TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 14
Number 2
June 2020

DOI: 10.12716/1001.14.02.01

Ensuring Cybersecurity in Shipping: Reference to Estonian Shipowners

D. Heering
Tallinn University of Technology, Tallinn, Estonia

ABSTRACT: Ships, ports and offshore facilities are increasingly becoming dependent on modern information and opera-tional technology. Cyber incidents on ships can create disruptions of critical systems that cause problems for the ship's safe operation. Therefore, the shipowners must be prepared to cope with rising cyber threats. In or-der to prevent cyber incidents happening on ships and in the companies, essential steps must be taken on the management level. This paper introduces results of two surveys on cybersecurity and cyber awareness carried out in between 2017 – 2019 among the shipping companies operating in Estonia. Feedback was received from 12 shipowners out of 19 and the results show that at least 7 organisations had been the victims to different types of cyberattacks. The results indicate that shipowners are not paying enough of attention to potential cyber threats and education of their employees. Finally, the paper proposes cyber risk mitigation means for the shipowners.

1 INTRODUCTION

Expanding at 4%, the fastest growth in five years, global maritime trade gathered momentum in 2017 and raised sentiment in the shipping industry. Total volumes have reached 10.7 billion tons (Asariotis et al. 2018), which was transported by sea on different types of ships (tankers, bulk carriers, container ships, general cargo ships, etc.). The world commercial fleet consisted of 94,171 ships on 01.01.2018, with a combined tonnage of 1.92 billion dead-weight tons (Asariotis et al. 2018).

With these volumes the importance of maritime transportation to the world economy cannot be over-emphasized. The global economic inter-dependency among the nations relies largely on the successful operation of the maritime industry. Since the shipping accidents have a significant negative impact on the surrounding environments and will heavily influence the world trade, the safety and security of today's modern shipping are of utmost importance. The safety and security of the ships is ensured by various onboard and onshore maritime systems working together simultaneously. These systems include among others cargo handling and management systems, Automatic Identification System (AIS), Global Navigation Satellite Systems (GNSS), Long Range Tracking and Identification (LRIT) System, Electronic Chart Display and Information System (ECDIS), Global Positioning System (GPS), ship propulsion and machinery management and power management system.

Traditionally, attacks on the ships have included piracy, boarding, theft and destruction. While these attacks have often been successful and still continue happening, they are well understood, the risks are known and appropriate measures can be taken to mitigate the threats. This includes also the education

and training of the seafarers. The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) sets the standards of competence for seafarers internationally (IMO 2019a). International Maritime Organization (IMO) has also developed a series of model courses which provide suggested syllabi, course timetables and learning objectives to assist instructors to develop training programs. They allow for maritime educational institutions to provide training that meets the STCW Convention standards.

Today, the cybersecurity in the shipping industry is a big challenge with a multidisciplinary nature for the shipping companies. Current cybersecurity strategies implemented by most of the shipping companies are not able to counter and deter efficiently intrusions in the maritime cyber domain. The maritime industry globally has failed to make the cybersecurity a priority (Caponi & Belmont 2015).

Increasing number of cybersecurity related incidents in the maritime sector is a clear sign that the problem is persistent and serious and requires more attention and actions from the industry. In June 2017 the world's largest container shipping company, A.P. Møller-Maersk was one of the companies which was hit by the malware NotPetya (Greenberg 2018). The infection with malicious software cost Maersk between $250 and $300 million. In November 2017 the London-based provider of shipping services Clarkson PLC confirmed that it was a subject to a cybersecurity incident which involved unauthorised access to the company's computer systems (Clarckson PLC 2017). COSCO Shipping Lines announced in July 2018 that the company was hit by the ransomware attack, which affected its operations in the Americas (Johnson 2018a). In September 2018 ports of Barcelona and San Diego were targeted by ransomware attackers (Johnson 2018b).

