Maritime Cyber Security

Submitted: 15 November, 2023
Reviewed: February 10, 2024
Revised: February 12, 2024
Accepted: February 14, 2024

Ekaterina Anyanova[*]
https://orcid.org/0000-0003-4478-5324

DOI: https://doi.org/10.26512/lstr.v16i2.47018

Article submitted to peer blind review

Abstract

[Purpose] The threat of cyber-attacks is very acute. The purpose of this paper is to examine the need of the amendment of rules of international law required for the cyber resilient enterprise.
[Methodology] This paper proposes a novel approach investigating whether the amendment of rules of international law is required for the cyber resilient enterprise. The methodology of international legal research and analysis of data is applied.
[Findings] The analyses in this paper show the impact of the cyber security on the shipping industry. The proposals of documents on cyber security and recommendations for maritime cyber risk management are discussed.
[Practical Implications] This study is useful for practitioners to consider and evaluate the cyber security. This study is useful for graduate students as well.
[Originality] Although some research is being conducted in this area, maritime cybersecurity has not been deeply investigated. This paper presents a detailed analysis of legal documents and research published in international studies on the law of cyber security for maritime industry highlighting security problems and challenges.

Keywords: Cybersecurity. Ports. Shipping. Maritime Industry. The International Ships and Port Facilities Security (ISPS) Code.

INTRODUCTION

Cyber incidents damage ship operations, cause financial losses. Cyber threats for maritime industry should not be underestimated.

Maritime industry including shipbuilders and ports has become increasingly vulnerable to cyber threats. Cyberattacks have been rapidly increasing over the years. Cybersecurity is the primary example of a developing maritime security threat. Maritime cyber risk is a potential threat to damage shipping-related operations, safety or security systems, their information.

[*] LL.M and Dr. Juris, Candidate of Juridical Science, Legal Consultant (Kaliningrad, Russian Federation). Address: 236022 Russia Kaliningrad ul. Repina 18-11. E-mail: ekaterina.anyanova@gmail.ru.

This paper will present how to shape cyber security toward international law. The problem of cybersecurity threat for shipping is considered. First, it explores cybersecurity concepts, cybersecurity risks and basics of the cyber risk management. The normative description of cyber security is examined. Second, it assesses cyber attacks examples.

Then it will explore cyber security concept under the principles of international law addressing cyber attacks in shipping. The paper then studies provisions on cyber security in the International Ships and Port Facilities Security (ISPS) Code. In this study juridical methodology and tools help the analysis of legal concepts of information and communication technology (ARANHA, 2011, p. 11), especially the concept of maritime cyber security.

Research methods have been used to analyse law on cyber security, examples of cyber attacks, international legal documents on cybersecurity such as the ISPS Code and the International Maritime Organization (IMO) guidance, countermeasures in cyber security.

Finally, a series of recommendations are made for maritime cyber risk management.

Cybersecurity for the maritime industry is particularly addressed at international level since 2017 by means of such documents as guidelines and recommendations (Port cybersecurity - Good practices for cybersecurity in the maritime sector, 2019, p. 12). However, there is no mandatory requirements. Documentary part of international law on cybersecurity in shipping is scarce. The issue of cyber security is a gap in the security of ships and port facilities.

Ports are active participants of global trade (IAPH Cybersecurity Guidelines for Ports and Port Facilities, Version 1.0, 2021, p. 10). At present in the maritime industry the digitalization, automation (SENARAK, 2021) and use of networks and online technologies increase (NAVAL DOME: MARITIME CYBERATTACKS UP 900 PERCENT IN THREE YEARS – PROFESSIONAL MARINER, 2023). But intelligent technologies reduce port laborers, increase efficiency, but face cyberthreat (SENARAK, 2021). These technologies are under the threat of cybercrimes (HACKING ATTACK IN PORT OF BARCELONA, 2018; THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY, 2023; POLICE WARNING AFTER DRUG TRAFFICKERS' CYBER-ATTACK, 2023).

Not being prepared for a cyber incident (OTHER MARITIME SECURITY THREATS, 2023) may result in the information systems being damaged (Maritime cyber risk, 2019). It may even have implications on the environment when the dangerous goods are transported (THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, VERSION 4, 2023).

