

Maritime Cyber Security Analysis – How to Reduce Threats?

Ivan Mraković, Ranko Vojinović

Maritime cyber security management requires a holistic approach as there is an increase in complexity, digitalization, and automation of systems in maritime industry. Numerous interconnected systems between ship and shore, which are in need of a special focus in the internet environment, are increasing on daily basis. Nowadays one of the major concerns in maritime computing is vulnerability to cyber-attacks. In maritime industry, cyber incidents can lead to loss of life, loss of control over ships or sensitive data, as well as ship and/or cargo hijacking. This paper therefore covers key problems of maritime industry from cyber security perspective and proposes solutions on how to eliminate or minimize them.

KEY WORDS

- ~ Maritime cyber security
- ~ Cyber threat
- ~ Cyber risk
- ~ Cyber-attack
- ~ Maritime industry

Mediterranean University, Faculty of Information Technologies, Podgorica, Montenegro

e-mail: iwanmrak@gmail.com

doi: 10.7225/toms.v08.n01.013

This work is licensed under 

1. INTRODUCTION

Maritime business is rapidly changing. The number of integrated and interconnected systems, as well as those where a company can access and operate from shore, is rapidly increasing. The term “maritime” refers to ships, yachts, offshore structures, other floating objects, infrastructure, and anything else that connects and unifies all of the afore mentioned elements in business.

Cloud computing is flourishing as well. It brings an increase in productivity, scalability, and a significant degree of independence of user location, able to access database from any location via internet connection. “Many organizations are now migrating towards cloud due to its favorable features” (Balobaïd and Debnath, 2018).

As an example, the shipping company “UASC” have migrated to a system for bunker ordering via cloud computing. The “classic” way of bunker ordering was inexpensive, so the representatives of “UASC” moved a step forward, signing the contract with “Shiptech” in order to create a cloud based bunker ordering platform. Migrating to the new system enables “UASC” to track market prices, to have a better communication with suppliers, to improve the ship’s performance monitoring and to plan bunkering of their whole fleet (Shiptech, 2015).

There is no company or ship operating totally or partly online which is immune to cyber threats. Research (Einsig, 2016) shows that business digitalization is obstructed by many factors. The biggest threat is security vulnerability, especially cyber security. In the end, cyber incidents are ranked as the second most important risk of running a company. In maritime shipping, 31% of respondents have stated that they are frightened of cyber-criminal, data theft, and other similar risks (Allianz Global Corporate & Specialty SE, 2018).

„Maritime cyber risk refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety, or security failures as a consequence of information or systems being corrupted, lost or compromised” (International Maritime Organization, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3, 2017).

The increase of cyber risks is a consequence of an increase in connectivity and dependency of global navigational systems. Therefore “cyber security refers to the protection of information

systems (hardware, software, and associated infrastructure), the data on them, and the services they provide, from unauthorized access, harm or misuse. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures” (Shaikh, 2017).

Vulnerable systems onboard include the navigation bridge, cargo handling equipment, the engine room, the power management system, and administrative as well as communicational systems. Numerous systems onboard which could be attacked are represented on Figure 1.