Researchers have successfully developed and demonstrated cyber attacks against the Integrated Navigation System (INS) and ECDIS (Lund et al. 2018), and have been able to manipulate with GPS signals (Bhatti & Humphreys 2017).

Seafarers are exposed to a set of different challenges when in geographical isolation. These can be pirate attacks, rough seas and stormy weather or a very busy traffic routes. With the arrival of new technologies and solutions assisting to sail safely and securely through these conditions, continuous interconnection between the critical maritime infrastructures and also continuous internet access at sea, the cyber threats have become one of the new challenges for the seafarers and cybersecurity awareness is a new item on the agenda of the maritime community.

Shipowners have to be prepared to cope with the rising cyber threats. They have to understand that it is not only the IT issue; the problems also arise among other from the ship's crew behaviour in Internet (chat forums, social media, downloading illegal software, cloud-based file storage, e-mails) and from third parties visiting ships (agents, customs, technicians, surveyors, port officials, vendors, pilots).

Although there has been an increasing awareness on maritime cybersecurity in the industry, the results of several surveys reveal that there is still a room for improvement from the technological and organisational point of view.

According to the Jones Walker LLP 2018 Maritime Cybersecurity Survey (Lee & Wogan 2018) only a minority (36%) of the 126 respondents from maritime companies across the United States believed that their own companies were prepared enough in cybersecurity and 38% of the respondents reported that cyber attackers targeted their companies in the past year.

Fairplay and Baltic and International Maritime Council (BIMCO) are jointly conducting an annual Maritime Cyber Security Survey in order to examine how the maritime industry is handling digital protection. From more than 350 individuals around the world who participated in the survey in 2018, 22% admitted of experiencing some kind of a cyber attack or incident (BIMCO & Fairplay 2018). Top incidents reported during the survey include: phishing, infection with malware, spear phishing, theft of credentials and ransomware.

Another survey undertaken by Futurenautics Maritime, Crew Connectivity 2018, reveals that 47% of the seafarers, who responded to the survey, have sailed on the ship that had become a target of cyber attack, but 85% of the respondents received no cyber training at all (Nguyen 2018). Same survey shows also that 49% of the seafarers confessed that they were unaware of their employers' cyber policies, and 41% thought the responsibility lies with the Master of the ship.

Although Estonia is considered as a maritime country, there were no ships with gross tonnage above 500 under Estonian flag in 2018; last two cargo ships left the Estonian register in 2014 (Reimer 2014). Consequently it is complicated to get a full overview of the companies operating with ships under the flag of another nation (Hunt et al. 2016). It is believed that Estonian shipowners own ca 50-60 cargo ships weighing in excess of 500 tons (Johanson 2016).

In this paper the author presents the results of the independent survey carried out among the Estonian shipowners between April 2017 and February 2019.

The results of the surveys indicate that the cybersecurity hasn't been the priority for the majority of the shipowners in Estonia. As the end users are considered to be the weakest link in cybersecurity, companies should put more emphasis to the cyber awareness training of their personnel and crew (Tam & Jones 2018). You may have the most up-to-date and expensive equipment, but one careless crew member can cause extensive damage to the ship and to the company with just a one click of a mouse.

2 METHODOLOGY

The aim of the research was to find out how much attention have Estonian shipowners paid to the increasing cyber threats, whether the organisations have been the victims of the cyber attacks or incidents and what steps have they taken in order to reduce the risks.

The surveys were carried out between April 2017 and February 2019. The study sample consisted of 19 Estonian organisations who are known to operate under Estonian and foreign flags with different types of ships, including ferries, passenger ships, tugboats, survey ships, multifunctional ships, general cargo vessels, icebreakers, offshore support vessels, etc. The sample list included both business entities and public organisations. The questionnaires were prepared the way that allowed organisations to respond to the survey anonymously and at the same time would also give a good overview of the present state of the cybersecurity among the Estonian shipowners.