Due to these incidents prevention of cyberattack became very important (SENARAK, 2021). The increased number of maritime cybersecurity incidents demonstrated the need to increase cybersecurity measures (Maritime cyber priority, 2023, p. 8).

Among the proposed counter measures there is a cyber risk management, which should be incorporated into the safety management system (MSC.428(98)). Besides after the number of cyber incidents increased, the companies started to take offline e-commerce platforms and data centres (Maritime cyber priority, 2023, p. 8). It is important to apply this concept as wide as possible.

In this article the special features of the regulation of the cyber security and the final purpose of these security measures - cyber resilient shipping industry are examined.

CYBERSECURITY THREAT FOR SHIPPING

Cyber security means a security concept used to protect the cyber environment, organisation and user (Code of Practice Cyber Security for Ships, 2017).

Cybersecurity for the maritime industry is particularly addressed at international level since 2017 by means of such documents as guidelines and recommendations (Port cybersecurity - Good practices for cybersecurity in the maritime sector, 2019, p. 12). However, there is no mandatory requirements. The issue of cyber security is a gap in the security of ships and port facilities.

The threat of cyber-attacks is very acute (DE FARIA, 2020, p. 164). Cyber threats for maritime industry should not be underestimated. Nowadays, the maritime industry, including shipbuilders and ports has become increasingly vulnerable to cyber threats (IAPH Cybersecurity Guidelines for Ports and Port Facilities, Version 1.0, 2021, p. 9).

Cyber incidents damage ship operations, cause financial losses (THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, VERSION 4, 2023).

Ports are active participants of global trade (IAPH Cybersecurity Guidelines for Ports and Port Facilities, Version 1.0, 2021, p. 10) from the perspective of the information revolution (ARANHA, CHACON, OLIVEIRA, 2014, p. 313). At present in the maritime industry the digitalization, automation (SENARAK, 2021) and use of networks and online technologies increase (NAVAL DOME: MARITIME CYBERATTACKS UP 900 PERCENT IN THREE YEARS – PROFESSIONAL MARINER, 2023). Intelligent technologies became part of the operation of ports and ships. Ships use information technologies (IT), which are networked together and connected to the internet. Such technologies reduce port laborers, increase efficiency, but face cyberthreat (SENARAK, 2021). These technologies are under the threat of cybercrimes (HACKING ATTACK IN PORT OF BARCELONA, 2018; THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY, 2023; POLICE WARNING AFTER DRUG TRAFFICKERS' CYBER-ATTACK, 2023).

A cyber security incident is likely to arise from unauthorised access to, misuse or fraudulent use of port or ship systems, malicious attack to network on ship including via removable media (OTHER MARITIME SECURITY THREATS, 2023). Such systems could be accesed via cellular connections, WiFi (NAVAL DOME: MARITIME CYBERATTACKS UP 900 PERCENT IN THREE YEARS – PROFESSIONAL MARINER, 2023). The vulnerabilities in the shipping industry could be caused by outdated software or ineffective firewalls, weak passwords, the absence of network segregation, inappropriate use of removable media such as a USB and memory stick (para 2.1.4-2.1.6 Guidelines on maritime cyber risk management).

A cyber security incident may result in loss or theft of assets, including documents and storage media; unauthorised access to data or information; loss, compromise, unauthorised manipulation or change of data or information; loss or compromise of ship assets connected to its systems; planting of bugs or other surveillance devices; and insertion of malicious software (Code of Practice Cyber Security for Ships, 2017).

The Internet may be used by terrorists to distribute propaganda and for communications purposes electronic and computer-based technologies to disrupt or damage ships by attacking ship and/or connected shore-based systems, also exploit poorly secured ship data to enable remote hostile reconnaissance of targets, thus reducing the time they need to spend in or near their target (Code of Practice Cyber Security for Ships, 2017).

