Developments in Maritime Technology and Engineering – Guedes Soares & Santos (eds)

Shortcomings in cybersecurity education for seafarers

D. Heering, O.M. Maennel & A.N. Venables
Tallinn University of Technology, Tallinn, Estonia

ABSTRACT: Ships, ports, terminals and offshore facilities are increasingly becoming dependent on networked information and communication technology (ICT). Seafarers must be ready to cope with a growing number of cyber threats onboard ships with cybersecurity awareness playing an important role in emergency and crisis management. Unfortunately, current maritime education and training (MET) programmes do not provide enough information on cybersecurity to seafarers to be able to identify and mitigate the prevailing cyber threat landscape. This paper provides a structured survey of published maritime cybersecurity research and gives an overview of the role of the cybersecurity component in MET for seafarers. The results show that currently there are no requirements for MET institutions to include cybersecurity awareness or cyber hygiene practice in the curricula. Some areas for future research are also proposed.

1 INTRODUCTION

International trade is highly dependent on the shipping industry. Shipping provides an efficient and low-cost transportation of goods and it is estimated that over 90% of the world's trade is carried by sea (United Nations, n.d.). Maritime trade expanded by 2.7% to reach 11billion tons in 2018 (UNCTAD, 2019). With these increasing volumes, the importance of maritime transportation to the world economy cannot be over-emphasized. The global economic inter-dependency among nations relies largely on the successful operation of the shipping industry. Since maritime accidents have a significant impact on the surrounding environments and heavily influences world trade, the safe and secure operation of today's modern shipping fleet is of utmost importance. This is ensured by various onboard and onshore maritime systems working together simultaneously.

The traditional physical security threats that may affect safe and secure ships' operation usually include piracy, smuggling, boarding, theft, stowaways and destruction. As these incidents have often been reported and continue to occur, they are well understood and the risks are known, enabling appropriate measures to be taken to mitigate these threats. One way this is achieved is through the structured education and training of seafarers. The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW), 1978, as amended, sets the standards of competence for seafarers internationally (Cockcroft & Lameijer, 2012). The International Maritime Organization (IMO) has also developed a series of model courses. These provide suggested syllabi, course timetables and learning objectives to assist instructors develop training programs to meet the STCW Convention standards for seafarers.

As the maritime industry embraces the digital era, new technological developments allow shipowners to operate ships more safely, securely and economically by optimizing routes and taking ship movement dynamics into account (Ishii et al., 2010). Smart shipping initiatives support crews and improve the performance of fleets. With the introduction of new digital solutions, ships are now more reliant on the internet to continually share data between the ship and shore. Connection to the cyber domain has exposed crew members, cargo, information technology (IT) and operational technology (OT) systems to a range of different cyber threats. Operational technology is the hardware and software that is dedicated to detecting and causing changes in physical processes through direct monitoring and control of physical devices, processes and events (Gartner, n. d.). Traditionally IT and OT have been separated, but with the widespread introduction of the Internet onboard ships, they are increasingly connected and the lines between them has started to blur. This poses a significant risk as any disruption in the operation of OT systems may impact the ship's safety (BIMCO et al., 2018). Cybersecurity has become a difficult challenge for the maritime industry with its multidisciplinary nature. The strategies that most shipping companies have currently implemented are not able to efficiently counter and deter intrusions in the maritime cyber domain. The maritime industry globally has failed to make the cybersecurity a priority (Caponi & Belmont, 2015) and Estonian shipowners are no exception (Heering, 2017a).

DOI: 10.1201/9781003216582-6

2 CYBERSECURITY IN MARITIME DOMAIN

New technologies implemented in the shipping sector have impacted on the responsibilities, skills and training of seafarers. The employment of advanced equipment and working in more automated and integrated environments has increased demands on the maritime community. In order to keep the systems functioning safely and securely it is important to protect them from cyber threats. When seafarers are sailing in different geographical locations (e.g. high seas, coastal areas, ports, high dangers areas etc.) they face different challenges, which now also include cybersecurity. For example, in 2019 the Norwegian National Security Authority (NSM) together with the Norwegian Shipowner's Association and Maritime Authority published recommended measures on ICT security and usage of social media. These recommendations were published based on information received regarding a cyber campaign targeting several different sectors and companies around the world (Norwegian Maritime Authority, 2019). Norwegian authorities assessed that "all types of ships and shipowners' land-based infrastructure can be vulnerable to cyber incidents. Shipowners that operate in ISPS/MARSEC level 2 areas or higher should be aware of the situation".

Recent cyber incidents that have taken place in the shipping sector and which have been publicized have proven that the sector is not immune to cyber criminals, state-sponsored hackers or to the reckless behaviour of their own people, which have exploited vulnerabilities in their systems. Table 1 includes some latest known cyber incidents in the sector. This list does not reflect all known cyber incidents.

It has been successfully demonstrated that both IT and OT systems used onboard ships have

Table 1. Latest known prominent cyber incidents in the sector.

2017	The ransomware NotPetya was released by a suspected state actor. While the main targets of the attack were companies in Ukraine, the malware crossed the border within hours and affected the operations of computers around the world. Among the victims was the world's largest container ship and supply vessel operator, A.P. Møller–Mærsk A/S (Greenberg, 2018). This incident impacted operations at Maersk terminals around the world, caused delays and disruption that lasted weeks. According to the company's interim financial report for the second quarter of 2017, the financial impact of the incident was estimated at between $200m to $300m (Maersk, 2017).
2018	In 2018 several ransomware attacks affected normal operations of major ports around the world (Cimpanu, 2018; Drougkas et al., 2019). These included the Port of Barcelona on September 20th and the Port of San Diego declared on September 25th. However, both ports were able to continue normal operations and ships continued to access their facilities without impacts from the cybersecurity incident (Port Strategy, 2018).
2018	China Ocean Shipping Company (COSCO) reported a cyber-attack. Its fleet comprises 1317 ships with a capacity of 105.36 million DWT, ranking it as the biggest in the world (COSCO Shipping, 2020). According to the company's statement, telephone networks and e-mail system were impacted in U.S, Canada, Panama, Argentina, Brazil, Peru, Chile and Uruguay. The incident affected the carrier's ability to communicate with its ships, customers, and marine terminals (Gallagher, 2018).
2019	The crew of a ship that was bound for the ports of New York and New Jersey in February 2019 reported to the Coast Guard that they were experiencing a significant cyber incident impacting their shipboard network. A team of cyber experts concluded that although the malware had significantly degraded the functionality of the onboard computer system, essential ship control systems had not been impacted (U.S. Coast Guard, 2019a). The team also found that the ship was operating without any effective cybersecurity measures and that the critical ship control systems were exposed to significant vulnerabilities. As the ship's crew was aware of the cyber risks and of possible malware infection presented in the shipboard network, they didn't use onboard computers for personal purposes (e.g. reading e-mails, making online purchases). However, they continued using the network for updating electronic charts, manage cargo data and communicating with relevant institutions.
2019	The Maritime Transportation Security Act (MTSA) facility was involved in a ransomware intrusion case. According to the U.S. Coast Guard, the attack vector was likely a phishing e-mail sent to the operators at the MTSA facility (U.S. Coast Guard, 2019b). The Ryuk ransomware was activated by an employee who clicked on an embedded malicious link in the sent e-mail. This allowed for malware to access significant enterprise IT network files and encrypt them. It also infected the industrial control systems that monitored and controlled cargo transfer disrupting the entire corporate IT network, including camera and physical access systems.
2019	The Kuwait transportation and shipping industry experienced two cyber-attack campaigns against their IT systems between May and June 2019. The intelligence team at Palo Alto Networks believed that the tools used to carry out the attacks were created by the same developer as The Ryuk ransomware (Loock, 2019).
2016-2020	Maritime industry has seen the rise of GPS jamming and spoofing cases in different parts of the world (GPS spoofing in the Black Sea on 2016, GPS outage in South Korea in 2016, GPS jamming and spoofing during NATO exercises in 2017 and 2018, GPS disruptions in the Mediterranean Sea in 2018) (Dunn, 2020).

vulnerabilities that can be exploited or exposed unintentionally by crew members. Researchers from the University of Texas at Austin have also demonstrated the capability to take over control of a 65-m yacht in the Mediterranean Sea. Experiments have shown that the ship's along-track and cross-track positions can be modulated by feeding false positions to the ship's autopilot system, that are offset from the ship's true position. Besides this system-level effect of spoofing, specific navigation and collision avoidance instruments can also be affected. These include automatic radar plotting, the automatic identification system, the dead reckoning system built into the ship's electronic chart display and information system (ECDIS), and the ship's satellite communications. All can all generate hazardously misleading information during a GNSS spoofing attack (Bhatti & Humphreys, 2017). In January 2016 two U.S. Navy patrol boats were intercepted by Iranian military in Iranian territorial waters. Officially, it was stated, that the U.S. sailors made a navigational error that mistakenly took them into Iranian territorial waters (Schmidt & Cooper, 2016). However, it is also suspected that the patrol boats were guided in the wrong direction and into the Iranian waters by manipulating GPS signals (e.g. spoofing) (Psiaki & Humphreys, 2016).