The questionnaire study was carried out in Estonian by using the Google Forms platform (docs.google.com/forms) for the preparation of the questionnaire. For analysing the results software Microsoft Excel was used. The organisations were given an option to receive the questionnaire also in English or Russian, if needed. An e-mail invitation was sent to the organisations known to own or operate with ships. In addition, information concerning the questionnaire was also sent to the Estonian Shipowners' Association.

Several reminders were sent by e-mails during the surveys and also many phone calls were made to explain the goal of the surveys and give some additional clarifications.

2.1 *Questionnaire*

The first survey, in 2017, consisted of 29 questions of which 11 were not mandatory to answer and the second survey consisted of 45 questions of which 7 were not mandatory to answer. This allowed to respect the respondent's anonymity and also allowed the respondent to skip the questions, to which the shipping company wouldn't like to answer.

Second survey, which was conducted in February 2019, was amended with the additional questions that allowed receiving a better overview of the current state of the cyber awareness training for the personnel of the organisations and the need for cybersecurity courses and exercises in the future.

Most of the questions had pre-defined multiple-choice answers with the option to include the comment in the text-field under each question. One sample question is presented below in Table 1.

Table 1. Sample question from the survey.

Question	Multiple-choice answer
What do you perceive is your organisation's biggest cyber vulnerability?	our employees our IT systems in the office our IT systems onboard ships our procedures third parties (suppliers, hackers, passengers, officials, etc.) our competition other...

Part of the survey questions were aimed to receive background information about the organisations (number of total employees, number of employees on ships, number of the fleet and ship types, etc.), questions in other sections inquired information about the cyber risk mitigation activities in the organisation, occurrences of cyber incidents and also related consequences, and cybersecurity related training.

3 RESULTS

In this section the author analyses the main results from two surveys. The research was aimed at identifying the current state of the cybersecurity in shipping industry with reference to Estonian shipowners. A total of 12 organisations filled in the questionnaires. 9 organisations participated in the first survey in April 2017 and 6 organisations in February 2019 of which 3 were new organisations.

The results were analysed in a qualitative manner due to the relatively small number of respondents. The respondents were asked to identify their organisation at the beginning of the questionnaire, but it was not mandatory. Some (4) decided not to reveal their organisation's name and contacts.

Table 2 shows the position of the respondents in their organisation.

Table 2. Respondents position in the organization.

Respondents position	Number
Top manager	7 (58.3%)
Manager	3 (25.0%)
Specialist	2 (16.7%)

Survey carried out in April 2017 included organisations with a total fleet of at least 52 ships. One respondent decided not to reveal the size of their fleet. Respondents to second survey in February 2019 have a fleet of 51 ships. Table 3 presents the ship types of the respondents.

Table 3. Types of ships included in two surveys.

Ship types	Survey 1	Survey 2
General cargo	x	x
Passenger	x	x
Container		x
Ferries	x	
Ro-ro	x	x
Ro-pax		x
Tugboats	x	
Multifunctional	x	x
Icebreaker		x
Pilot boat		x
Survey		x
Accommodation	x	
Offshore support	x	

The question related to the IMO Resolution MSC.428(98) and the requirement of addressing the cyber risks appropriately in the Safety Management System (SMS) was included in the second survey as the Resolution MSC.428(98) was adopted by the IMO Maritime Safety Committee at its 98th session in June 2017. This resolution encourages administrations to

ensure that cyber risks are appropriately addressed in existing Safety Management Systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021 (IMO 2019b). None of the respondents had yet taken any action on this matter (in February 2019). The organisations have the plan to implement necessary steps in 2019 (1 organisation) and in 2020 (3 organisations). One shipping company responded that most probably they will sell their last ship before 2021 and one organisation is not planning to make any changes to their Safety Management System.

Maritime industry in general has approached the cybersecurity seriously and as a result many cybersecurity guidelines have been published by different actors in recent years (Rizvanolli et al. 2018). Table 4 below gives an overview of the guidelines that respondents are using.