Such systems are vulnerable for cyber-attacks. Advanced technologies mean controlling them from a remote-control station, e.g., using remote-control cranes, self-driving trucks. Ports use technologies to automate and digitalize their operation activities, in particular in port operation, loading and unloading operations, cargo handling, navigation, electronic customs service, the automatic identification system, the X-ray and gamma-ray imaging systems, uncrewed vehicles and equipment. Cybertechnologies are used in cranes; management systems; propulsion and machinery management and power control systems; access control systems; passenger servicing and management systems; bridge systems; the engine room (DE FARIA, 2020, p. 164); public networks; administrative and crew welfare systems; communication systems (IMO Guidelines on maritime cyber risk management. MSC-FAL.1-Circ.3-Rev.2, 2022, para. 2.1.5.); vessel berthing systems, safety and security systems, etc. (para 2.1.1 Guidelines on maritime cyber risk management).

Cyberthreats cover threats of cyber criminality, cyber espionage, cyber terrorism (SENARAK, 2021), phishing attacks redirecting legitimate payments.

Not being prepared for a cyber incident (OTHER MARITIME SECURITY THREATS, 2023) may result in the information systems being damaged (Maritime cyber risk, 2019). It may even have implications on the environment when the dangerous goods are transported (THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS, VERSION 4, 2023).

CYBER ATTACKS EXAMPLES

The number of reported incidents of cyberattacks on the maritime industry increased in the last years.

For example, the ‘NotPetya’ attack on Maersk caused loss approximately $300 million (Maritime cyber priority, 2023, p. 8). In July 2017, the Danish shipping company in container transport “MAERSK” was attacked by the

"NotPetya" ransomware. This malware had already attacked the Dutch company TNT Express in June 2017.

The NOT PETYA virus originated in a small Ukrainian software company. The programme came to the Maersk terminal in Rotterdam from the Ukrainian branch of Maersk which had this software on one of their computers. This attack disabled the terminal, and port terminal operations were managed manually for more than two weeks (Port cybersecurity - Good practices for cybersecurity in the maritime sector, 2019, p. 33). Through the connected device in their network the programme damaged Maersk's systems worldwide (DRYAD: OLD TOOLS VS NEW THREATS?, 2023).

In 2013, the port of Antwerp was attacked via the remote access to the terminal systems and containers were stolen (HACKING ATTACK IN PORT OF BARCELONA, 2018; THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY, 2023; POLICE WARNING AFTER DRUG TRAFFICKERS' CYBER-ATTACK, 2023).

In 2016 the navigation systems of approximately 280 vessels were disrupted in one of the most digitally developed countries in the world - South Korea.

In 2017 76 APM Terminals in the United States, India, Spain, and the Netherlands were attacked by cyber-criminals.

In 2018 the ports of Barcelona, Australian defense shipbuilder Austal, customer service centre of COSCO Shipping Lines terminals in Long Beach Port and Port of San Diego in the United States (SENARAK, 2021) were attacked.

In 2020 the Geneva HQ (Maritime cyber risk, 2019) of shipping major like Mediterranean Shipping Company was attacked by a malware. As a result of this attack its customer website did not function for several days.

French container shipping major CMA CGM was also attacked by cyber-criminals in 2020 and 2021. In 2020 the cyber-attack of the Iran's Shahid Rajaee port in the Strait of Hormuz created traffic jams of delivery trucks and delays in shipments (MARITIME BUSINESSES SEE FOURFOLD INCREASE IN CYBER ATTACKS SINCE FEBRUARY: ASTAARA, 2023).

In 2022 Sea-Invest, one of the largest Belgian-based port terminals has shut down all operations due to a hacking attack.

In 2022 a Singapore shipbuilder Sembcorp Marine was attacked by an unauthorized user, who gained access to the IT network through third-party software. IT system of a Singapore maritime company Voyager Worldwide was attacked in December 2022.

The website and internal computer system of the Port of Lisbon were disrupted in December 2022 and did not work for several days after a cyberattack.

Norwegian shipping classification society *Det Norske Veritas* (DNV) was attacked by a ransomware attack in 2023 (MARITIME CYBERSECURITY ATTACKS ON THE RISE - MARPOINT, 2023). The IMO was also attacked in 2020 and 2023. The Port of Los Angeles is constantly attacked by ransomware, malware and spear-phishing attacks.

Due to these incidents prevention of cyberattack became very important (SENARAK, 2021). After the number of such incidents increased, the companies started to take offline e-commerce platforms and data centres (Maritime cyber priority, 2023, p. 8).

