For this reason, and based on the clarity of the legislation, it is crucial for ship owners to have specific directions that will help them to proceed as far as possible within the legislative framework but also to deal with any costs, either financial or bureaucratic that may arise.

Legislation, being more specific and descriptive, will make all necessary measures and procedures clearer for the forthcoming inspection. It is essential to quantify the risk factors in cyberspace, so that the inspector who will carry

out the inspection can control "measurable" figures, and to be able to carry out valid decisions. The preparation therefore of a Risk Assessment, is necessary to be as clear and descriptive as possible so that the inspector based on the data and results will know what to do and what to decide.

A key issue in all this is the training of the crew on matters of cyber risk. At the moment the crew of a ship, officially, does not follow any kind of cyber security training. At the same time, onboard personnel, receive training on other topics such as navigation, safety for property, etc. It is therefore imperative to provide specific training procedures on the subject of cyberspace. The IMO is currently creating legislation for education through a subcommittee - the MSC core committee - called Human element, Training and Watchkeeping (HTW).

AREAS OF FUTURE RESEARCH

A period of significant changes in the shipping industry is expected until 2030. The so-called 4th industrial revolution, which already greatly affects the daily lives of people on land, is taking its first dynamic steps in shipping. The unmanned terminals in the ports are constantly multiplying, while in the shipyards the demand for workers is decreasing due to the dynamic entry of automation, robotics and communication in the industry. "Green" ships, autonomous ships, smart ships, digitization, Internet of things, blockchain and the diffusion of information, artificial intelligence, robotics, are the next challenges for the shipping industry. This is because all the above mentioned are very closely related to cyber security.

A key issue that has to be considered in future research is Maritime insurance. Maritime insurance, with regard to cyber risk coverage, must act in parallel with the subsidiary protection measures taken by each company. Its importance is great, as it will relieve companies by providing protection against the financial impact of a cyber attack and helping those who fight daily for data security and protection. However, insurers remain wary of cyber risks, mainly due to their complex nature and their innumerable and unpredictable consequences.

REFERENCES

Aboul-Dahab, K. M. A. (2020). Demonstrating the cyber vulnerabilities of significant maritime technologies to the port facilities and on board of vessels. *information technology*, *29*, 31.

Androjna, A., & Twrdy, E. (2020). Cyber threats to maritime critical infrastructure. *Cyber Terrorism and Extremism as Threat to Critical Infrastructure Protection; Ministry of Defence Republic of Slovenia: Ljubljana, Slovenia*.

Awan, M. S. K., & Al Ghamdi, M. A. (2019). Understanding the vulnerabilities in digital components of an integrated bridge system (IBS). *Journal of Marine Science and Engineering*, *7*(10), 350.

BIMCO. (2016). *The Guidelines on Cyber Security Onboard Ships*. BIMCO.

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

Burmester, C. (2005). International Ship and Port Facility Security (ISPS) Code: the perceptions and reality of shore-based and sea-going staff. *Maritime Security and MET*, 185-194.

Caponi, S. L., & Belmont, K. B. (2015). Maritime cybersecurity: a growing threat goes unanswered. *Intellectual Property & Technology Law Journal*, *27*(1), 16.

Chang, C. H., Wenming, S., Wei, Z., Changki, P., & Kontovas, C. A. (2019, November). Evaluating cybersecurity risks in the maritime industry: a literature review. In *Proceedings of the international association of Maritime Universities (IAMU) Conference*.

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *The TQM Journal*.

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

Geister, R. M., Buch, J. P., Niedermeier, D., Gamba, G., Canzian, L., & Pozzobon, O. (2018). Impact study on cyber threats to GNSS and FMS systems.

Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. *Wired, August*, *22*.

Guard, U. C. (2005). National Plan to achieve Maritime Domain Awareness. *Washington, DC*.

Hayes, C. R. (2016). *Maritime cybersecurity: the future of national security* (Doctoral dissertation, Monterey, California: Naval Postgraduate School).

Heering, D. (2020). Ensuring Cybersecurity in Shipping: Reference to Estonian Shipowners. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, *14*(2).

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 65-98.

Karamperidis, S., Kapalidis, C., & Watson, T. (2021). Maritime Cyber Security: A Global Challenge Tackled through Distinct Regional Approaches. *Journal of Marine Science and Engineering*, *9*(12), 1323.