Table 4. Guidelines and standards used by the respondents.

Guidelines	Respondents
IMO Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3)	1
The Guidelines on Cyber Security onboard Ships (BIMCO)	1
Cyber security resilience management for ships and mobile offshore units in operation (DNV GL)	2
Deploying information and communications technology in shipping (Lloyd's Register)	1
ISO/IEC 27001:2013	1
Guidelines from the classification society	1
ISKE (three-level IT Baseline Security System developed for Estonian public sector)	2
Other guidelines or standards	6
Don't use any guidelines or standards	3

The results from the survey indicate that respondents have taken some measures in their organisations to reduce the cyber risks. Most popular actions taken by the organisations are described in the Table 5.

Table 5. Risk mitigation measures in the organisations.

Risk mitigation measure	Respondents
Virus protection and regular virus scans	12
Using firewalls	11
Software and firmware are updated regularly	10
Regular backups of critical information	10
Privilege user account management has been implemented	10
Backups are kept in several locations	9
Employees are using separate e-mail addresses for work and personal use	9
Restrict using removable media (e.g. USB memory sticks)	4
Employees are regularly reminded about the possible cyber threats	7

Two organisations pointed out in the comments field that it is sometimes impracticable to restrict the usage of removable media onboard ships when visiting the ports. Necessary information is still shared in many places via USB flash drives (cargo plans, need for printing documents for port authorities, updating of ECDIS software or electronic charts, manuals, etc.) and it is very difficult to control and verify that the removable media in use is clean from possible malware and safe to use.

A cybersecurity risk assessment and gap analysis allows the organisations to identify and prioritise the cyber risks by understanding the information and assets they need to protect and the threats they need to be protected from. Only 3 shipowners out of 12 reported that they have carried out the risk assessment in their organisation and on the ships. One respondent confirmed that they are planning to undertake the assessment in the near future.

The question about the establishment of the cybersecurity incident response plan in the organisation received 7 negative answers. Only 5 shipowners had a cybersecurity response plan in place in the organisation.

According to the Allianz Risk Barometer 2018, cyber incidents (cyber crime, IT failure, data breaches) are considered as one of the top five risks in the shipping industry (Allianz Global Corporate & Specialty 2018). The results of the survey show that 7 shipowners (58%) have admitted that their organisations have experienced cyber incidents in the last few years. The types of the cyber incidents are presented in Table 6. Two respondents decided not to share the information about the possible cyber incidents within their organisations.

Table 6. Main types of the cyber attacks or incidents.

Cyber incident	Respondents
Infection with malware	3
Phishing attack	7
E-mail spoofing	4
Problems with network	1
GPS interference	1
Ransomware	2

The organisations who experienced some cyber incident sustained following damages:
- loss or leakage of company data (1);
- access to the employees account (1)
- measurable financial damages (1);
- damages to the IT systems (2);
- damages to the organisation's reputation (2).

Three respondents decided not to share the information about the damages the cyber incidents had caused to their organisations.

The author asked the respondents to evaluate the likelihood of a cyber attack or a cyber incident in their organisation on a scale of 1 – 5, 1 being less likely and 5 being very likely. According to the results below (Figure 1 and Figure 2) the organisations don't see that the possibility of a cyber incident on their ships or in the offices would be high or very high. On the contrary, compared to the situation in 2017, the organisations believe in February 2019 that the likelihood of an incident is less.

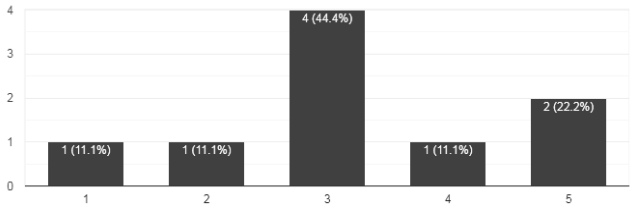

Figure 1. Respondents (9) evaluating the likelihood of a cyber incident in their organisation in April 2017.