INTERNATIONAL LAW USED TO ADRESS CYBER ATTACKS IN SHIPPING

Documentary part of international law on cybersecurity in shipping is scarce.

The IMO's Guidelines on maritime cyber risk management were adopted in 2017 (IMO Guidelines on maritime cyber risk management. MSC-FAL.1-Circ.3-Rev.2, 2022) and put into effect in 2021 in order to combat cyber threats in the shipping industry.

The cyber guidelines contained recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities (Port cybersecurity - Good practices for cybersecurity in the maritime sector, 2019, p. 12). The recommendations are complementary to the safety and security management practices already established by IMO (Maritime cyber risk, 2019). The International Safety Management (ISM) Code is the legal foundation for those guidelines (PORT CYBERSECURITY: INCORPORATING THE IAPH'S NEW GUIDELINES INTO THE ISPS CODE, 2023).

Cybertechnologies and operational systems in the shipping are interconnected. Such interconnecting leads to cyber risks (para 2.1.1 Guidelines on maritime cyber risk management).

Para. 2.1.8 of Guidelines emphasizes that the computer technologies are rapidly changing, therefore it is difficult to address these risks only through technical standards. A risk management approach to cyber threat is recommended in addition to the existing safety and security measures.

Shipping operations must be based on the risk management, including cyber risk management (para 1.4 Guidelines on maritime cyber risk management). The Guidelines on maritime cyber risk management contain recommendations for maritime cyber risk management (para 1.1. Guidelines on maritime cyber risk management).

Para. 18 of Guidelines emphasizes that the risk management approach is necessary for the cyber security of shipping due to the reliance of the shipping operations on digitization, network-based systems (MSC 104/7/1). The document is intended to safeguard the shipping from cyber threats arising from digitization, integration and automation of processes and systems in shipping (para 1.2 Guidelines on maritime cyber risk management)

These guidelines recognize that all organizations in the shipping industry shall refer to Member Governments' and Flag Administrations' requirements and relevant international or industry standards and best practices (e.g. The Cybersecurity Framework 2.0 of the National Institute of Standards and Technology, ISO/IEC 27001 standard for information security management systems) in order to address the most relevant security measures (Port cybersecurity - Good practices for cybersecurity in the maritime sector, 2019, p. 13).

The Resolution MSC.428(98) adopted by the Maritime Safety Committee (MSC) on 16 June 2017 concerns Maritime Cyber Risk Management in Safety Management Systems (Maritime cyber risk, 2019). The Resolution recognizes the urgent need to raise awareness on cyber risk threats and vulnerabilities. An approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code.

Additional guidance and standards include the Guidelines on Cyber Security Onboard Ships. The document was produced and supported by the International Chamber of Shipping (ICS), the International Union of Marine Insurance e.V. (IUMI), Baltic and International Maritime Council (BIMCO), the Oil Companies International Marine Forum (OCIMF), the International Association of Indepedent Tanker Owners (INTERTANKO), the International Association of Dry Cargo Shipowners (INTERCARGO), International Ship Managers' Association (INTERMANAGER)**, t**he World Shipping Council (*WSC*)**, t**he Superyacht Builders Association (SYBAss)**.**

The Cybersecurity Guidelines for Ports and Port Facilities were developed by the International Association of Ports and Harbors (IAPH) in 2021. The document was presented at the 104th session of the IMO MSC in 2021. This document contains cyber security measures for the maritime transportation sector including personnel cybersecurity training and exercises, regular cybersecurity assessments and developing cyber security plans (CSPs), proper staffing, threat detection, and incident response and reporting.

CYBER SECURITY IN THE ISPS CODE

In order to ensure the security of port facilities against attacks from within the cyber domain, it is proposed to use the ISPS Code (PORT CYBERSECURITY: INCORPORATING THE IAPH’S NEW GUIDELINES INTO THE ISPS CODE, 2023).

The ISPS Code was added to the Safety of Life at Sea (SOLAS) Convention in 2002 with maritime security mandatory requirements and recommendations that ships and port facilities must follow. The ISPS Code was developed in direct response to the 9/11 attacks in the United States on the global transportation system. It contains the IMO’s comprehensive mandatory security regime.