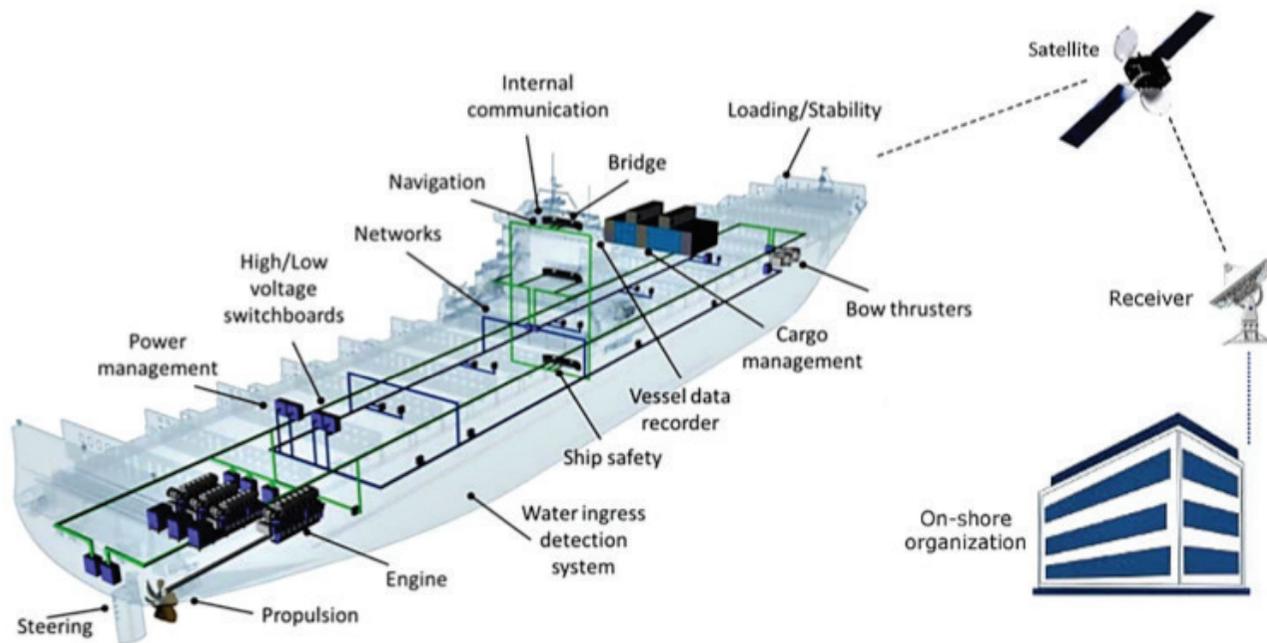


Figure 1. Connectivity between ship’s systems – all of them represent potential targets (Ording, 2019).

Risk management is fundamental for safe and secure maritime operations and it should adapt to the world of digitalization, automation, and interconnected businesses (International Maritime Organization, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3, 2017).

In the following sections we review the most common forms of cyber-attacks in maritime industry, the most important threats and ways of defending upon them with a focus on ship’s infrastructure and operations.

2. INTERNATIONAL REGULATION AND GUIDELINES

Upon analyzing literature sources we have arrived at the conclusion that many maritime transport participants, in the first-place regulatory bodies and international organizations, are

taking part and offering different solutions for dealing with cyber threats in maritime industry.

The common feature of all analyzed sources is setting risk assessment as a first step towards protection from unwanted consequences.

The National Institute of Standards and Technology (NIST) brings „NIST Framework” which is widely used as approach to cyber security assessment, as well as a step towards the fulfillment of cyber risk management. The advantage of “NIST framework” lies in its universality and flexibility, which is why it can be employed in many industries, including the maritime one (National Institute of Standards and Technology NIST, 2018).

The International Maritime Organization (IMO) has taken decisive steps in order to solve and control maritime cyber risks.

Actually, Maritime Safety Committee (MSC) and The Facilitation Committee (FAL) have issued “Guidelines on maritime cyber risk management” (MSC-FAL.1/Circ.3) as an answer to the increased number of cyber-attacks. The Guidelines completely accept NIST framework with five key elements: identification, protection, detection, response, and recovery (International Maritime Organization, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3, 2017).

There is also a Resolution numbered as MSC.428(98) – “Maritime Cyber Risk Management in Safety Management Systems”. This Resolution encourages flag states to force the companies to treat cyber security management at company level through “Safety Management System” (SMS) as the requirement of “International Safety Management Code” (ISM). Such a requirement should be fulfilled no later than first annual ISM verification after 1.1.2021. (International Maritime Organization, Maritime cyber risk management in safety management systems, MSC.428(98), 2017). If the companies fail to implement the required measures, their ships could be detained by Port State Control (PSC), thereby causing additional costs and business losses.

The IMO have developed a Strategic plan (International Maritime Organization, Strategic plan for the organization for the six-year period (2018 to 2023), A 30/Res.1110, 2017) for the period between 2018 and 2023 where the need for an integration between the existing and new technologies in the regulatory process is recognized, aiming at balancing benefits between

security, safety, and environmental protection as well as the influence on personnel both onboard and ashore.