3 CYBERSECURITY EDUCATION FOR SEAFARERS

We argue that the regulatory framework for seafarer's training is struggling to keep pace with the technological change taking place in the maritime industry. Current multilateral decision-making processes mean that STCW Convention revisions can take a long time to adopt and incorporate into the curriculum. At the same time, seafarers' skills are in urgent need for an upgrade. This means that both the MET institutions and seafarers need to be agile (Alfultis, 2018).

A number of maritime organizations have already taken steps to address this significant problem and the threat to the shipping industry. The International Maritime Organization (IMO) has issued guidelines for shipowners and authorities on maritime cyber risk management (MSC-FAL.1/Circ.3) and has also adopted Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management Systems. This resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code). This should be achieved no later than the first annual verification of the company's Document of Compliance after 1 January 2021 (International Maritime Organization, 2020).

In addition to the IMO there are a range of different guidelines from other industry organizations. This include the International Chamber of Shipping (ICS), INTERCARGO, INTERTANKO, Oil Companies International Marine Forum (OCIMF), the International Union of Marine Insurance (IUMI), BIMCO, Department for Transport (UK), DNV GL and others.

Studies have shown that the main type of cyber breaches that organizations face (phishing, viruses and ransomware attacks) are related to human error and technical cybersecurity vulnerabilities (Klahr et al., 2017). Employees are perceived as the weak link in relation to the cybersecurity breaches (Canfield et al., 2016; Safa & Maple, 2016).

The IBM X-Force Threat Intelligence Index 2020 shows, that there was a 2000% increase in operational technology targeting incidents in 2019 (IBM X-Force Incident Response and Intelligence Services, 2020). This predicts a rising number of threat actors attacking industrial systems in the future. According to the report, the top three infection vectors in 2019 were phishing (31%), scan and exploit (30%) and stolen credentials (29%). The same report also shows that over 8.5 billion records were compromised in 2019 and that careless employees can be largely responsible for a rise of more than 200% compared to the records lost in 2018. The transportation sector was the third-most attacked in 2019, after financial services and retail sector. One of the reasons the cyber threats have spread around the world so rapidly in last few years is a lack of awareness on cybersecurity.

Although cybersecurity knowledge has increased somewhat in the maritime sector, partly also due to the publicly known cyber incidents, the results indicate that there is still a long way to go. Onboard personnel have a key role to play when operating IT and OT systems onboard. Therefore, it is of the utmost importance that the crew know how to operate the systems safely and securely, understand the risk, including cyber risks, and can identify and report suspected cyber incidents.

A 2018 Maritime Cybersecurity Survey revealed, that only 36% of the 126 respondents from maritime companies across the United States believed that their own companies were prepared enough in cybersecurity. 38% of the respondents reported that cyber attackers targeted their companies in the past year (Lee & Wogan, 2018).

Key findings from Crew Connectivity 2018 Survey Report show that the number of seafarers who have access to the internet is increasing with every year (Futurenautics Ltd, 2018). The survey comprised 5889 seafarers of which 75% confirmed that they have some form of Internet access while at sea. At the same time only 15% of seafarers disclosed that they had received any form of cybersecurity training. Of the training that did take place, most was provided by the crewing and manning companies before joining their next ship. Worryingly 47% of seafarers said that they had sailed on a ship that had been a target of a cyber-attack. The same survey also showed that 49% of the seafarers confessed that they were unaware of their employers' cyber policies, and 41% thought the responsibility lay with the ship's master. One Dutch ship owner declared during the Digital Ship Maritime Cyber Resilience Forum in Rotterdam

in 2017 that all the recent incidents in his company could have been prevented from individual users being more alert (de Vleeschhouwer, 2017).

As new technologies, increasing automation and emerging threats from cyberspace are transforming seafarers' skills and responsibilities, it is important that future seafarers are supported. This requires skills training during their studies at the maritime education and training institutions including an increased focus on improving cyber resilience.

Although there is an abundance of research on cybersecurity and maritime safety and security, there is a lack of evidence highlighting the gaps and challenges of cybersecurity education for seafarers. The overall aim of this paper is to provide an overview of the research field, conclusions made to date and synthesize the collective knowledge of the field. This will provide the justification for recommended future research directions.

Table 2. List of keywords used in the literature review.

automatic identification system	maritime accidents
autonomous ship	maritime safety
bridge operations	maritime security
bridge procedures	maritime threat actors
cyber attacks	mitigation
cyber awareness	navigation
cyber risk management	cyber risk assessment
cyber security	satellite communication
cybersecurity	seafarer
cyber situational awareness	ship
cyber threats	shipping
ECDIS	simulator training
e-navigation	situational awareness
education and training	smart ship
global maritime distress and	spoofing
safety system	STCW
global positioning system	unmanned ship
human factor	vessel
jamming	vulnerabilities

4 METHODOLOGY

In this section we discuss the research methodology and limits of our survey. The method applied in this study was a comprehensive literature review. The review focused on published journal articles discussing cybersecurity in the maritime domain and those that take notice on the needs for future education and training of seafarers.

The literature search was conducted using a number of the databases These included IEEE, ScienceDirect, Springer, Google Scholar, ResearchGate, TransNav Journal, The Journal of Navigation, WMU Journal of Maritime Affairs, International Maritime Science Conference and the Digital Collection of Tallinn University of Technology Library. The focus was on the publications published within the last 7 years (2013-2020).

The keywords employed for the publication search are listed in Table 2. Keywords were used in search engines both separately and in combination in order to expand the results of the search. The scope of the survey includes the cyber threats and their impacts in maritime cybersecurity and the cybersecurity component in the maritime education and training (MET).

A selection process was also used to exclude papers that were not relevant to the current review. Papers only referring to maritime logistics, piracy, hijacking, financial risks, digital twin, cybersecurity in other domains, vessel traffic service, ship design, ship collisions, spatial planning and ship performance were excluded.

The search resulted in a range of papers covering cybersecurity threats in the shipping industry. These also included the challenges of big data in shipping, risks related to autonomous ships, vulnerabilities of the ship systems, the role of human error in ship accidents, maritime education and training, cyber situational awareness and cyber risk assessment methods.

Papers were excluded that were not related to the scope of the review and which were not accessible on the internet. A total of 88 unique papers were retrieved and analysed (Table 3.).

5 RESULTS

In this section, the authors provide a review of the literature and the role of cybersecurity training in the maritime education and training sector. Until recently, cybersecurity in the maritime domain has not been seen as a significant issue. The European Union Agency for Network and Information Security (ENISA) carried out a study on cybersecurity challenges in the maritime industry in 2011 (Cimpean et al., 2011). The aim of the study was to assist the sector to understand better its key cybersecurity risks. The target audience of the study included organizations, national authorities, government bodies and private companies that were involved in maritime activities. The following key findings were made:

- The awareness of cybersecurity is either at a very low level or even non-existent in the maritime sector. This observation was applicable at all layers, including government bodies, port authorities and maritime companies.
- ICT systems supporting maritime operations, from port management to ship communication, are generally highly complex and employ a variety of ICT technologies that also include very specific elements.