The ISPS Code takes the approach that ensuring the security of ships and port facilities is a risk management activity and determines what security measures are appropriate, an assessment of the risks must be made in each particular case. The Code provides a framework for the assessment and detection of possible security threats to ships or port facilities. It applies to vessels engaged in international voyages including passenger vessels, cargo vessels of 500 gross tonnage and above, mobile offshore drilling units, and port facilities (DRYAD: OLD TOOLS VS NEW THREATS?, 2023).

One of the objectives of the ISPS Code (para 1.2.) is to to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade.

The ISPS Code requires ports to design a Port Facility Security Assessment (PFSA) to identify possible threats and countermeasures and a Port Facility Security Plan (PFSP) to identify for different security levels the measures to be put in place and the actions to be undertaken. The PFSA must address within a port facility, the following aspects: physical security, structural integrity, personnel protection systems, procedural policies, radio and telecommunication systems, including computer systems and networks and relevant transportation infrastructure. The PFSP must address access to the port facility, restricted areas within the port facility, handling of cargo, delivery of ship's stores and monitoring the security of the port facility.

The risk management activities in the ISPS Code cover mostly physical risks (Cyber security in ports business as usual?, p. 2). This instrument contains some regulations on computer systems and networks.

The ISPS Code has two parts: a mandatory Part A and a recommendatory Part B. There are no cybersecurity provisions in Part A.

Part B mentions cybersecurity as it encourages port facilities to consider "radio and telecommunications equipment, including computer systems and networks" in the assessment of physical security vulnerabilities. The cybersecurity provisions in Part B of the ISPS Code are soft law. This is non-binding instructive guidance (PORT CYBERSECURITY: INCORPORATING THE IAPH'S NEW GUIDELINES INTO THE ISPS CODE, 2023).

The provisions on the PFSA among other elements of a port facility regulate radio and telecommunication systems, including computer systems and networks (ISPS Code, Part B, 15.3 sub 5).

The mandatory part A of the ISPS Code in cl. 15.5. stipulates that the port facility security assessment shall include, at least, the following elements: identification and evaluation of important assets and infrastructure; possible threats to them and weaknesses, including human factors in the infrastructure, policies and procedures; counter measures. Although these provisions on the PFSA do not directly mention the cyber area, in the PFSA it shall be identified, when computer systems and network pose a cyber threat to the ship/port (Port Community Cyber Security, 2020).

COUNTER MEASURES

Cyber security means a security concept used to protect the cyber environment, organisation and user (Code of Practice Cyber Security for Ships, 2017).

The increased number of maritime cybersecurity incidents demonstrated the need to increase cybersecurity measures (Maritime cyber priority, 2023, p. 8).

Cyber risk management should be incorporated into the safety management system (MSC.428(98)).

The goal of the cyber security measures is cyber resilient ships (Recommendation on Cyber Resilience. Corr2, 2022).

In order to ensure safe and secure shipping cyber risk management is applied (Maritime cyber risk, 2019). The cyber risk management includes the processes of identifying, analysing, assessing a cyber-related risk.

It is necessary to apply a risk management approach (IMO Guidelines on maritime cyber risk management. MSC-FAL.1-Circ.3-Rev.2, 2022), since IT technologies are constantly changing.

Besides after the number of cyber incidents increased, the companies started to take offline e-commerce platforms and data centres (Maritime cyber priority, 2023, p. 8). It is important to apply this concept as wide as possible.

The counter-measures shall be aimed at reducing the risk of unauthorised access to the ship including its cyber-physical systems. The protection from unauthorised access includes measures to check any removable media or portable devices that will be connected to the system for malware (for example, software updates on USB memory sticks or diagnostic software on laptops or tablet devices). Access to systems consoles, displays, etc. shall be password protected.

A special attention shall be paid to cabling routes and their containment (for example ducts and trunking); control systems; critical permanent plant or machinery (Code of Practice Cyber Security for Ships, 2017).

A series of recommendations are made for maritime cyber risk management. Proposals of measures to be taken to protect against a cyber incident in the maritime industry.