For the same purpose the Baltic and International Maritime Councils (BIMCO) in (BIMCO, 2017) rely on publications of NIST and IMO. The BIMCO’s attitude is published as „Guidelines on Cyber Security Onboard Ships“. BIMCO approaches to cyber risk problems through the following items: 1-identification of threats and vulnerabilities, 2-assesment of risk exposure, 3-development of protection and detection measures, 4-establishment of contingency plans to respond and recover upon a cyber security incident.

In “Code of Practice – Cyber Security for Ships” (Boyes, H. and Isbell, 2017) cyber risk problems are solved without reliance on the afore mentioned NIST framework. Actually the development of cyber risk management plan should rely upon cyber risk security assessment, which remind us of the fundamentals of “International Ship and Port Facility Security Code” (ISPS) dealing with general security onboard ships and at port facilities.

All that has been stated above is complemented by numerous classification societies which are publishing guidelines in order to direct their clients towards the right path. In (DNV-GL, 2016), the most important classification society „DNVGL“, taking into consideration the IMO’s and BIMCO’s guidelines, as well as NIST framework, defines three factors as key elements in order to improve cyber security: 1-assessment, 2-improvement, 3-verification, followed by validation.

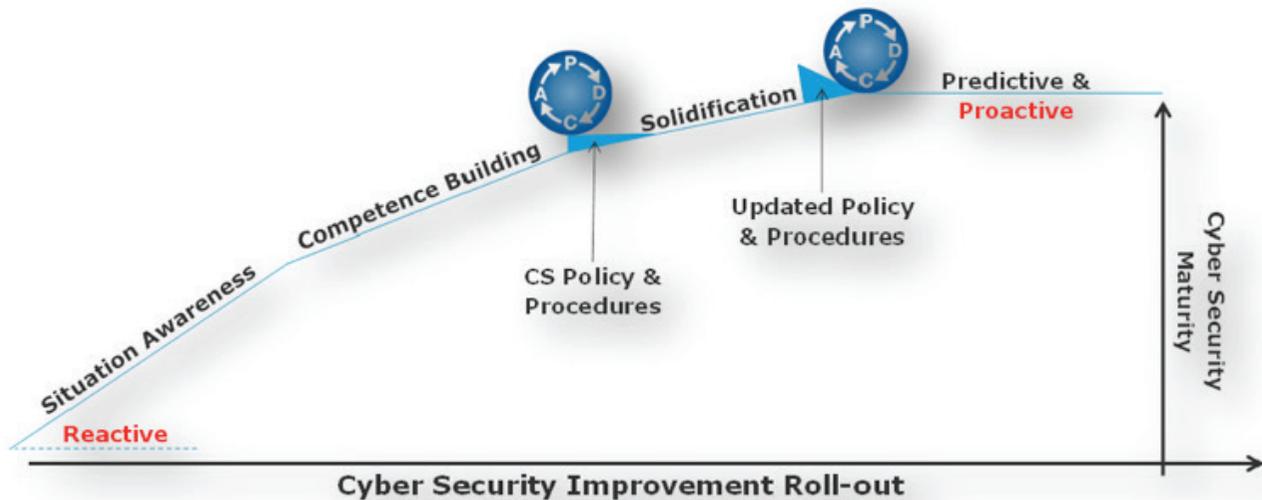


Figure 2. Flow of adequate approach to cyber security problem onboard (DNV-GL, 2016).

“DNVGL” relies on Deming circle, namely „PDCA“ cycle, as it is trying to induce maritime transport participants to continually assess their current risk using the risk matrix and other methods, with a view to creating a productive and proactive system (Figure 2). Due to a rapid technology development, cyber security assessment should not rely only upon the well-known risks. On the contrary, it requires a predictive and proactive approach which takes into account all systems onboard and ashore, their design, interconnection, and management manner.

In repetitive „PDCA“ cycle, the human factor must be acknowledged as equally important as all other business aspects - “the desired behavior and awareness in terms of cyber security therefore needs to be evaluated just like any other objective” (DNV-GL, 2016).