Katsikas, S. K. (2017, April). Cyber security of the autonomous ship. In *Proceedings of the 3rd ACM workshop on cyber-physical system security* (pp. 55-56).

Kessler, G. C., Craiger, J. P., & Haass, J. C. (2018). A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, *12*(3), 429.

Kettani, H., & Cannistra, R. M. (2018, October). On cyber threats to smart digital environments. In *proceedings of the 2nd international conference on smart digital environment* (pp. 183-188).

Kettani, H., & Wainwright, P. (2019, March). On the top threats to cyber systems. In *2019 IEEE 2nd international conference on information and computer technologies (ICICT)* (pp. 175-179). IEEE.

Lee, A. & Wogan, H. (2018). Jones Walker LLP Maritime Cybersecurity Survey. Available from: https://www.joneswalker.com/en/insights/jones-walker-maritime-cybersecurity-survey.html

Lehto, M. (2021). Cyber security challenges in aviation and maritime. *Cyberwatch Magazine*, *2021*(2).

Lovell, K. N., & Heering, D. (2019, June). Exercise Neptune: MaritiMe cybersecurity training using the navigational siMulators. In *Proceedings of the 5th Interdisciplinary Cyber Research Conference* (p. 34).

Manesh, M. R., Kenney, J., Hu, W. C., Devabhaktuni, V. K., & Kaabouch, N. (2019, January). Detection of GPS spoofing attacks on unmanned aerial systems. In *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)* (pp. 1-6). IEEE.

Miranda Silgado, D. (2018). Cyber-attacks: a digital threat reality affecting the maritime industry.

Mraković, I., & Vojinović, R. (2019). Maritime cyber security analysis–How to reduce threats?. *Transactions on maritime science*, *8*(01), 132-139.

Mraković, I., & Vojinović, R. (2020). Evaluation of Montenegrin Seafarer's Awareness of Cyber Security. *Transactions on Maritime Science*, *9*(02), 206-216.

Pajunen, N. (2017). Overview of maritime cybersecurity.

Pelton, J. N. (2019). The Growth and Expansion of Precise Navigation and Timing. In *Space 2.0* (pp. 47-58). Springer, Cham.

Rana, A. (2019). Commercial maritime and cyber risk management. *Safety & Defense*, *5*(1), 46-48.

Razzaq, A., Latif, K., Ahmad, H. F., Hur, A., Anwar, Z., & Bloodsworth, P. C. (2014). Semantic security against web application attacks. *Information Sciences*, *254*, 19-38.

Ringsberg, A. H., & Cole, S. (2020). Maritime security guidelines: a study of Swedish ports' perceived barriers to compliance. *Maritime Policy & Management*, *47*(3), 388-401.

Saravanan, K., Aswini, S., Kumar, R., & Son, L. H. (2019). How to prevent maritime border collision for fisheries?-A design of Real-Time Automatic Identification System. *Earth Science Informatics*, *12*(2), 241-252.

Suppiah, R. (2009). International Ship and Port Facility Security (ISPS) code and crew welfare. *Maritime Affairs: Journal of the National Maritime Foundation of India*, *5*(1), 57-72.

Svilicic, B., Kamahara, J., Celic, J., & Bolmsten, J. (2019). Assessing ship cyber risks: A framework and case study of ECDIS security. *WMU Journal of Maritime Affairs*, *18*(3), 509-520.

Tam, K., & Jones, K. (2018, June). Cyber-risk assessment for autonomous ships. In *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-8). IEEE.

Thomas, J. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business Management*, *12*(3), 1-23.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data

collecting companies. *Computer Law & Security Review*, *34*(1), 134-153.

Trautman, L. J., & Ormerod, P. C. (2016). Corporate directors' and officers' cybersecurity standard of care: The Yahoo data breach. *Am. UL Rev.*, *66*, 1231.

Tusher, H. M., Munim, Z. H., Notteboom, T. E., Kim, T. E., & Nazir, S. (2022). Cyber security risk assessment in autonomous shipping. *Maritime Economics & Logistics*, 1-20.

Tusher, H. M., Munim, Z. H., Notteboom, T. E., Kim, T. E., & Nazir, S. (2022). Cyber security risk assessment in autonomous shipping. *Maritime Economics & Logistics*, 1-20.

Walker, M. (2012). CEH certified ethical hacker exam one: all in one.