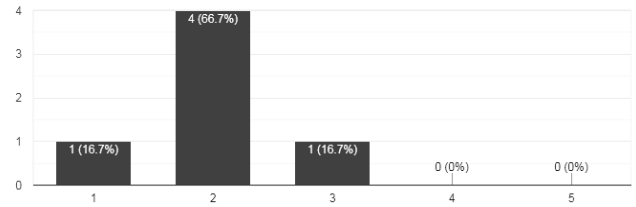

Figure 2. Respondents (6) evaluating the likelihood of a cyber incident in their organisation in February 2019.

The question "Has your organisation reported any cyber attack or incident to the relevant authorities" was included in the second survey, in February 2019. The feedback to that question revealed that none of the respondents have reported any cyber incidents to the relevant authorities, national Computer Emergency Response Team (CERT) or to any dedicated cyber incident platform (e.g. Maritime Cyber Alliance, www.maritimecyberalliance.com). As the number of serious cyber attacks and incidents in the maritime domain is growing, it is of utmost importance to share the information about the incidents with other stakeholders and organisations in the industry. The incidents happen every day. Unfortunately majority of them are never reported, thus creating the sense that the cybersecurity is not a critical part of the organisation's security.

The author was also interested if the organisations have any procedures in place for reporting the cyber incidents onboard ships. 3 organisations confirmed that such procedure exists and 3 organisations indicated that they don't have the procedures for reporting the office. This question was added to the 2019 survey.

One section of the survey concentrated on the cyber awareness and cyber hygiene training for the personnel and ships' crews. The aim was to get an overview how much emphasis have the organisations placed on the education and training.

The question about providing cyber awareness and cyber hygiene training to the employees received only 3 confirmative replies. The rest of the respondents (9) replied that no training on cybersecurity or cyber hygiene has been provided for their personnel. At the same time 7 organisations think that their personnel needs some training on cybersecurity and 5 organisations still could do without it.

Additional questions on education and training were enclosed in the 2019 survey. The results are shown in the Table 7 below.

Table 7. Results of the questions on cyber awareness and cyber hygiene training, 2019 survey (6 respondents).

Question	Yes	No
Has your organisation conducted any cyber crisis management scenarios or exercises for shipboard personnel?	0	6
Has your organisation conducted any cyber crisis management scenarios or exercises for the office personnel?	1	5
Has the respondent received any cyber hygiene and awareness training?	1	5
Would your organisation be interested to carry out cyber incident training on ships?	4	2

The author also asked the respondents in the 2019 survey to choose or propose the biggest vulnerabilities to their organisations. The results are presented in the Table 8. Third parties visiting the ships and their own crews are considered as biggest vulnerabilities to the organisations.

Table 8. Biggest cyber vulnerabilities to the organisation perceived by the respondents (6 respondents).

Vulnerability	Respondents
Third parties (suppliers, hackers, passengers, officials, etc.)	3
Our employees and crews	3
Out IT systems on ships	1
Our procedures	1

Several survey questions were related to the financial aspects. To the question, if the organisation's insurance is covering also the cyber risks (e.g. ransomware, privacy breach, and data loss), only 2 organisations respondent positively, 4 shipowners replied that their insurance doesn't cover cyber risks and 6 respondents decided not to reveal this information.

The cybersecurity predictions for the coming years are tough: Artificial Intelligence (AI) will be used by the cyber criminals to implement and enhance their cyber attacks, deployment of 5G network infrastructure will expand the attack surface area, more poorly secured Internet of Things (IoT) devices will be targeted and used for harmful purposes, organisations will be targeted by using more sophisticated malware, etc. (Thompson & Trilling 2018).

Therefore the author added to the 2019 survey additional question, which asked the organisations to indicate, if they have allocated any finances in the budget of 2019 for cyber risk mitigation. Out of 6 organisations 4 had additional budget dedicated for the cybersecurity in 2019.