Table 3. List of articles (sorted by publishing year).

Year	No of articles	Reference
2014	2	(Boyes, 2014), (Škrlec et al., 2014)
2015	3	(Rødseth & Burmeister, 2015), (Fitton et al., 2015), (DiRenzo et al., 2015)
2016	3	(Burke & Clott, 2016), (Jones et al., 2016), (Bolat et al., 2016)
2017	14	(Glomsvoll & Bonenberg, 2017), (Bhatti & Humphreys, 2017), (Batalden & Sydnes, 2017), (Garcia-Perez et al., 2017), (Hassani et al., 2017), (Kolev & Dimitrov, 2017), (Bhandari et al., 2017) (Tucci, 2017), (Bothur et al., 2017) (Y.-C. Lee et al., 2017), (Becmeur et al., 2017), (Bou-Harb et al., 2017), (Radmilo et al., 2017), (Botunac & Gržan, 2017)
2018	15	(Kessler et al., 2018), (Filić, 2018), (Ahvenjärvi, 2018), (Svilicic et al., 2018) (Hareide et al., 2018), (Zăgan et al., 2018), (Kimberly Tam & Jones, 2018a), (Vinnem & Utne, 2018), (Forbes, 2018) (Alfultis, 2018), (Mileski et al., 2018), (Lund, Hareide, et al., 2018), (Jacq et al., 2018), (Lund, Gulland, et al., 2018), (Kimberly Tam & Jones, 2018b)
2019	44	(Svilicic, Kamahara, Rooks, & Yano, 2019), (Lovell & Heering, 2019), (Nasaruddin & Emad, 2019), (Svilicic, Rudan, Jugović, et al., 2019), (Kitada & Baum-Talmor, 2019), (Greiman, 2019), (Baskar et al., 2019), (Bolmsten et al., 2019), (Kavallieratos et al., 2019), (Chia, 2019), (Mednikarov et al., 2019), (Oruc, 2019), (Kidd & Mccarthy, 2019), (Kitada et al., 2019), (Zăgan & Raicu, 2019), (Ahvenjärvi, Czarnowski, Kåla, et al., 2019), (Kimberly Tam & Jones, 2019a), (Kimberly Tam & Jones, 2019d), (Svilicic, Brčić, Žuškin, & Kalebić, 2019), (Svilicic, Rudan, Frančić, et al., 2019), (Svilicic, Kamahara, Celic, & Bolmsten, 2019), (Park et al., 2019), (Jacq et al., 2019), (Rana, 2019), (Hong et al., 2019), (Bolat & Kayişoğlu, 2019), (Kimberly Tam & Jones, 2019b), (Mraković & Vojinović, 2019), (Ahvenjärvi, Czarnowski, & Mogensen, 2019), (Sakar et al., 2019), (Voliotis & Filippopoulos, 2019), (Kaleem Awan & Ghamdi, 2019), (Lutzhoft et al., 2019), (K Tam et al., 2019), (Blagovest, 2019), (Heffner & Rødseth, 2019), (Hult et al., 2019), (Kimberly Tam & Jones, 2019c), (Said & Agamy, 2019), (Dimakopoulou et al., 2019), (Vidan et al., 2019), (Lušić et al., 2019), (Alop, 2019), (Daum, 2019)
2020	7	(Svilicic et al., 2020), (Alcaide & Llave, 2020), (Hynnekleiv et al., 2020), (Emad et al., 2020), (Caprolu et al., 2020), (Heering, 2020), (Kimberly Tam et al., 2020)

- In the current regulatory context for the maritime sector on global, regional and national levels, there is very little consideration given to cyber security. Most security related regulation only includes provisions relating to safety and physical security concepts.
- No holistic approach to maritime cyber risks exists. It was observed that maritime stakeholders are setting and managing cyber security expectations and measures in a rather ad hoc manner. Not all of the actual risks are being considered, such as the disruption of critical telecommunication means or the exposure of cargo information.

One of the high-level recommendations made in the ENISA study was the need for the development and implementation of awareness raising campaigns targeting the maritime sector and provision of appropriate cybersecurity training to relevant stakeholders (e.g. shipping companies, ship crews, port authorities etc.).

Categorization in chronological order allows to follow the developments in the maritime sector in regard to cybersecurity education and training. The reviewed papers were published between 2014 and 2020.

(Bloor & Sampson, 2009) describes the issues with the quality of seafarer training which were affecting maritime sector before 2010, and which are also still relevant today. The quality of the maritime education and training is not on the level that it should be. It varies widely, from clearly substandard to the highest international quality. Cybersecurity was not on the agenda at that time.

The importance of providing training on cybersecurity for shipping companies and crews was brought up by ENISA in 2011 (Cimpean et al., 2011). It pointed out the problems and shortcomings in maritime sector concerning cybersecurity. This was described at the beginning of this section. In (Rødseth & Burmeister, 2015) the authors discuss and describe the risk assessment method related to the MUNIN project; a feasibility study on an unmanned bulk carrier on an intercontinental voyage. A total of 65 main hazards were identified and then classified according to its consequence and

the probability that it will happen. Risks related to cyber domain were not included.

In their work Fitton et al., 2015 address cyber operations in the maritime domain in three elements: information, technology and people. Ship crews who have been isolated from the rest of the world for many years, are now, due to the needs of a modern maritime business, are constantly connected to the Internet. It also means, that once unreachable individuals can now be targeted by the cyber criminals. In their paper the authors recommend for preventing, spotting and defending against cyber-attacks to educate, train and drill people, so that they could continue to operate under cyber-attack conditions. They also stress the importance of understanding social engineering attacks and recommend appropriate training to mitigate it.

But it is only in 2016-2017, when the importance of cybersecurity training for the shipping companies and personnel was emphasized more strongly by researchers, e.g. (Becmeur et al., 2017; Bothur et al., 2017; DiRenzo et al., 2015; Fruth & Teuteberg, 2017; Garcia-Perez et al., 2017; Heering, 2017b; Jones et al., 2016; Kolev & Dimitrov, 2017; Radmilo et al., 2017).

The case of A.P. Møller-Maersk in June 2017 (Greenberg, 2018) did finally raise the awareness of the vulnerabilities of shipping companies and ports to technological failure. This was followed by the increasing number of articles published from 2017 on the threats and vulnerabilities in shipping (Table 3.).

Articles published in 2018-2020 provide preliminary recommendations for maritime cybersecurity training (Ahvenjärvi, 2018; Alfultis, 2018; Daum, 2019; Hareide et al., 2018; Kidd & Mccarthy, 2019; Mileski et al., 2018; Kimberly Tam et al., 2020; Kimberly Tam & Jones, 2018b; Zăgan et al., 2018).

The vigilant seafarer onboard the ship is the most important security asset for the shipping company. (Hareide et al., 2018) emphasize that in addition to the need for a high degree of situational awareness in order to be able to make well informed navigation decisions, the navigators need to be also situationally aware of the status of the new IT systems and the limitations and possibilities they present. If one lacks system awareness, one would lack a vital part of the overall situational awareness and potentially present a risk factor rather than a risk reduction factor. So, in order to utilize the human capacity to be the strongest link in the maritime cybersecurity chain, it has to become a part of education and training in order to enhance the navigator's competence by increasing system awareness (Lund, Hareide, et al., 2018).

(Roolaid, 2018) hypothesized in his dissertation that maritime educational institutions have not given enough attention to specific cybersecurity education in deck officers training to ensure their ability to operate the ships safely. The author carried out research (surveys, interviews) among the European maritime educational institutions. The aim of the research was to find out which institutions are providing cybersecurity training for the seafarers. The author searched for the study programs, different courses and their learning outcomes related to cybersecurity. Information was received from about 35 MET institutions. The quantitative results of the mapping are:

- 2 institutions out of 35 provided specific cybersecurity education for ship's officers;
- 3 institutions out of 35 provided only general cybersecurity awareness education for ships' officers;
- 11 institutions out of 19 thought that it was necessary to teach cybersecurity to ships' officers;
- 7 institutions out of 19 thought that cybersecurity education will be necessary in the future;
- 1 institution out of 19 thought that cybersecurity education is not necessary for ship's officers.