It is proposed to develop new cybersecurity guidelines for maritime domain with the participation of the IMO. Sometimes the proposals are made to amend the ISPS Code and to cover cybersecurity standards for ports and port facilities (PORT CYBERSECURITY: INCORPORATING THE IAPH'S NEW GUIDELINES INTO THE ISPS CODE, 2023).

The proposed amendments of the ISPS Code consider certain threats and include enforceable cybersecurity rules in order the ISPS Code to be an effective instrument against threats in the cyber domain.

Since port systems become more connected and digitalised, it is important to build security and resilience into processes and training (MARITIME BUSINESSES SEE FOURFOLD INCREASE IN CYBER ATTACKS SINCE FEBRUARY: ASTAARA, 2023).

One proposal concerns the amending Part B Section 18 to encompass training, drills, and exercises specific to cybersecurity. Such cyber-specific requirements do not presently exist. Section 18 do not cover cybersecurity training, skills and exercises, but covers areas, where the Port Facility Security Officer and Port facility personnel with specific security duties, all other port facility personnel should have knowledge and receive training, the objective and number of different types of drills and exercises.

Another proposal concerns the port facility security assessment. Cyber systems are not covered in the port facility security assessment. Such assessment shall include, at least, the identification and evaluation of important assets and infrastructure, possible threats and weaknesses, counter measures and procedural changes and their level of effectiveness in reducing vulnerability (clause 15.5 Part A). Section 15 of Part B contains rules on port facility security assessment, the elements and fields which should be addressed in the PFSA. For these purposes identification and evaluation process is carried out. Assets and infrastructure that should be considered important to protect include radio and telecommunication systems and computer systems and networks (clause 15.8, Part B). Identification of vulnerabilities should include consideration of measures to protect radio and telecommunication equipment, port services and utilities, including computer systems and networks (clause 15.16.5 Part B). Section 15 of Part A and Part B might be amended to expressly require a cybersecurity assessment to be carried out. The cybersecurity assessment would be separate from and a complement to the facility security assessment already required by Section 15 of the code.

The rules on Ship Security Assessment (SSA) carried out for each of the ships in the Company's fleet (clause 8.1 part A) propose to address physical security; radio and telecommunication systems, including computer systems and networks; and other areas (clause 8.3.). Those involved in a SSA should have expert knowledge on radio and telecommunications systems, including computer systems and networks (clause 8.4.11.).

In Part B of the ISPS Code, paragraphs 8.1 to 8.10 provide measures to be included in the SSA, for example the assessment of the vulnerabilities including any security equipment and systems, including telecommunication systems (para 8.10.5), (including computer systems and networks), and other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations on board the ship or within a port facility.

One of the main ideas of the proposed measures is to carry out a cyber security assessment (CSA). It is recommended that qualified and experienced individuals carry out the CSA. It is even proposed to review the maritime security rules in this regard.

On the basis of this ruling ship's CSA shall be carried out. During the cyber security assessment, a risk management is applied. The attention shall be paid also on the human factors, and weaknesses in the infrastructure and procedures (Code of Practice Cyber Security for Ships, 2017). On the basis of the ship security assessments a CSP shall be developed.

Another proposal to amend the ISPS Code is a change to Section 16 of Part A and Part B to require port facilities to prepare and governments to approve CSPs. The CSP should be an independent document, a supplement to the already required facility security plan (PORT CYBERSECURITY: INCORPORATING THE IAPH'S NEW GUIDELINES INTO THE ISPS CODE, 2023).

CSP shall be based on a risk-based approach (Code of Practice Cyber Security for Ships, 2017). CSP shall include regular training and cyber risk assessment for persons having access to cyber systems. The completed CSP for the ship should be protected from unauthorised access or disclosure and should form an annex of the ship security plan (SSP).

CSP shall contain a mechanism for periodic, at least annual, reviews of the CSP to verify that it remains effective and update it.

In order to promote the cyber security management, the proposal was made to designate the cyber security officer (CySO). This CySO shall be responsible for all security aspects of cyber-enabled systems on the ship, i.e. both the IT and communications systems. The CySO should also be responsible for the development of the CSA/CSP and implementing the CSP.

The CySO shall have the authority to act (Code of Practice Cyber Security for Ships, 2017), but it is important that the responsibility for cybersecurity is shared by the CySO with other managers. Not only the IT department shall participate in the cyber security measures, but also port executives, managing governance in order to build an organizational culture and develop cybersecurity strategies.