The latest regulation, which will certainly have a great impact on shipping companies, is EU “General Data Protection Regulation” (GDPR) which came into force in May, 2018. GDPR forces shipping companies to conduct an assessment of impact on personal privacy at any time when there is an increased risk of privacy violation. Companies are obliged to report any system violation within 72 hours in order to enable the entire industry to react quickly upon potential cyber-attacks (EUGDPR.org, 2018).

However, the insurance against the cyber related risks is still unrecognized for the maritime industry sector. The hull and machinery insurance (H&M) policies exclude cyber related risks by inserting relevant clauses, such as Cyber Attack Exclusion Clause (CL380), while Protection and Indemnity Insurance (P&I) offer pools with a limit of \$30 million USD per ship in case of cyber-attacks which are not related to war or terrorist attack activities (Lagouvardou, 2018).

3. HISTORIC REVIEW OF MARITIME CYBER-ATTACKS

The exact number of maritime cyber-attacks is unknown and can be considered to be much greater than reported, as attacks are frequently unnoticed or companies do not want to publish such information in order not to endanger their business or frighten their customers.

In the recent era a set of attacks has resulted in data, system, and equipment breaches, as well as serious financial losses. Depending on the kind of attack, consequences vary from minor to moderate, such as in the case of data theft, while in the case of taking control over the whole system, for instance a vessel, they seem to be reaching catastrophic levels.

Large cargo shipments usually travel for weeks across the oceans before reaching their final destination, which makes them highly vulnerable to cyber-attacks as there is enough time to remove evidence of the crime (Jones, Tam and Papadaki, 2016).

The following is a list of the most important maritime cyber-attacks:

1. Few companies providing security onboard ships sailing through “High Risk Area” (HRA) were subject to hacker attacks back in 2011. Pirates successfully accessed sensitive data on vessels movement, their cargo and insurance. Using that, they were able to plan their further actions and request ransom. Those attacks had the same scenario – “key log” malwares were used to record each keyboard press, and send the logs further to pirates’ e-mail addresses (Frodl, 2012).

2. Port of Antwerp in Belgium was under hacker attacks committed by sophisticated drug smugglers in the period between 2011. and 2013. Using malwares and, subsequently, on, other methods, the hackers were successfully finding out the location of cargo containers containing narcotics. Afterwards they used to send their own drivers to collect the goods before the real owner could come to pick up the container. The Port authorities realized that something was going on just after whole containers had started to disappear (Bateman, 2013).

3. Despite the fact that the main purpose of Automatic Identification System (AIS) is increase in safety, easier identification and communication at sea, a research (Balduzzi, Wilhoit and Pasta, 2014) shows that AIS has many deficiencies, especially in terms of cyber security because it is completely cyber unprotected. There were tests carried out to confirm such issues, during which false AIS symbols were generated on various locations around the world. The consequences which can result from a misuse of AIS are enormous.

4. A group of students successfully proved weaknesses and imperfections of Global Positioning System (GPS). In 2013 they hacked the GPS signal on a private yacht and distributed false position data to navigational equipment. As the track-pilot was active, automatic correction of course had been initiated in order to put the yacht back on route (Vaas, 2013).

5. Jamming of the GPS signal can cause a lot of trouble for navigation and positioning, both ashore and at sea. As GPS is under the control of the USA, the representatives of the White House issued a diplomatic warning to North Korea, due to a strong jamming encountered in Seoul. At that time the propagation of strong radio waves caused a lot of trouble to airplanes flying over the area affected (GPS World, 2016).

6. In 2014 hackers used malware to shut off an oil platform and completely disable it for a period of 19 days (Wagstaff, 2014).

7. In June 2017 the biggest container operator in the world “Maersk”, suffered an enormous cyber-attack. “NotPetya” malware triggered a need for reinstallation of more than 4,000 servers and 45,000 PCs. The company was forced to transport, load, and discharge containers without the IT support for 10 days (Cimpanu, 2018).

8. Also, in the summer of 2017, “Svitzer” company was a victim of data theft – over 5,000 e-mails with personal data were redirected to outside addresses. More than 400 employees

were endangered. The problem arose 10 months before it was discovered and then fixed within 5 hours. The investigation confirmed that messages had been redirected to the outside addresses but, when the mailboxes become full, the e-mails were returning as non-delivered (Bogle, 2018).

9. Another gigantic company "COSCO" was a victim of „NotPetya“ malware in July 2018. During the attack, communication channels were disabled, first at port of Long Beach and then in the whole USA territory (Cimpanu, 2018).

4. ATTACK FORMS

The Classification society "Lloyd Register" in (Lloyd's Register, 2018) states that the number of cyber-attacks has increased by 27 % per year, while 86 % of companies were victims of cyber-attack during 2017. The same source states that 44 % of companies believe their IT system requires upgrade in order to meet cyber security requirements, especially because 39 % of those companies suffered attacks during 2017.

According to another research (IHS Markit, 2018), the most significant maritime cyber problems are manifested in one of the following forms:

1. „Phishing“ is the most common form of cyber incident. Attacks can be classified in two groups – the first one known as social engineering and the second one based on malwares (Gupta et al., 2017). In the case of social engineering, the attackers try to cause harm via e-mail which seems harmless at a glance, or via fake web site. On the other hand, malware phishing uses malwares installed on client's PC.

This kind of threat is common onboard vessels in the form of e-mail. Usually e-mail contains a hyperlink to a fake web site where the user will, due to inattention or lack of knowledge, type personal details, such as username and password, to access their account. This usually happens when, due to being extremely busy, crew members do not pay attention to the e-mail content or the hyperlink.

2. Malware is a „computer code written to steal or harm. It includes viruses, spyware, and ransomware. Sometimes malware only uses computing resources (e.g. memory), but at other times it can record your actions or send your personal and sensitive information to cyber criminals“ (Paulsen and Toth, 2016).

3. "Spear phishing" is a form of "phishing" and represents one way of unauthorized collection of personal and sensitive data. Hence the hacker performs a "spear phishing" attack in the following manner: he contacts person „A“ inside the company, introducing himself as person „B“, who is at the same time superior to person „A“. He uses fake e-mail address, but very similar to the company official's one, attaching a file or a hyperlink to the e-mail. By clicking the file in the attachment or by opening the link, login details are shared, transactions are

authorized, or whole company's network becomes infected. Therefore person „A“ shares login details or passwords thinking that he is communicating with the superior.

4. Identity fraud – cyber-attacks can be aimed exclusively at stealing identity in order to use it for further crimes. Identity fraud is commonly committed by using „Trojan“ malware.

5. Ransomware is a kind of malware. A seemingly normal and harmless e-mail can cause a lot of trouble. Ransomware is usually in form of „.pdf“ or „.zip“ files attached to e-mail. By opening these files the system is brought to danger as the malware initiates denial of access to document or to the system. The solution is in paying off ransom in order to restore access to files or system.

6. „Man in the middle“ (MITM/MIM) is a kind of malware which relies on SSL/TSL protocol weakness, being correspondent in communication between two network users (Čekerevac et al., 2017; Mallik et al., 2019). In such a case, downloading of important data occurs while users can rarely detect it.

7. Data theft usually goes unnoticed or is discovered too late. Data is being copied or downloaded without authorization. Committing criminal activities by using ransomware and malware, unauthorized access results in data theft and data deletion in order to hide the traces or to cause a lot of harm to business (Borazjani, 2017). This is supported by the fact that over 50,000 e-mails of "Svitzer" company were subject to data theft back in the summer of 2017 (Bogle, 2018).

5. HOW TO SOLVE A PROBLEM?

Issuing the „Guidelines on Maritime Cyber Risk Management“ the IMO responded to an increase in cyber-attacks by accepting the NIST framework containing of five elements: identification, protection, detection, response, and recovery (International Maritime Organization, 2017). Similarly, BIMCO (BIMCO, 2017) defines the circle process based on the NIST approach (Figure 3).

Identification is a process of identification OF internal and external weaknesses or risks. It contains knowledge about: personnel and their abilities to recognize risks; systems; data and other elements that can cause a risk due to disruption of normal IT process within the company.

Detection means that it is necessary to conduct activities in order to spot the cyber threat as soon as possible. Hence, early threat detection leads to early detection of malicious intentions followed by on-time steps which will limit the consequences to the part of the system, protecting the rest of it.

Protection requires following of contingency plans in case of threat or incident, as well as procedures and measures to recover from the attack in good time.

Response to threats depends on the development and implementation of plans and activities which will restore the system upon cyber-attack.



Figure 3.
Cyber risk management (BIMCO, 2017).

Recovery is the last phase which requires implementation of measures to restore the system and the data which were under attack. This phase precedes the first one – identification of risks and weaknesses.

Notwithstanding the fact that these elements have a general character, they provide clear guidelines to companies which are free to create their own procedures and solutions in order to satisfy their own needs.

We believe that there are three basic considerations upon which cyber security measures must rely:

1. *Human resources* – personnel should be aware of risks and have adequate skills and qualifications. Also, employees should be familiar with the procedures, levels of authorization, physical security barriers, and they should be well trained in risk response.
2. *Technology* – adequate system design is a requirement. Software configuration should satisfy further inspection, verification, and testing processes.
3. *Processes* – include management of systems and networks, management policies and procedures, audits, contracts with third parties etc.

It is for these reason that the cyber security battle is not dependent solely on IT. Hence, it should start at the top of the company with implementation of cyber security procedures through the SMS. That is the most important precondition for the future plan development, education and training of seafarers,

as well as for creating appropriate conditions for successful protection against attacks and threats.

Every single user onboard, as well as ashore at the company headquarters, should be limited with user rights with regard to some information, data, or parts of the system. The reason which lies behind limitation of access and user rights is mainly referred to steps made due to lack of knowledge or unintentionally, causing the system to become vulnerable and exposed to data theft or similar incidents.

IT network onboard is the crucial element of defense against cyber-attacks. However, the real disposition and protective measures onboard vessels are usually not as prescribed by international recommendations. Therefore the network configuration and its protective measures are of utmost importance, which can be achieved by following recommendations and company procedures. At first, the use of firewall to separate internal (safe) network from external (unsafe) network is crucial.

Performing of security assessment will enable the company to spot its weaknesses and vulnerabilities and to minimize them to the maximum extent. Based on the remaining and unsolved weaknesses and vulnerabilities, it is necessary to develop preventive measures, as well as recovery measures, in case of a successful cyber-attack.

In order to meet all of the afore mentioned requirements, it is necessary to monitor obeying the procedures, tasks and activities, as well as to monitor personnel behaviour in relation to the usage of IT resources.

Since there is an increasing number of systems onboard which are accessible from the company's headquarters, such systems should be treated with special attention, protected with additional procedures which will enable safe and secure access whenever it is necessary.

Implementation of anti-malware and anti-virus is a must, and there is no need to particularly underline it within this article.

It is very common for the whole systems to get infected onboard ship by using infected USB drives. This can be classified as user's insufficient knowledge. Companies should find a way to overcome such and similar occurrences – usually by implementation of online trainings provided by renowned companies „VIDEOTEL“ or „SEAGULL“, or even by classification societies. Tanker shipping companies have widely accepted newly introduced „OCIMF“ requirements by using „Tanker management and self-assessment“ (TMSA) tool (OCIMF, 2018). Employees' education expenses are negligible in comparison to the costs which may arise in case of a cyber-attack.

There is also a need for introducing “Cyber Security Officer” (CySO) (Boyes, H. and Isbell, 2017). CySO should be delegated to perform cyber security assessment and to implement actual security plan, as well as to educate crew to respond to more and more frequent threats. Of course, CySO should be adequately educated and certified to conduct such a demanding task.

6. CONCLUSION

Cyber threats, vessels, port terminals and other maritime systems evolve simultaneously. Negative effects of cyber-attack are evident not only onboard the victim vessel, but in a much wider sector including shipping companies, port terminals, interconnection systems etc.

GPS signal jam causing the crude oil tanker to ground in dense fog is much more serious than the grounding itself, by far exceeding the average costs. In such a case, the oil spillage is bound to cause an ecological catastrophe. Apart from GPS imperfections and its misuse, this article has presented other unpleasant events with, in the majority of cases, serious consequences.

Apart from the great attention which is already being given to maritime cyber security, much more should be done. Regulation is just one step towards the goal achievement. However, the personnel seems to present an even bigger problem than the regulation itself, because it often happens that the crew onboard, with minimum or no knowledge about this

matter, inadvertently perform some tasks, frequently resulting in the system being exposed and open to attack.

Awareness is a necessity in all business aspects – if there is no awareness among employees at the company headquarters, then all awareness onboard ship will not have a great impact. Sooner or later, the difference between successful and unsuccessful business companies will be in their sustainability in response to cyber-attacks.

Our future work will be aimed at improving the efficiency of seafarers' education related to minimizing the number of successful cyber-attacks onboard vessels. Special attention should be given to various forms of training which will become mandatory in the near future. The creation of comparative analyzes, assuming that companies abide by the new European Union “General Data Protection Regulation“, should provide answers as to what extent the maritime industry has successfully responded to new form of war – cyber threats.

REFERENCES

- Allianz Global Corporate & Specialty SE, 2018. Allianz Risk Barometer 2018: Appendix. Available at: https://www.agcs.allianz.com/assets/PDFs/Reports/Allianz_Risk_Barometer_2018_APPENDIX.pdf, accessed on: 20 November 2018.
- Balduzzi, M., Pasta, A. & Wilhoit, K., 2014. A security evaluation of AIS automated identification system. Proceedings of the 30th Annual Computer Security Applications Conference on - ACSAC '14. Available at: <http://dx.doi.org/10.1145/2664243.2664257>.
- Balobaid, A. and Debnath, D., 2018. Cloud Migration Tools: Overview and Comparison, in: Yang, A. et al. (eds), SERVICES 2018, LNCS 10975, pp.93-106., Available at: <https://doi.org/10.1007/978-3-319-94472-2>
- Bateman, T., 2013. Police warning after drug traffickers' cyber-attack, BBC News. Available at: <http://www.bbc.co.uk/news/world-europe-24539417>, accessed on: December 2nd 2018.
- BIMCO, 2017. The guidelines on cyber security onboard ships, version 3. Available at: <http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=16>, accessed on: November 1st 2018.
- Bogle, A., 2018. Svitzer employee details stolen in data breach affecting almost half of its Australian employees, ABC News. Available at: <https://www.abc.net.au/news/2018-03-15/sensitive-data-stolen-from-global-shipping-company-svitzer/9552600>, accessed on: November 30th 2018.
- Borazjani, P.N., 2017. Security Issues in Cloud Computing. Lecture Notes in Computer Science, pp.800–811. Available at: http://dx.doi.org/10.1007/978-3-319-57186-7_58.
- Boyes, H. and Isbell, R., 2017. Code of Practice Cyber Security for Ships, London: Institution of Engineering and Technology.
- Čekerevac, Z. et al., 2017. MAN-IN-THE-MIDDLE ATTACKS AND INTERNET OF THINGS Z. Čekerevac, ed. FBIM Transactions, 5(2). Available at: <http://dx.doi.org/10.12709/fbim.05.05.02.03>.

- Cimpanu, C., 2018. Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover From NotPetya Attack, Bleeping Computer. Available at: <https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/>, accessed on: December 7th 2018.
- Cimpanu, C., 2019. Ransomware Infection Cripples Shipping Giant COSCO's American Network, Bleeping Computer. Available at: <https://www.bleepingcomputer.com/news/security/ransomware-infection-cripples-shipping-giant-coscos-american-network/>, accessed on: January 4th 2019.
- DNV-GL, 2016. Recommended practice: Cyber security resilience management for ships and mobile offshore units in operation, DNVGL-RP-0496.
- Einsig, B., 2016. Cloud Computing, The Internet of Things and Maritime Transportation, Cisco. Available at: <http://aapa.files.cms-plus.com/SeminarPresentations/2016Seminars/2016SecurityIT/Einsig.pdf>, accessed on: December 4th 2018.
- EUGDPR.org, 2018. GDPR Key Changes. Available at: <https://eugdpr.org/the-regulation/>, accessed on: December 14th 2018.
- Frodil, G.M., 2012. Pirates Exploiting Cybersecurity Weaknesses in Maritime Industry - Wave of cyber-attacks, SAFETY4SEA. Available at: <https://safety4sea.com/pirates-exploiting-cybersecurity-weaknesses-in-maritime-industry>, accessed on: February 2nd 2019.
- GPS World, 2016. State Department issues notice on North Korean jamming. Available at: <http://gpsworld.com/state-department-issues-notice-on-north-korean-jamming>, accessed on: November 1st 2018.
- Gupta, B.B. et al., 2016. Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, 28(12), pp.3629–3654. Available at: <http://dx.doi.org/10.1007/s00521-016-2275-y>.
- IHS Markit, 2018. Maritime Cyber Survey 2018 - the results. Available at: <https://bi-cd02.bimco.org/-/media/bimco/news-and-trends/news/security/cyber-security/2018/fairplay-and-bimco-maritime-cyber-security-survey-2018.ashx>, accessed on: December 5th 2018.
- International Maritime Organization, 2017. Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3. Available at: [http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20\(Secretariat\).pdf](http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf), accessed on: November 15th 2018.
- International Maritime Organization, 2017. Maritime cyber risk management in safety management systems, MSC.428 (98). Available at: [http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428\(98\).pdf](http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf), accessed on: November 15th 2018.
- International Maritime Organization, 2017. Strategic plan for the organization for the six-year period 2018 to 2023, A 30/Res.1110. Available at: <http://www.imo.org/en/About/strategy/Documents/A%2030-RES.1110.pdf>, accessed on: November 15th 2018.
- Jones, K.D., Tam, K. & Papadaki, M., 2012. Threats and Impacts in Maritime Cyber Security. *Engineering & Technology Reference*, 1(1). Available at: <http://dx.doi.org/10.1049/etr.2015.0123>.
- Lagouvardou, S., 2018. Master thesis: Maritime Cyber Security: concepts, problems and models, Technical University of Denmark – DNU. Available at: http://orbit.dtu.dk/files/156025857/Lagouvardou_MScThesis_FINAL.pdf, accessed on: April 14th 2019.
- Lloyd's Register, 2018. Building resilience against new risks - cyber security for an era of innovation. Available at: https://info.lr.org/l/12702/2018-09-03/5bl2c4/12702/196667/lr_cyber_security_brochure_digital_201809.pdf, accessed on: November 1st 2018.
- Mallik, A. et al., 2019. Man-in-the-middle-attack: Understanding in simple words. *International Journal of Data and Network Science*, pp.77–92. Available at: t.
- National Institute of Standards and Technology NIST, 2018. Framework for Improving Critical Infrastructure Cybersecurity, 1.1. Available at: <https://doi.org/10.6028/NIST.CSWP.04162018>
- OCIMF, 2018. About TMSA. Available at: <https://www.ocimf.org/sire/about-tmsa/>, accessed on: November 30th 2018.J.
- Ording, K., 2019. Ethical Hacking, DNV GL. Available at: <https://www.dnvgl.com/feature/ethical-hacking.html#start>, accessed on: February 1st 2019.
- Paulsen, C. and Toth, P., 2016. Small Business Information Security: The Fundamentals, NIST Interagency/Internal Report (NISTIR) - 7621 Rev 1. Available at: <https://doi.org/10.6028/NIST.IR.7621r1>, accessed on: November 11th 2018.
- Shaikh, S.A., 2017. Future of the Sea: Cyber Security - Foresight Evidence Review, Government Office for Science, London: Crown. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/671824/Future_of_the_Sea_-_Cyber_Security_Final.pdf, accessed on: December 15th 2018.
- Shiptech, 2015. United Arab Shipping Company (UASC) implements Shiptech to streamline its fuel purchasing. Available at: <http://www.shiptech.com/press-release/uasc-2015/>, accessed on: December 15th 2018.
- Vaas, L., 2013. \$80 million yacht hijacked by students spoofing GPS signals, Naked Security. Available at: <https://nakedsecurity.sophos.com/2013/07/31/80-million-yacht-hijacked-by-students-spoofing-gps-signals/>, accessed on: December 9th 2018.
- Wagstaff, J., 2014. All at sea: global shipping fleet exposed to hacking threat, Reuters. Available at: <https://www.reuters.com/article/us-cybersecurity-shipping/all-at-sea-global-shipping-fleet-exposed-to-hacking-threat-idUSBREA3M20820140423>, accessed on: December 7th 2018.