The results of the survey confirm that even though the reports and industry guidelines recommend educating and training for the cadets, the collaboration between the shipping companies and educational institutions in Europe is still lacking the cybersecurity component.

According to Roolaid's research the main obstacles in providing cybersecurity training to the seafarers are: already excessive workload of the teachers, lack of study materials in native language, already filled curricula, and a lack of specific requirements in the STCW Code (Roolaid, 2018). The same issue has been brought up by (Kidd & Mccarthy, 2019). Roolaid recommends starting with a two-day cybersecurity course for ship officers. This would comprise teaching theoretical knowledge about cybersecurity in shipping and risk assessment training based on given scenarios. The practical part of the course could be based on a model-based framework for maritime cyber risk assessment created by the University of Plymouth (Kimberly Tam & Jones, 2019a).

Similar research was carried out by researchers within the project "Addressing Cyber Security in Maritime Education and Training" (CYMET) (Ahvenjärvi, Czarnowski, Kåla, et al., 2019). Ten different bachelor's degree programs on navigation in ten European maritime universities were analysed. None of the study programs included courses in maritime cybersecurity. Only two programs provided basic computer science with some elements of cybersecurity. The authors found the results to be unsatisfactory considering the importance of cybersecurity awareness and the need for proper cyber risk management on the ships.

An important part of understanding the cyber risks and in the detection of cyber incidents lies on forensic readiness of ships. This is covered by (Kimberly Tam & Jones, 2019d). The risks and forensic needs of ships are highly divergent from traditional

systems (Jones et al., 2016). Currently, ship crews receive no training for recognising cyber-elements and there are no IMO requirements for cyber-related evidence to be stored. In their recommendations for improving forensic readiness in the maritime sector are steps for training staff, crew members and management to increase the cyber-incident awareness and for secure evidence handling.

(Alcaide & Llave, 2020; Bolat et al., 2016; Bolat & Kayişoğlu, 2019; Dimakopoulou et al., 2019; Heering, 2020; Kimberly Tam & Jones, 2019b, 2019c) have conducted surveys among shipping companies and maritime professionals. The purpose of these surveys is to appreciate the state of cybersecurity in the sector, understand the motivation of actions of the companies, increase the level of cyber awareness and understand the needs of the sector related to education and training of their personnel (on shore and onboard ships). The results show that seemingly cyber-secure maritime domain and ships exhibit vulnerabilities and critical components. The research carried out in Estonia (Heering, 2020) reveals that the cyber threats at sea are very real and inflict damage to the shipping operations. The main cyber incidents that were mentioned by the companies were: ship computers infecting with malware, phishing attacks, e-mail spoofing, GPS interference, ransomware in ship computers and network problems. According to the feedback from the companies the biggest cyber threats are from third parties (hackers, suppliers, passengers, port officials), company's own employees and crews, IT systems on ships and the procedures. The results also show that companies are interested in providing cyber hygiene and awareness training for their personnel and also would like to carry out cyber incident trainings onboard ships (drills).

In June 2018, the Tallinn University of Technology organised a Cyber Security Summer School. The main focus was on maritime cybersecurity. In (Lovell & Heering, 2019) the authors give an overview of the exercise developed and carried out. A novel method was used to present different approach to cybersecurity-related education and training of seafarers. This included simulator-based exercise on Wärtsilä bridge simulators and developing possible cyber-attack vectors via open-source intelligence (OSINT). The results were surprising: participants successfully developed cyber-attacks against opposing ships, were able to get hold of over 7000 usernames and passwords used by the employees and crews of NATO warships, track NATO ships using Snap Map, Twitter and other social media sites. Webcams in ports were accessed to use as intelligence gathering assets.

The maritime industry, being quite conservative has been behind other sectors in adopting new technologies. Now, when modern ships have reduced crews, the demand for adequately educated and trained professionals is on the rise. Several reviewed papers address the deficiencies and shortcoming in maritime education and training related to digital skills. The EU funded project SkillSea has been initiated with the aim of ensuring that maritime professionals possess key digital, green and soft management skills for the rapidly changing maritime labour market. In their latest report on current skills needed, the consortium addresses the main challenges the maritime shipping sector must face in nearest future (Zec et al., 2020). As the digital services are increasing, the digital skills of maritime professionals are becoming more and more important. This also includes skills required to maintain cybersecurity onboard ships or on shore. As already mentioned in this paper the STCW Convention does not make any reference to digital skills, including skills to ensure cybersecurity onboard ships. The threats and vulnerabilities described and presented in the articles in this review give completely a different view to maritime safety and security. They describe risks that didn't exist or weren't relevant in the maritime domain 10-15 years ago. They are now, but STCW Convention doesn't address them. This should change with the next revision of the Convention. The same conclusions and finding have also been made by (Ahvenjärvi, Czarnowski, & Mogensen, 2019; Ahvenjärvi, Czarnowski, Kåla, et al., 2019; Alfultis, 2018; Blagovest, 2019; Bolat et al., 2016; Bolat & Kayişoğlu, 2019; Bothur et al., 2017; Botunac & Gržan, 2017; Boyes, 2014; Burke & Clott, 2016; Emad et al., 2020; Fitton et al., 2015; Heering, 2020; Hong et al., 2019; Kidd & Mccarthy, 2019; Kolev & Dimitrov, 2017; Lovell & Heering, 2019; Lušić et al., 2019; Lutzhoft et al., 2019; Mednikarov et al., 2019; Nasaruddin & Emad, 2019; Sakar et al., 2019; Vidan et al., 2019).

The authors argue that including cybersecurity awareness training into the MET programmes of all specialities is essential. The next step would be specifying additional concrete skills and knowledge that are essential for different positions onboard the ship (bridge, engine room, etc.). These would be related to their duties and include the development of the framework for a holistic approach to increased cybersecurity awareness and competence on ships in order to avoid accidents caused by cyber incidents. This includes (i) theoretical and practical training in classrooms and simulated environments (Lovell & Heering, 2019; Kimberly Tam et al., 2020), (ii) demonstrations and experiments in special laboratories or platforms (Becmeur et al., 2017; K Tam et al., 2019; Zăgan et al., 2018) and (iii) development of bridge and operational procedures that assists the crew in identifying possible cyber threats and the immediate measures to contain them.

6 DISCUSSION

The authors speculate that in the near future shipowners will start requiring a proof or a certificate from crew members joining their ships of passing a course on basic cybersecurity or attending cyber awareness course. In the long-term these measures can play a significant role in reducing the risks of possible cyber incidents that may cause severe consequences and expenses for the company and to the environment.

Crew members should be able to understand the cyber threats that they are facing when using internet-connected and sophisticated equipment. They should also be able to question if the systems they are using, are properly updated and securely configured.

Baptiste Ossena, Global Product Leader of AGCS Hull and Marine Liabilities has said "As the use of new technologies on board vessels grows, we expect to see changes in both the risk profile of shipowners and the maritime loss environment in future. Insurers will have to deal with a growing number of more technical claims - such as cyber incidents or technological defects - in addition to traditional losses, such as collisions or groundings." (Allianz Global Corporate & Specialty, 2018).

It is only a question of time when the next big cyber-attack will hit the shipping industry. In the last few years there have been many wake-up calls. The criminal activity in the Port of Antwerp (Pol, 2015), the NotPetya malware in 2017 (Greenberg, 2018; Mimoso, 2017), the cyber-attack in shipbroking company Clarkson in 2017 (PLC, 2017), a cyber-attack on COSCO in 2018 (Mongelluzzo, 2018) and the cyber-attack on the Port of San Diego in 2018 (Cimpanu, 2018).