Such position of CySO is introduced in certain places. For example, in the Rotterdam port the Port Security Officer has recently also been appointed Cyber Resilience Officer. However, this position is not required by the ISPS Code (Cyber security in ports business as usual?, p. 2).

In such a way, it is proposed to amend the provisions of the SOLAS Convention and the ISPS Code with the cyber security provisions (DE FARIA, 2020, p. 178). The question arises whether it is necessary to introduce additional measures regulating the cyberthreat in the ISPS Code. The amendment of the ISPS Code is a difficult procedure. Part B of the ISPS Code contains a series of recommendations. The amendments to the Part B of the Code shall be adopted by the MSC in accordance of the rules of its work. Part A of the Code is mandatory. The amendments to the Part A of the ISPS code are adopted after consideration within the Organization and voting in the MSC. The Part A of the ISPS code could also be amended by a convened Conference of Contracting Governments to consider amendments to the present Convention.

The conclusion is made that the amendment of the ISPS Code is not advisable, since the ship and port facility security could be achieved by the existing regulation. However, these cyber threats shall be considered of the work and activity of maritime industry. It is possible to imagine, one could carry out the necessary procedures for computer systems and networks of ship or enterprise without the amendment of the ISPS Code.

CYBERSECURITY THREAT FOR SHIPPING

Cyber security means a security concept used to protect the cyber environment, organisation and user (Code of Practice Cyber Security for Ships, 2017).

CONCLUSIONS

Nowadays the maritime industry has become increasingly vulnerable to cyber threats. This paper argues that recent examples from the shipping industry have demonstrated that cyber incidents have the potential to disturb ship operations and cargo management and cause significant financial losses, reputational damage. Cyberattacks could result in the lack of control of dangerous goods and damage the safety of people and environment. Terrorists could make use of the Internet to distribute propaganda and for communications purposes.

The modern technologies for the bridge, the engine room and the whole vessel in general make shipping dependent on IT. Cybercriminals can access the cranes, storage and operational systems.

The numerous cyber-attacks demonstrated the vulnerability of the maritime industry, for example, a cyberattack in 2020 at the Shahid Rajaee port in the Strait of Hormuz (created traffic jams of delivery trucks and delays in shipments), a cyberattack in 2017 with the "NotPetya" ransomware at the shipping company in container transport (the Danish "MAERSK") (damaged its information technology systems for several weeks), cyberattacks in the early 2020s at the shipping majors like Cosco, MSC and CMA CGM (took e-commerce platforms and vital data centres offline), a cyberattack in January 2023 at Norwegian shipping classification society DNV (a ransomware on the servers of its software), cyberattacks in 2022 and 2023 at the Port of Los Angeles (ransomware, malware and spear-phishing incidents). In 2022 maritime cybersecurity incidents occurred at Singapore shipbuilder Sembcorp Marine (an unauthorized access to the network), the Port of Lisbon (a cyberattack on the port's website and internal computer system).

Maritime organizations also face such cybersecurity risks as phishing attacks.

The security of shipping industry against cyber-attacks is regulated by international legal instruments including the ISPS Code. The Code recommends a risk management approach to cyber risks, however does not encompass a CSA and CSPs. The numerous proposals to amend the ISPS Code regarding the cybersecurity requirements are made. It is necessary to build cybersecurity rules into functional processes and training.

The shipping industry is not immune to cyber-attacks. The port facilities become ever more connected and digitalized. Since shipping industry is a part of global trade, maritime cybersecurity is very important for shipping industry.

The cyber resilient approach to ships and port facilities would require additional cyber security measures.

REFERENCES

Aranha, M. (2011). Hermeneutical Model for Identification of Juridical Variables in the ICT Comparative Research. *SSRN Electronic Journal* (May 2, 2011). Available at: http://dx.doi.org/10.2139/ssrn.2079096.

Aranha, M.; Chacon, G.; Oliveira, F. (2014). ICT Variables for Development in South America Through Federal Lenses. *SSRN Electronic Journal*. Available at: 10.2139/ssrn.2462565.