The question "Does your organisation have a business continuity plan?" had five options for answering: no, 0-6 months, 6-12 months, 12+ months, I don't know. 4 respondents replied that they are not aware of such continuity plan and 2 respondents replied that the business continuity plan does not exist at all.

The result of the BIMCO, Fairplay and ABS Advanced Solutions cybersecurity survey show that more than a fifth of the respondents (22%) had been the victim of a cyber attack. Results of the survey

carried out among Estonian shipowners reveal that the percentage of the victims of a cyber crime in the shipping industry can be higher, in this case 58% of respondents. Survey carried out by Jones Walker LLP among the maritime companies in the United States reveal that 38% of the respondent organisations were targeted by the cyber criminals within last year (Lee & Wogan, 2018).

Regarding the nature of the incidents, then here we can see the resemblance. Most common cyber incidents reported by the respondents of all three surveys involve phishing methods, infections with malware (Trojans, viruses, worms, etc.), spear phishing, ransomware and theft of credentials.

All main types of the incidents are related to inappropriate behaviours of humans with IT systems. As the human factor is increasingly targeted by the cyber criminals, more emphasis should be placed on the training and educating of the end users (office personnel and crews on ships) (Maennel et al. 2018).

According to the BIMCO, Fairplay and ABS Advanced Solutions cybersecurity survey results 27% of respondents reported that they had never received cyber security training. In case of the survey among the Estonian shipowners only 25% of the respondent organisations have provided cyber hygiene or cyber awareness training for their employees (3 out of 12 respondents). Jones Walker LLP has divided the companies into three categories: small companies (1-49 employees), mid-size companies (50-400 employees) and large companies (more than 400 companies). Among the mid-size companies the cybersecurity training program for employees has been provided within 55% of the respondent organisations in the United States. This number is even lower regarding small companies (11%).

4 PROPOSALS FOR CYBER RISK MITIGATION

In this section the author points out some proposals for the cyber risk mitigation that shipowners can employ. As the cybersecurity has a multidisciplinary nature the approach to the cybersecurity has to be diverse. As the information technology has become an important part of the commercial process the first important step that the organisations have to do is to acknowledge on the highest level of the management that the cybersecurity problem exists and no-one is safe. Only then it is possible to move forward and talk openly about the problem and take necessary steps for cyber risk mitigation, including provision of sufficient financial support for the IT department, training personnel, etc.

Cyber hygiene training should be provided to all employees of the organisation. They are the first line of the defense and can decrease the likelihood of a successful cyber attack or prevent unwanted cyber incident. Being the weakest link in the information technology and not receiving any proper cyber hygiene training the personnel will keep making mistakes that can cost the organisation a fortune or even bring down their operations for good. Also the cyber awareness training should be considered for the ships' crews and basic knowledge about cybersecurity.

International shipping organisations have in recent years published several guidelines for the industry in order to raise the awareness in cybersecurity and to provide some guidance for the companies how to reduce the cyber risks and enhance the maritime safety and security. The list of the guidelines is available online and includes publications among others from BIMCO, IMO, DNV GL, Lloyd's Register and Bureau Veritas (DNV GL 2016; Lloyd's Register 2016; BIMCO 2017; IMO 2017).

Setting up the proper support from the shore office for the crew in case of a cyber incident is an important measure. This has to taken into account when developing contingency plans. These plans have to take into account various case scenarios and include the actions to be taken in case of disruption of critical systems.

Regular software and hardware updates are crucial. It has to be kept in mind, that those versions of software or hardware that are not supported by the developers are not receiving any updates either. In many cases Windows XP and Windows 7 are still in use on the workstation PC's for running ECDIS software (Dyryavyy 2014). Hereby, the use of obsolete software onboard ships should be carefully evaluated by the shipowner.

Consequently, the cyber risk assessment has to be carried out. This includes the mapping of the ship's functions and systems, identifying critical IT and operational technology (OT) equipment, reviewing the documentation on maintenance and support of IT and OT systems, etc.

In addition, penetration tests by third-party experts can be performed in order to identify whether the actual security level matches the desired level.

The author also proposes to carry out cybersecurity related drills on the ships to test the readiness of the crew and the effectiveness of the established procedures. The possible scenarios could include loss of GPS signal, malfunction of the sensor readings for critical operations or infection of ECDIS with malware via USB port.

Strict rules and policies understandable to all employees have to be implemented on ships for the use of IT equipment, removable media, charging of the mobile devices, generation of passwords, etc. These rules should not only be applied to the crew but also to the visitors (agents, vendors, etc.). These rules would reduce the possible cyber risks happening onboard significantly.

For the shipowner it is crucial to know that the software that is being used in the ship's network is of legal origin and not warez (pirated software) and that the end users, the seafarers, are visiting websites that are safe from malware.

It is important to be aware and informed about the trends in the industry. Knowing that certain threats exist in the cyber worlds allows the shipowners to be better prepared. Therefore it is important to report about the cyber incidents in the organisation and on the ships to the national authorities and also inform the international community. This will create a better

awareness of the problem and will also keep the ships safe.

5 LIMITATIONS

Taking into account that the shipping industry is often characterised as highly conservative and also considering the seriousness and sensitivity of the research topic, one can expect, that the feedback to cybersecurity related surveys would be reserved and partial. This can be observed also during the two surveys described in this paper. To some questions the respondents decided not to provide direct answers.

6 CONCLUSIONS

This paper provides, what the author believes, the first detailed study on the state of cybersecurity specifically aimed at the Estonian shipowners. The purpose of the study was to get an overview of the state of cybersecurity among the Estonian shipowners and to understand the motivations for their actions related to cybersecurity. Based on the conducted surveys, the author has found that some of the Estonian organisations operating with ships have experienced a cyber attack or an incident to some extent. Although the shipping organisations in Estonia have already suffered from the cybersecurity incidents and have incurred losses in connection with this, the assessment of the level of probability of possible future cyber incident in their organisations is still medium to low.

The shipping industry is undergoing a fundamental transformation. Digitalisation and automation of the supply chain has significantly changed the shipping industry in recent years. With the arrival of new technological solutions the shipping is also facing new and unknown threats to the industry. Undoubtedly the maritime sector is behind of other transportation sectors in terms of cybersecurity. This includes the protection measures for the IT and OT systems and networks, implementation of the cybersecurity guidelines and standards in the organisation and also training the personnel in the offices and crews onboard ships.

While the surveys carried out between 2017 and 2019 might have a positive effect to the increase of the cyber awareness among the Estonian shipowners, it is expected to be a continued process by the Estonian researches in this field that will assist the enterprises to improve their cybersecurity related activities and risk mitigation procedures. The author will make any effort to improve the educational programmes for the seafarers in Estonia and other personnel involved in the shipping industry. Also propose proper cyber mitigation procedures and training requirements for the shipping companies and for enhancing the understanding of the maritime cyber space in order to tackle with the impending cyber threats.

The author also proposes to continue with similar survey once in a year or in every second year and to involve the shipping industry also beyond Estonia.

REFERENCES

Allianz Global Corporate & Specialty. 2018. Safety and Shipping Review 2018: 25.

Asariotis, Regina, Mark Assaf, Hassiba Benamara, Jan Hoffmann, Anila Premti, Luisa Rodríguez, Mathis Weller, et al. 2018. *Review of Maritime Transport 2018*.

Bhatti, Jahshan, and Todd E. Humphreys. 2017. Hostile Control of Ships via False GPS Signals: Demonstration and Detection. *Navigation, Journal of the Institute of Navigation*. doi:10.1002/navi.183.

BIMCO, Fairplay, ABS Advanced Solutions. 2018. *Maritime Cyber Survey 2018 - the results*.

BIMCO. 2017. The Guidelines on Cyber Security Onboard Ships.

Caponi, Steven L, and Kate B Belmont. 2015. Maritime Cybersecurity: A Growing Threat Goes Unanswered. *Intellectual Property & Technology Law Journal; Clifton*. doi:10.1093/ser/mwy024.

Clarckson PLC. 2017. Notice of cyber security incident. https://www.clarksons.com/news/notice-of-cyber-security-incident/

DNV GL. 2016. Cyber security resilience management for ships and mobile offshore units in operation. *Dnvgl-Rp-0496*.

Dyryavyy, Yevgen. 2014. *Preparing for Cyber Battleships – Electronic Chart Display and Information System Security*.

Greenberg, Andy. 2018. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Hunt, Tõnis, Kadi Kasepõld, and Madli Kopti. 2016. *Merendussektori majandusmõju uuring. I etapp.* Tallinn.

IMO. 2019a. International Convention on Standards of Training, Certification and Watchkeeping for Seafarers , 1978. http://www.imo.org/en/OurWork/HumanElement/TrainingCertification/Pages/STCW-Convention.aspx. Accessed February 20.

IMO. 2019b. Maritime cyber risk. http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx. Accessed March 4.

IMO. 2017. Guidelines on Maritime Cyber Risk Management.

Johanson, Adele. 2016. No major cargo ship registered in Estonia. *news.postimees.ee*. https://news.postimees.ee/3855923/no-major-cargo-ship-registered-in-estonia

Johnson, Jennifer. 2018a. Cosco Shipping hit by ransomware attack. *The Institute of Marine Engineering, Science and Technology*. https://www.imarest.org/themarineprofessional/item/4357-cosco-shipping-hit-by-ransomware-attack

Johnson, Jennifer. 2018b. Ports of Barcelona and San Diego hit by cyber attacks. *The Marine Profesional - Online News website of The Institute of Marine Engineering, Science and Technology*. https://www.imarest.org/themarineprofessional/item/4473-ports-of-barcelona-and-san-diego-hit-by-cyber-attacks

Lee, Andrew, and Hansford Wogan. 2018. *Jones Walker LLP 2018 Maritime Cybersecurity Survey*.

Lloyd's Register. 2016. Deploying information and communications technology in shipping – Lloyd's Register's approach to assurance.

Lund, Mass Soldal, Odd Sveinung Hareide, and Øyvind Jøsok. 2018. An Attack on an Integrated Navigation System. *Sjøkrigsskolen* 3: 149–163. doi:10.21339/2464-353x.3.2.149.

Maennel, K., Mäses, S. and Maennel, O. (2018) 'Cyber Hygiene: The Big Picture', in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). doi: 10.1007/978-3-030-03638-6_18.

Nguyen, Lili. 2018. Crew Connectivity 2018 Survey Results. *KNect365*. https://knect365.com/shipping/article/37c4946d-cae7-4749-98dd-a4bc1f5b11e8/crew-connectivity-2018-survey-results

Reimer, Andres. 2014. Last large cargo ship exits Estonian flag. *Postimees*. https://news.postimees.ee/2779320/last-large-cargo-ship-exits-estonian-flag

Rizvanolli, Anisa, Ole John, and Carlos Jahn. 2018. Cyber security in shipping and navigation: a framework for ship design and compliance check 1 . Need for Cyber Security in Shipping. In *ISIS-MTE*.

Tam, Kimberly, and Kevin D. Jones. 2018. Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*: 1–18. doi:10.1080/23738871.2018.1513053.

Thompson, Hugh, and Steve Trilling. 2018. Cyber Security Predictions: 2019 and Beyond. *Symantec*. https://www.symantec.com/blogs/feature-stories/cyber-security-predictions-2019-and-beyond