The industry has to be prepared for more damaging incidents in the future. This could involve a vessel carrying hazardous or polluting material, a passenger vessel with large numbers of tourists on board, or a loaded container vessel in a narrow passage. The cybersecurity company Naval Dome has reported that cyber-attacks on maritime OT systems have increased by 900% in last three years (SAFETY4SEA, 2020).

7 CONCLUSION AND FUTURE WORK

This paper reviewed the literature and research done on maritime cybersecurity with the focus on education and training for ships' crews. The results of this review indicate that there is a need for more research on cybersecurity education and training for seafarers. In most guidelines a proper cybersecurity education and cyber awareness development are seen as an important part of prevention and protection, but we conclude that education and awareness are important in all phases. The key to cyber-safer maritime operations is raising the awareness of seafarers of all possible cyber threats, make them understand the challenges, prepare them to prevent cyber incidents on ships, train them to act properly if the problems arise, and also make them aware of their digital behaviour in cyber space in relation to cybersecurity. It's not just an issue for the crew on board, but also for office personnel and third parties, who have access to their systems.

The authors propose to introduce cybersecurity education in the maritime education and training of seafarers without delay by adopting and integrating the best practices and tools implemented and used in other sectors. The need for additional cybersecurity training has been discussed and emphasized in many research papers and reports. The review of the literature show, that although the importance of cybersecurity has increased in the maritime domain, the role and importance of maritime education and training has been so far undervalued. The training programmes should be tailored to each profession and rank onboard the ship.

Cybersecurity cannot be handled exclusively by the company IT department alone. Future research has to also investigate the cybersecurity needs for different ship crew positions (e.g. navigating officer, electrical engineer, engineer, master, ratings etc.). Currently published research provides a good overview of existing cyber threats and vulnerabilities in the maritime domain. This research can be used when updating existing educational programmes for seafarers with a cybersecurity component.

The future work and research will focus on the development of a blueprint for maritime cybersecurity courses for deck officers taking into account the guidelines and workbook published by BIMCO and ICS (BIMCO et al., 2018; BIMCO & ICS, 2019), IMO guidelines MSC-FAL.1/Circ.3 and IMO resolution MSC.428(98) (International Maritime Organization, 2017b, 2017a) and testing it in the maritime educational institution.

REFERENCES

Ahvenjärvi, S. (2018). Addressing cyber security in training of the mariner of the future - the CYMET project. *International Symposium on Integrated Ship's Information Systems & Marine Traffic Engineering Conference*. https://www.dgon-isis.org/index.php?id=46

Ahvenjärvi, S., Czarnowski, I., Kåla, J., Kyster, A., Meyer, I., Mogensen, J., & Szyman, P. (2019). Safe information exchange on board of the ship. *TransNav*, *13*(1), 165–171. https://doi.org/10.12716/1001.13.01.17

Ahvenjärvi, S., Czarnowski, I., & Mogensen, J. (2019). Joint production of web-learning material by IAMU member universities. *20th Commemorative Annual General Assembly, AGA 2019 - Proceedings of the International Association of Maritime Universities Conference, IAMUC 2019*, 175–181.

Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*. https://doi.org/10.1016/j.trpro.2020.03.058

Alfultis, M. A. (2018). Educating the future maritime workforce in a sea of constant disrupters and change. *AGA 2018-19th Annual General Assembly (AGA) of the International Association of Maritime Universities (IAMU)*, 87–93.

Allianz Global Corporate & Specialty. (2018). *Safety and Shipping Review 2018*. 25. https://www.agcs.allianz.com/assets/PDFs/Reports/AGCS_Safety_Shipping_Review_2018.pdf

Alop, A. (2019). The Main Challenges and Barriers to the Successful "Smart Shipping." *The International Journal on Marine Navigation and Safety of Sea Transportation*, *13*(3). https://doi.org/10.12716/1001.13.03.05

Baskar, K., Kala, N., & Balakrishnan, M. (2019). Cyber Preparedness in Maritime Industry. *International Journal of Scientific and Technical Advancements*.

Becmeur, T., Boudvin, X., Brosset, D., Héno, G., Merien, T., Jacq, O., Kermarrec, Y., & Sultan, B. (2017). A Platform for Raising Awareness on Cyber Security in a Maritime Context. *Proceedings - 2017 International Conference on Computational Science and Computational Intelligence, CSCI 2017*. https://doi.org/10.1109/CSCI.2017.17

Bhandari, R., Mohanty, S. S., & Wylie, J. (2017). Cyber security the unknown threat at sea. *18th Annual General Assembly of the International Association of Maritime Universities - Global Perspectives in MET: Towards Sustainable, Green and Integrated Maritime Transport, IAMU 2017*.

Bhatti, J., & Humphreys, T. E. (2017). Hostile Control of Ships via False GPS Signals: Demonstration and Detection. *Navigation, Journal of the Institute of Navigation*, *64*(1), 51–66. https://doi.org/10.1002/navi.183

BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF, & World Shipping Council. (2018). *The Guidelines on Cyber Security onboard Ships*. https://www.bimco.org/products/publications/free/cyber-security

BIMCO, & ICS. (2019). *Cyber Security Workbook for On Board Ship Use. 1st Edition 2019*. https://www.witherbyseamanship.com/cyber-security-workbook-for-on-board-ship-use-1st-edition-2019.html

Blagovest, B. (2019). Maritime education development for environment protection behaviour in the autonomous ships era. *Scientific Bulletin of Naval Academy*, *22*, 21–27. https://doi.org/10.21279/1454-864X-19-I1-003

Bloor, M., & Sampson, H. (2009). Regulatory enforcement of labour standards in an outsourcing globalized industry: The case of the shipping industry. *Work, Employment and Society*, *23*(4), 711–726. https://doi.org/10.1177/0950017009344915

Bolat, P., & Kayişoğlu, G. (2019). Antecedents and Consequences of Cybersecurity Awareness: A Case Study for Turkish Maritime Sector. *Journal of ETA Maritime Science*. https://doi.org/10.5505/jems.2019.85057

Bolat, P., Yüksel, G., & Uygur, S. (2016). A Study for Understanding Cyber Security Awareness Among Turkish Seafarers. *SECOND GLOBAL CONFERENCE ON INNOVATION IN MARINE TECHNOLOGY AND THE FUTURE OF MARITIME TRANSPORTATION*. https://doi.org/10.1007/s11628-013-0202-1

Bolmsten, J., Kasepõld, K., Heering, D., Kaizer, A., Ziemska, M., Alop, A., Chesnokova, M., Sköld, D., & Olena, S. (2019). Maritime Innovation Management - A concept of an innovative course for young maritime professionals. *Proceedings of the International Association of Maritime Universities Conference*, 268–274. http://iamu-edu.org/wp-content/uploads/2019/11/IAMUC2019_Proceedings-1.pdf

Bothur, D., Zheng, G., & Valli, C. (2017). A critical analysis of security vulnerabilities and countermeasures in a smart ship system. *Proceedings of the 15th Australian Information Security Management Conference, AISM 2017*, 81–87.

Botunac, I., & Gržan, M. (2017). Analysis of software threats to the automatic identification system. *Brodogradnja*, *68*(1), 97–105. https://doi.org/10.21278/brod68106

Bou-Harb, E., Kaisar, E. I., & Austin, M. (2017). On the impact of empirical attack models targeting marine transportation. *5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems, MT-ITS 2017 - Proceedings*. https://doi.org/10.1109/MTITS.2017.8005665

Boyes, H. A. (2014). Maritime Cyber Security – Securing the Digital Seaways. *Engineering & Technology Reference, April*, 56–63. https://doi.org/10.1049/etr.2014.0009

Burke, R., & Clott, C. (2016). Technology, collaboration, and the future of maritime education. *RINA, Royal Institution of Naval Architects - International Conference on Education and Professional Development of Engineers in the Maritime Industry, EPD 2016*, *September*.

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying Phishing Susceptibility for Detection and Behavior Decisions. *Human Factors*. https://doi.org/10.1177/0018720816665025

Caponi, S. L., & Belmont, K. B. (2015). Maritime Cybersecurity: A Growing Threat Goes Unanswered. *Intellectual Property & Technology Law Journal; Clifton*. https://doi.org/10.1093/ser/mwy024

Caprolu, M., Di Pietro, R., Raponi, S., Sciancalepore, S., & Tedeschi, P. (2020). Vessels Cybersecurity: Issues, Challenges, and the Road Ahead. *ArXiv*. http://arxiv.org/abs/2003.01991

Chia, R. (2019). The Need for Ethical Hacking in the Maritime Industry. *The Society of Naval Architects and Marine Engineers, Singapore*, *38*, 108–121.

Cimpanu, C. (2018). *Port of San Diego suffers cyber-attack, second port in a week after Barcelona*. ZDNet. https://www.zdnet.com/article/port-of-san-diego-suffers-cyber-attack-second-port-in-a-week-after-barcelona/

Cimpean, D., Meire, J., Bouckaert, V., Stijn, V. C., Pelle, A., & Hellebooge, L. (2011). *Analysis of cyber security aspects in the maritime sector*. https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1

Cockcroft, A. N., & Lameijer, J. N. F. (2012). International convention on standards of training, certification and watchkeeping for seafarers, 1978, as amended. In *A Guide to the Collision Avoidance Rules (Seventh Edition)*. https://doi.org/10.1371/journal.pone.0029637

COSCO Shipping. (2020). *COSCO Shipping, Group profile*. COSCO SHIPPING Group. http://en.coscocs.com/col/col6918/index.html

Daum, O. (2019). Cyber security in the maritime sector. *Journal of Maritime Law and Commerce*.

de Vleeschhouwer, S. (2017). *Safety of data The risks of cyber security in the maritime sector*. https://maritimetechnology.nl/media/NMT_Safety-of-data-The-risks-of-cyber-security-in-the-maritime-sector.pdf

Dimakopoulou, A., Nikitakos, N., Dagkinis, I., Lilas, T. E., Papachristos, D. A., & Papoutsidakis, M. (2019). The

New Cyber Security Framework in Shipping Industy. *Journal of Multidisciplinary Engineering Science and Technology*, *6*(12), 11227–11233.

DiRenzo, J., Goward, D. A., & Roberts, F. S. (2015). The little-known challenge of maritime cyber security. *6th International Conference on Information, Intelligence, Systems and Applications (IISA)*, 1–5. https://doi.org/10.1109/IISA.2015.7388071

Drougkas, A., Sarri, A., Kyranoudi, P., & Zisi, A. (2019). *Port Cybersecurity. Good practices for cybersecurity in the maritime sector*. https://doi.org/10.2824/328515

Dunn, K. (2020, January 22). *Mysterious GPS outages are wracking the shipping industry*. Fortune. https://fortune.com/longform/gps-outages-maritime-shipping-industry/

Emad, G. R., Khabir, M., & Shahbakhsh, M. (2020). Shipping 4. 0 and Training Seafarers for the Future Autonomous and Unmanned Ships. *Marine Industries Conference*, *January*.

Fitton, O., Prince, D., Germond, B., & Lacy, M. (2015). *The Future of Maritime Cyber Security*. Lancaster University. http://www.research.lancs.ac.uk/portal/en/publications/the-future-of-maritime-cyber-security(d6a02f20-3125-4337-b189-e8420ca71316).html

Forbes, V. L. (2018). *The Global Maritime Industry Remains Unprepared for Future Cybersecurity Challenges. December 2014*.

Fruth, M., & Teuteberg, F. (2017). Digitization in maritime logistics—What is there and what is missing? *Cogent Business and Management*. https://doi.org/10.1080/23311975.2017.1411066

Futurenautics Ltd. (2018). *Crew Connectivity 2018 Survey Report*. https://knect365.com/shipping/article/37c4946d-cae7-4749-98dd-a4bc1f5b11e8/crew-connectivity-2018-survey-results

Gallagher, J. (2018). *Cyber attack hits COSCO Shipping*. Safety at Sea. https://safetyatsea.net/news/2018/cyber-attack-hits-cosco-shipping/

Garcia-Perez, A., Thurlbeck, M., & How, E. (2017). Towards cyber security readiness in the Maritime industry : A knowledge-based approach. *Semantic Scholar*, 1–7. https://www.semanticscholar.org/paper/Towards-cyber-security-readiness-in-the-Maritime-%3A/0bca56d7f4c56899540d3ee9180ee6c8557a813b

Gartner. (n.d.). *Operational Technology (ot)*. Gartner Glossary. Retrieved February 19, 2020, from https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

Glomsvoll, O., & Bonenberg, L. K. (2017). GNSS jamming resilience for close to shore navigation in the Northern Sea. *The Journal of Navigation*, *70*, 33–48. https://doi.org/10.1017/S0373463316000473

Greenberg, A. (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/

Greiman, V. (2019). Navigating the cyber sea: Dangerous atolls ahead. *14th International Conference on Cyber Warfare and Security, ICCWS 2019*.

Hareide, O. S., Josok, O., Lund, M. S., Ostnes, R., & Helkala, K. (2018). Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *Journal of Navigation*, *71*(5), 1025–1039. https://doi.org/10.1017/S0373463318000164

Hassani, V., Crasta, N., & Pascoal, A. M. (2017). Cyber security issues in navigation systems of marine vessels from a control perspective. *Proceedings of the International Conference on Offshore Mechanics and Arctic Engineering - OMAE*. https://doi.org/10.1115/OMAE201761771

Heering, D. (2017a). *Ensuring Cyber Security in Shipping with Reference to Estonian Shipowners and Proposals for Risk Mitigation* [Tallinn University of Technology]. https://digi.lib.ttu.ee/i/file.php?DLID=8512&t=1

Heering, D. (2017b). *Küberturvalisuse tagamine laevanduses eesti laevaomanike näitel ning ettepanekud riskide maandamiseks*. https://digikogu.taltech.ee/et/Item/7bb85829-2c56-4c8e-9895-f955385f627b

Heering, D. (2020). Ensuring Cybersecurity in Shipping: Reference to Estonian Shipowners. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, *14*(2), 271–278. https://doi.org/10.12716/1001.14.02.01

Heffner, K., & Rødseth, Ø. J. (2019). Enabling Technologies for Maritime Autonomous Surface Ships. *Journal of Physics: Conference Series*, *1357*, 12021. https://doi.org/10.1088/1742-6596/1357/1/012021

Hong, J.-H., Lee, C.-H. L., & Yun, G. (2019). A Study on the New Education and Training Scheme for Developing Seafarers in Seafarer 4. 0 - Focusing on the MASS. *Journal of the Korean Society of Marine Environment and Safety*, *25*(6), 726–734. https://doi.org/https://doi.org/10.7837/kosomes.2019.25.6.726

Hult, C., Praetorius, G., & Sandberg, C. (2019). On the Future of Maritime Transport – Discussing Terminology and Timeframes. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, *13*(2), 269–273. https://doi.org/10.12716/1001.13.02.01

Hynnekleiv, A., Lutzhoft, M., & Earthy, J. V. (2020). Towards an ecosystem of skills in the future maritime industry. *Human Factors*, *February*.

IBM X-Force Incident Response and Intelligence Services. (2020). *X-Force Threat Intelligence Index 2020*. https://www.ibm.com/security/data-breach/threat-intelligence

International Maritime Organization. (2017a). *Guidelines on maritime cyber risk management*.

International Maritime Organization. (2017b). *Resolution MSC.428(98) Maritime cyber risk management in safety management systems*.

International Maritime Organization. (2020). *Maritime cyber risk*. International Maritime Organization. http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx

Ishii, E., Kobayashi, E., Mizunoe, T., & Maki, A. (2010). Proposal of new-generation route optimization technique for an oceangoing vessel. *OCEANS'10 IEEE Sydney, OCEANSSYD 2010*. https://doi.org/10.1109/OCEANSSYD.2010.5603624

Jacq, O., Boudvin, X., Brosset, D., Kermarrec, Y., & Simonin, J. (2018). Detecting and Hunting Cyberthreats in a Maritime Environment : Specification and Experimentation of a Maritime Cybersecurity Operations Centre. *2018 2nd Cyber Security in Networking Conference (CSNet)*, 1–8.

Jacq, O., Merino, P., Brosset, D., Simonin, J., Kermarrec, Y., Giraud, M., Lab-sticc, I. M. T. A., & Cedex, F.-B. (2019). *Maritime Cyber Situational Awareness Elaboration for Unmanned Vehicles*.

Jones, K. D., Tam, K., & Papadaki, M. (2016). Threats and Impacts in Maritime Cyber Security. *Engineering & Technology Reference*, 1–12. https://doi.org/10.1049/etr.2015.0123.Published

Kaleem Awan, M. S., & Ghamdi, M. A. A. (2019). Understanding the vulnerabilities in digital components of an integrated bridge system (IBS). *Journal of Marine Science and Engineering*. https://doi.org/10.3390/jmse7100350

Kavallieratos, G., Katsikas, S., & Gkioulos, V. (2019). Cyber-attacks against the autonomous ship. In *Lecture Notes in Computer* Science *(including subseries Lecture Notes in Artificial* Intelligence *and* Lecture Notes in Bioinformatics): Vol. 11387 LNCS. https://doi.org/10.1007/978-3-030-12786-2_2

Kessler, G. C., Craiger, P., & Haass, J. C. (2018). A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, *12*(3), 429–437. https://doi.org/10.12716/1001.12.03.01

Kidd, R., & Mccarthy, E. (2019). Maritime Education in the Age of Autonomy. *WIT Transactions on The Built Environment*, *187*, 221–230. https://doi.org/10.2495/mt190201

Kitada, M., Baldauf, M., Mannov, A., Svendsen, P. A., Baumler, R., Schröder-Hinrichs, J. U., Dalaklis, D., Fonseca, T., Shi, X., & Lagdami, K. (2019). Command of vessels in the era of digitalization. In *Advances in Human* Factors, *Business* Management *and* Society. AHFE 2018. Advances in *Intelligent* Systems *and* Computing (Vol. 783). Springer, Cham. https://doi.org/10.1007/978-3-319-94709-9_32

Kitada, M., & Baum-Talmor, P. (2019). Maritime digitisation and its impact on seafarers' employment from a career perspective. *20th Commemorative Annual General Assembly, AGA 2019 - Proceedings of the International Association of Maritime Universities Conference, IAMUC 2019, November*, 259–267.

Klahr, R., Shah, J. N., Sheriffs, P., Rossington, T., & Pestell, G. (2017). Cyber Security Breaches Survey 2017: Main report. *UK Government*. https://doi.org/10.13140/RG.2.1.4332.6324

Kolev, K., & Dimitrov, N. (2017). Cyber threat in maritime industry-Situational awareness and educational aspect. *18th Annual General Assembly of the International Association of Maritime Universities*, *1*, 352–360.

Lee, A., & Wogan, H. (2018). *Jones Walker LLP 2018 Maritime Cybersecurity Survey*. https://sites-communications.joneswalker.com/38/990/landing-pages/2018-maritime-cybersecurity-survey-landing-page-only-(v1).asp

Lee, Y.-C., Park, S.-K., Lee, W.-K., & Kang, J. (2017). Improving cyber security awareness in maritime transport: A way forward. *Journal of the Korean Society of Marine Engineering*, *41*(8), 738–745. https://doi.org/10.5916/jkosme.2017.41.8.738

Loock, J. (2019). *Two Major Cyberattacks Have Targetted Kuwait Transportation and Shipping Industry This Year*. Maritime Security Review. http://www.marsecreview.com/2019/10/two-major-cyberattacks-have-targetted-kuwait-transportation-and-shipping-industry-this-year/

Lovell, K. N., & Heering, D. (2019). Exercise Neptune: Maritime Cybersecurity Training Using the Navigational Simulators. *5th Interdisciplinary Cyber Research Conference (ICR2019), June*, 34–37.

Lund, M. S., Gulland, J. E., Hareide, O. S., Josok, eyvind, & Weum, K. O. C. (2018). Integrity of Integrated Navigation Systems. *2018 IEEE Conference on Communications and Network Security (CNS)*, 1–5. https://doi.org/10.1109/CNS.2018.8433151

Lund, M. S., Hareide, O. S., & Jøsok, Ø. (2018). An Attack on an Integrated Navigation System. *Sjøkrigsskolen*, *3*(2), 149–163. https://doi.org/10.21339/2464-353x.3.2.149

Lušić, Z., Bakota, M., Čorić, M., & Skoko, I. (2019). Seafarer market – challenges for the future. *Transactions on Maritime Science*, *8*(1), 62–74. https://doi.org/10.7225/toms.v08.n01.007

Lutzhoft, M., Hynnekleiv, A., Earthy, J. V., & Petersen, E. S. (2019). Human-centred maritime autonomy-An ethnography of the future. *Journal of Physics: Conference Series*. https://doi.org/10.1088/1742-6596/1357/1/012032

Maersk. (2017). *Interim Report Q2 2017*. https://investor.maersk.com/news-releases/news-release-details/interim-report-q2-2017

Mednikarov, B., Kalinov, K., Kanev, D., Madjarova, T., & Lutzkanova, S. (2019). Current trends in the maritime profession and their implications for the maritime education. In B. Svilicic, Y. Mori, & S. Matsuzaki (Eds.), *Proceedings of the International Association of Maritime Universities Conference* (pp. 275–286). International Association of Maritime Universities. http://iamu-edu.org/wp-content/uploads/2019/11/IAMUC2019_Proceedings-1.pdf

Mileski, J., Clott, C., & Galvao, C. B. (2018). Cyberattacks on ships: a wicked problem approach. *Maritime Business Review*, *3*(4), 414–430. https://doi.org/10.1108/mabr-08-2018-0026

Mimoso, M. (2017). *Maersk Shipping Reports $300M Loss Stemming from NotPetya Attack*. ThreatPost - The Kaspersky Lab Security News Service. https://doi.org/10.1177/1077546308094431

Mongelluzzo, B. (2018). *Cosco's pre-cyber attack efforts protected network*. JOC.Com Magazine, Maritime News. https://www.joc.com/maritime-news/container-lines/cosco/cosco's-pre-cyber-attack-efforts-protected-network_20180730.html

Mraković, I., & Vojinović, R. (2019). Maritime cyber security analysis – How to reduce threats? *Transactions on Maritime Science*, *8*(1), 132–139. https://doi.org/10.7225/toms.v08.n01.013

Nasaruddin, M. M., & Emad, G. R. (2019). Preparing maritime professionals for their future roles in a digitalized era: Bridging the blockchain skills gap in maritime education and training. *20th Commemorative Annual General Assembly, AGA 2019 - Proceedings of the International Association of Maritime Universities Conference, IAMUC 2019*.

Norwegian Maritime Authority. (2019). *Martime cyber risks*. Norwegian Maritime Authority. https://www.sdir.no/en/news/news-from-the-nma/cyber-risk-in-the-maritime-sector/

Oruc, A. (2019). Tanker Industry is More Ready against Cyber Threats. *International Conference on Marine Engineering and Technology (ICMET), November*. https://doi.org/10.24868/icmet.oman.2019.030

Park, C., Shi, W., Zhang, W., Kontovas, C., & Chang, C. H. (2019). Cybersecurity in the maritime industry: A literature review. *20th Commemorative Annual General Assembly, AGA 2019 - Proceedings of the International Association of Maritime Universities Conference, IAMUC 2019*, 79–86.

PLC, C. (2017). *Notice of cyber security incident*. https://www.clarksons.com/news/notice-of-cyber-security-incident/

Pol, W. van de. (2015). *Gehackte haven, cokesmokkel 2.0 (#1)*. Crimesite. https://www.crimesite.nl/gehackte-haven-cokesmokkel-2-0-1/

Port Strategy. (2018). *San Diego cyber-attack included ransom note*. https://www.portstrategy.com/news101/world/americas/cyber-attack-on-san-diego-included-ransom-note

Psiaki, M. L., & Humphreys, T. E. (2016). Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies. *IEEE Spectrum*, *53*(8), 26–53. https://doi.org/10.1109/MSPEC.2016.7524168

Radmilo, I., Gudelj, A., & Ristov, P. (2017). Information Security in Maritime Domain. *International Maritime Science Conference*, 76–93.

Rana, A. (2019). Commercial Maritime and Cyber Risk Management. *Safety & Defense*, *5*(1), 46–48. https://doi.org/10.37105/sd.42

Rødseth, Ø. J., & Burmeister, H.-C. (2015). Risk Assessment for an Unmanned Merchant Ship. *The International Journal on Marine Navigation and Safety of Sea Transportation*, *9*(3), 357–364. https://doi.org/10.12716/1001.09.03.08

Roolaid, L. (2018). *Küberturbe haridus laevaohvitseride väljaõppes ning soovitused selle korraldamiseks* [Tallinn University of Technology]. https://digi.lib.ttu.ee/i/file.php?DLID=10538&t=1

Safa, N. S., & Maple, C. (2016). Human errors in the information security realm – and how to fix them. *Computer Fraud and Security*. https://doi.org/10.1016/S1361-3723(16)30073-2

SAFETY4SEA. (2020). *Cyber attacks on maritime OT systems increased 900% in last three years*. SAFETY4SEA. https://safety4sea.com/cyber-attacks-on-maritime-ot-systems-increased-900-in-last-three-years/

Said, K., & Agamy, M. (2019). The impact of cybersecurity on the future of Autonomous ships. *International Journal of Recent Research in Interdisciplinary Sciences*, *6*(2), 10–15.

Sakar, C., Koseoglu, B., Buber, M., & Toz, A. C. (2019). Are The Ships Fully Secured Against The Cyber-Attacks? *Global Conference on Innovation in Marine Technology and the Future of Maritime Transportation*, 276–288.

Schmidt, M. S., & Cooper, H. (2016). *Defense Secretary Says U.S. Sailors Made Navigational Error Into Iranian Waters*. The New York Times. https://www.nytimes.com/2016/01/15/world/middleeast/us-navy-iran.html

Škrlec, Z., Bićanić, Z., & Tadić, J. (2014). Maritime Cyber Defense. *6th International Maritime Science Conference (IMSC 2014)*, *1*, 19.

Svilicic, B., Brčić, D., Žuškin, S., & Kalebić, D. (2019). Raising awareness on cyber security of ecdis. *TransNav*. https://doi.org/10.12716/1001.13.01.24

Svilicic, B., Celic, J., Kamahara, J., & Bolmsten, J. (2018). *A framework for cyber security risk assessment of ships*. 21–28.

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. https://doi.org/10.1007/s13437-019-00183-x

Svilicic, B., Kamahara, J., Rooks, M., & Yano, Y. (2019). Maritime Cyber Risk Management: An Experimental Ship Assessment. *Journal of Navigation*. https://doi.org/10.1017/S0373463318001157

Svilicic, B., Rudan, I., Frančić, V., & Doričić, M. (2019). Shipboard ECDIS cyber security: Third-party component threats. *Pomorstvo*, *33*(2), 176–180. https://doi.org/10.31217/p.33.2.7

Svilicic, B., Rudan, I., Frančić, V., & Mohović, D. (2020). Towards a Cyber Secure Shipboard Radar. *Journal of Navigation*, *73*(3), 547–558. https://doi.org/10.1017/S0373463319000808

Svilicic, B., Rudan, I., Jugović, A., & Zec, D. (2019). A study on cyber security threats in a shipboard integrated navigational system. *Journal of Marine Science and Engineering*, *7*(10), 1–11. https://doi.org/10.3390/jmse7100364

Tam, K, Forshaw, K., & Jones, K. (2019). Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities. *International Conference on Marine Engineering and Technology*. https://doi.org/10.24868/icmet.oman.2019.005

Tam, Kimberly, & Jones, K. (2018a). Cyber-Risk Assessment for Autonomous Ships. *2018 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2018*. https://doi.org/10.1109/CyberSecPODS.2018.8560690

Tam, Kimberly, & Jones, K. (2019a). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*. https://doi.org/10.1007/s13437-019-00162-2

Tam, Kimberly, & Jones, K. D. (2018b). Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, *3*(2), 147–164. https://doi.org/10.1080/23738871.2018.1513053

Tam, Kimberly, & Jones, K. D. (2019b). Situational Awareness : Examining Factors that Affect Cyber-Risks in the Maritime Sector. *International Journal on Cyber Situational Awareness*, *4*(1), 40–68. https://doi.org/10.22619/IJCSA.2019.100125

Tam, Kimberly, & Jones, K. D. (2019c). Factors Affecting Cyber Risk in Maritime. *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 1–8. https://doi.org/10.1109/CyberSA.2019.8899382

Tam, Kimberly, & Jones, K. D. (2019d). Forensic Readiness within the Maritime Sector. *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 1–4. https://doi.org/10.1109/CyberSA.2019.8899642

Tam, Kimberly, Moara-Nkwe, K., & Jones, K. (2020). The Use of Cyber Ranges in the Maritime Context: Assessing maritime-cyber risks, raising awareness, and providing training. *Maritime Technology and Research*, *3*(1). https://doi.org/10.33175/mtr.2021.241410

Tucci, A. E. (2017). Cyber Risks in the Marine Transportation System. In R. M. Clark & S. Hakim (Eds.), *Cyber-Physical Security* (pp. 113–131). Springer, Cham. https://doi.org/10.1007/978-3-319-32824-9_6

U.S. Coast Guard. (2019a). Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels. In *Marine Safety Alert*. https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Office-of-Investigations-Casualty-Analysis/Safety-Alerts/

U.S. Coast Guard. (2019b). Cyberattack Impacts MTSA Facility Operations. In *Marine Safety Information Bulletin*. https://www.dco.uscg.mil/Portals/9/DCO Documents/5p/MSIB/2019/MSIB_10_19.pdf?ver=2019-12-23-134957-667

UNCTAD. (2019). Review of Maritime Transport 2019. In *Review of Maritime Transport*. UNCTAD. https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2563

United Nations. (n.d.). *IMO profile*. Business.Un.Org. Retrieved June 2, 2020, from https://business.un.org/en/entities/13

Vidan, P., Bukljaš, M., Pavić, I., & Vukša, S. (2019). Autonomous Systems & Ships - Training and Education on Maritime Faculties. *8th International Maritime Science Conference*. https://www.bib.irb.hr/1005959?rad=1005959

Vinnem, J. E., & Utne, I. B. (2018). Risk from cyberattacks on autonomous ships. *Safety and Reliability - Safe Societies in a Changing World - Proceedings of the 28th International European Safety and Reliability Conference, ESREL 2018*. https://doi.org/10.1201/9781351174664-188

Voliotis, A., & Filippopoulos, I. (2019). *An Integrated Maritime Cyber Security Policy Proposal. August*.

Zăgan, R., & Raicu, G. (2019). Understanding the OT cyber risk on board ship and ship stability. *Analele Universităţii "Dunărea de Jos" Din Galaţi. Fascicula XI, Construcţii Navale/Annals of "Dunărea de Jos" of Galati, Fascicle XI, Shipbuilding*, *42*, 81–90. https://doi.org/10.35219/annugalshipbuilding.2019.42.11

Zăgan, R., Raicu, G., Hanzu-Pazara, R., & Enache, S. (2018). Realities in Maritime Domain Regarding Cyber Security Concept. *Advanced Engineering Forum*, *27*, 221–228. https://doi.org/10.4028/www.scientific.net/aef.27.221

Zec, D., Maglic, L., Šimić, H. M., & Gundić, A. (2020). *Current Skills Needs: Reality and Mapping*. https://www.skillsea.eu/index.php/news-events/spotlight/106-read-the-full-report-on-currents-skills-needs