Code of Practice Cyber Security for Ships. [s.l.]: The UK Department for Transport, 2017. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf. 11 nov. 2023.

Dryad: Old Tools Vs New Threats?. [*S. l.: s. n.*], 2023. Available at: https://www.hellenicshippingnews.com/dryad-old-tools-vs-new-threats/. Acesso em: 11 nov. 2023.

Faria, D. L. De (2020). The impact of cybersecurity on the regulatory legal framework for maritime security. *Janus.net, e-journal of international relations*, v. 11 (1).

Hacking Attack In Port Of Barcelona. [*S. l.: s. n.*], 2018. Available at: https://www.securitynewspaper.com/2018/09/26/hacking-attack-in-port-of-barcelona/. 11 nov. 2023.

IAPH Cybersecurity Guidelines for Ports and Port Facilities, Version 1.0. IAPH. Disponível em: 02 sep. 2023. 11 nov. 2023.

IMO Resolution MSC.428(98). Maritime cyber risk management in safety management systems, 16 June 2017.

Maritime Businesses See Fourfold Increase In Cyber Attacks Since February: ASTAARA. [*S. l.: s. n.*], 2023. Disponível em: https://www.captiveinternational.com/services/actuarial-underwriting/maritime-businesses-see-fourfold-increase-in-cyber-attacks-since-february-astaara-3568. 11 nov. 2023..

Maritime Cyber Priority. DNV. Acesso em: 11 nov. 2023.

Maritime Cyber Risk. The IMO. Disponível em: https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx. 11 nov. 2023.

Maritime Cybersecurity Attacks On The Rise - Marpoint. [*S. l.: s. n.*], 2023. Disponível em: https://marpoint.gr/blog/maritime-cybersecurity-attacks-on-the-rise/.

Measures to Enhance Maritime Security. IAPH Cybersecurity Guidelines for Ports and Port Facilities, MSC 104/7/1, 2 July 2021: IMO Maritime Safety Committee, 2021.

Moerel, L.; Dezeure, F. Cyber security in ports business as usual? Disponível em: https://www.freddydezeure.eu/11-cybersecurity-in-ports-business-as-usual.

Naval Dome: Maritime Cyberattacks Up 900 Percent In Three Years – Professional Mariner. [*S. l.: s. n.*], 2023. Disponível em: https://professionalmariner.com/naval-dome-maritime-cyberattacks-up-900-percent-in-three-years/.

Other Maritime Security Threats. [*S. L.: S. N.*], 2023. Disponível Em: Https://On-Shore.Mschoa.Org/Media/1253/Other-Maritime-Security-Threats.Pdf.

Police Warning After Drug Traffickers' Cyber-Attack. [*S. l.: s. n.*], 2023. Disponível emCY: https://www.bbc.com/news/world-europe-24539417.

Port Community Cyber Security.: IAPH, 2020. Disponível em: https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf. 11 nov. 2023.

Port Cybersecurity - Good practices for cybersecurity in the maritime sector. European Union Agency for Cybersecurity (ENISA). 11 nov. 2023.

Port Cybersecurity: Incorporating the IAPH's New Guidelines into the ISPS Code | Center for International Maritime Security. [*S. l.: s. n.*], 2023. Disponível em: https://cimsec.org/incorporating-the-iaphs-new-cybersecurity-guidelines-into-the-international-ship-and-port-facility-security-code/.

Recommendation on Cyber Resilience. Corr2.: International Association of Classification Societies, 2022.

Senarak, C. (2021). Cybersecurity knowledge and skills for port facility security officers of international seaports: Perspectives of IT and security personnel. *The Asian Journal of Shipping and Logistics*, 37 (4), 345–360.

The Guidelines On Cyber Security Onboard Ships, Version 4. [*S. l.: s. n.*], 2023. Available at: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/ANNEX%20Guidelines%20on%20Cyber%20Security%20Onboard%20Ships%20v.4.pdf.

The IMO. IMO Guidelines on maritime cyber risk management. MSC-FAL.1-Circ.3-Rev.2. [s.l.: s.n.], 2022.

The Untold Story Of Notpetya, The Most Devastating Cyberattack In History. [*S. l.: s. n.*], 2023. Disponível em: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET