THE ANNALS OF "DUNAREA DE JOS" UNIVERSITY OF GALATI
FASCICLE XI – SHIPBUILDING. ISSN 1221-4620, e-ISSN 2668-3156
DOI: https://doi.org/10.35219/AnnUgalShipBuilding/2024.47.04
2024

ASSESSING CYBER RISKS ON BOARD SHIPS: A LITERATURE REVIEW

Costel Ungureanu
"Dunarea de Jos" University of Galati,
Faculty of Naval Architecture, Galati,
47 Domneasca Street, 800008, Romania,
E-mail: costel.ungureanu@ugal.ro

Carmen Gasparotti
"Dunarea de Jos" University of Galati,
Faculty of Naval Architecture, Galati,
47 Domneasca Street, 800008, Romania,
E-mail: carmen.gasparotti@ugal.ro

ABSTRACT

Due to the multiple cyber-attacks that resulted in financial losses and personal information breaches, cyber security has become an essential issue for the maritime industry today. This research aims to identify the potential cyber risks associated with operational technology (OT) systems on board ships that influence the cyber security of vessels through a state-of-the-art literature review. Assessment of the cyber risks on board is carried out according to their likelihood and severity, using a risk score matrix, based on which, they are classified into three categories: high risk, medium risk, and low risk. Based on the classification of cyber risks on board the ship in the three categories, the measures to mitigate them can be defined, to ensure cyber hygiene on board the ship.

Keywords: cyber risk, cyber security, OT systems, score matrix, maritime industry

1. INTRODUCTION

Cyber security has become a vital topic in the last period, for the maritime industry, due to the digital advances made to improve maritime operations. With all the benefits brought, however, the digital operations on board the ship can constitute a significant threat to the safety of the vessel and the crew, without an awareness of the cyber security role and how cyber hygiene can be put into practice [1, 2]. All existing systems on the ship (routers, network cables, IT and OT systems, communication systems, machinery and power control systems, propulsion systems, cargo management systems, and navigation systems) must be protected from any cyber threat, which can have a major impact on ship safety. That is why the cyber risk management associated with the systems on the ship is a major priority today [2]. To address the impact of these cyber risks on shipboard systems and the necessary security controls, guidelines have been developed by several bodies and companies such as the American Bureau of Shipping (ABS), International Maritime Organization (IMO), iTrust Center for Research in Cyber Security, National Institute of Standards and Technology (NIST), Digital Containership Association (DCA), Baltic and International Maritime Council (BIMCO), Cruise Lines International Association (CLIA), Det Norske Veritas (DNV), International Chamber of Shipping (ICS), International Association of Independent Tanker Owners (INTERTANKO), International Association of Dry Cargo Shipowners (INTERCARGO), Oil Companies International Marine Forum (OCIMF) etc.) [2], [3], [4], [5], [6], [7]. These guidelines created are feasible and cost-effective to be applied by both ship owners and maritime authorities, and they list the attack surfaces and cyber risks associated with shipboard OT systems while presenting a description of the potential scenari-

os of attack. The large-scale introduction of automation, network-based systems, and the growing dependence on digitization, have led to the focus of cyber risk management in the maritime industry. The paper aims to present a methodology for assessing cyber risks on board the ship to highlight the severity and likelihood of these risks, should they occur, and also the framing of cyber risks associated with the OT systems on board the ship by risk levels.

2. LITERATURE REVIEW

Cybersecurity considers how cyber risks are managed, which can affect information and technology, to protect the confidentiality, integrity, and availability of informational and technological assets, with the role of protecting the economy and people's lives [7]. The maritime sector has an essential role in international trade. Considering the very high economic impact of a cyber-attack on sea transport, which means extremely high costs, major damages, and significant disadvantages, ensuring the cyber security of this industry becomes a necessity [2]. Changki et al. (2019) stated that cyber-attack incidents in the maritime industry have led to unquantifiable monetary losses, the loss of intellectual property, and decreased customer trust. However, there is limited research in the literature regarding maritime cyber security. Also, the authors define maritime cyber risk, as the extent to which a technological asset is threatened by a potential event, which could lead to operational, safety, or security failures of the transport at sea, due to corrupt or compromised systems. Following resolution MSC.428 (98), adopted by the IMO in 2017 (Maritime Cyber Risk Management in Safety Management Systems), cyber risk management must be included in the ship's safety management system, considering the objectives and functional requirements of international safety management [2]. IMO also refers to the guidelines published by maritime organizations (BIMCO, Intercargo, INTERTANKO, DCA, ICS, etc.), in 2020, regarding cyber security on board ships, focusing on the need for cyber security awareness, highlighting cyber risks, but also recommendations regarding their management, as well as the best measures to be implemented to ensure cyber security on board the ship [4]. On the other hand, DNV (2016), has made recommendations on cyber security measures, based on the guidelines issued by IMO and BIMCO, focusing on the validation mechanisms necessary to increase the resilience of cyber security to shipboard [8]. In 2020, the guide provided by DNV on "cyber security" for class notation focused both on the cyber security of the ship's primary functions (propulsion, navigation, steering, power generation, etc.), as well as on the operational needs of ship owners [7].

3. RESEARCH METHODOLOGY

Based on the evidence presented above, it follows that it is essential for the maritime industry to address cyber security quickly. This paper wants to identify the main risks (threats) that influence cyber security on board the ship and how they can be evaluated, considering the severity and likelihood of these risks, based on the study of the latest specialized literature. A first step in risk assessment can be to review the potential cyber risks on board the vessel. For this research, the authors studied some guidelines and codes of practice from (1) ABS, (2) IMO, (3) iTrust Center for Research in Cyber Security, (4) NIST, (5) BIMCO, (6) DNV, regarding cyber security in the maritime industry, but also several scientific articles [2], [3], [4], [6], [7]. Several keywords were used "cyber risks on board the ship", "cyber risk management", "cyber-attack in the maritime industry", and "cyber security assurance". From all the literature studied, 15 guides/articles were selected and used as a data source. Based on the analysis of these

materials was established a methodology for addressing cyber risks identified on board the ship. Given the shipboard OT systems, fundamental to the ship's operations (propulsion systems, communications, navigation, shipboard cargo management, and power control), which are vulnerable to cyber-attacks, either as a result of any deficiencies of these systems, either due to the network deficiencies to which they are connected, the potential cyber risks on board the ship were identified, from the studied literature, and classified, according to their severity and likelihood of occurrence [1].

4. CYBER RISK ASSESSMENT ON BOARD SHIP

OT systems are connected to the Internet for communications, operations, etc. This interconnectivity between shipboard OT systems and the IT network can be the entry point for hackers seeking to damage or gain access to existing shipboard systems. The potential cyber risks, corresponding to the OT systems on board the ship, are presented in Table 1.

Table 1 Cyber risks of shipboard OT systems (processing according to [1])

Shipboard OT system	Potential cyber risk
1. Propulsion and power control systems	
- *the energy management system* - *the generators* - *the fuel supply system and the engine control system*	-malware attack through USB ports that are infected to activate the data transfer right, -Man-in-the-middle (MITM) attack, which allows the hacker to read/modify a conversation
2. The communication system	
-*satellite communication system* - *the integrated communications system*	-malware attack through phishing e-mails, -exploiting vulnerabilities in outdated VSAT software, by hackers using weak points/errors in the operating system to gain unauthorized access to resources/compromise data/take control over the system, -script exploits to attack the website server, - interceptions by ear
- *wireless local area network (WLAN)*	- Denial of Service (DoS) attack, which interrupts the network service, - interceptions by ear, - falsification of access points
3. Load management systems	
- *the ship's ballast system*	-Phishing emails, -malware attack, which damages/compromises data or blocks access to the system
-*load control room*	-malware attack, which damages/compromises data or blocks access to the respective device, -ransomware that blocks access to data
4. Navigation system	
-*integrated navigation system*	-Man-in-the-middle (MITM) attack, which allows the hacker to read/modify a conversation, -arbitrary overwriting of files and remote code execution, a risk that requires improved security measures

-global positioning system (GPS)	-GPS spoofing/jamming
- the electronic map display and information system	-malware attack through USB ports that are infected to activate the data transfer right, -Denial of Service (DoS) attack, which interrupts the network service, -spoofing, by which the return address of sent e-mails is falsified, hiding the identity of the real address from which the message originates
- the automatic vessel identification system (AIS)	-spoofing, by which the return address of sent e-mails is falsified, hiding the identity of the real address from which the message originates -software manipulation,
- the radar system	-Man-in-the-middle (MITM) attack, which allows the hacker to read/modify a conversation, -malware attack, which damages/compromises data or blocks access to the system
- the global maritime safety system	-denial of service (DoS) attack, which denies legitimate users access to a resource (access to a website, a network, etc.), -falsification of data

The assessment of cyber risks on board the ship can be carried out, taking into account the impact (the effect produced if a cyber risk occurs) and the likelihood (the chance that the cyber risk will occur) of them, with the possibility of identifying the places where the security controls are needed.

When shipboard systems are updated or new software is installed, risk assessment becomes a necessity. To be able to assess the severity (impact) and likelihood of a cyber risk, a risk score matrix is usually used, which allows the calculation of this score for each cyber risk in the ship's OT system (risk score = the product between the severity score and likelihood). Depending on the complexity of the cyber-attack on the ship's systems and the attacker's access to resources and attack surface, the risk likelihood score can be decided. The severity of the risk can be determined depending on the extent of the damage caused to the environment, and the loss of integrity, finances, and confidentiality, which may result from a cyber-attack [1], [11]. Table 2 shows how the likelihood and severity scores are evaluated.

Table 2 Definition of likelihood and severity of cyber risks (processing according to [1])

Score	Level	Likelihood of cyber risk
4	High	The attack can be carried out from the external network, either remotely or with physical access to open ports and systems on the ship, with minimal technical knowledge and publicly available resources.
3	Medium-high	The attack can be carried out with basic technical knowledge, without modifying the exploits, the attacker being in the

		internal or external network.
2	Medium-low	The attack can be carried out with moderate technical knowledge, with minor changes to the exploits, the attacker being in the internal or external network.
1	Low	The attack can be carried out with advanced technical knowledge, by chaining several exploits, with physical or remote access to the OT systems on the ship, where there is restricted access.
Score	**Level**	**Cyber risk severity**
4	Critical	Consequences of a cyber-attack can be on the ship, ship operations, and crew, and these could be: loss of the ship, data, operating systems and resources may be unavailable, affecting all operations, which could lead to collision, imbalance, and sinking of the ship.
3	Severe	The consequences of the cyber-attack can lead to unauthorized access to the ship's network, data system, and other resources that affect the ship's operations, such as communications, propulsion, navigation, disruption of the ship-shore connection, etc.
2	Moderate	The consequences of the cyber-attack can cause damage to the ship or cargo, the authorized functionality of the networks can be affected, the lack of availability of systems or applications, the disruption of the operations on the ship, a deceptive communication between the systems on the ship.
1	Light	The consequences of the cyber-attack may consist of unauthorized access to the ship's systems, which may lead to a data breach.

Cyber risks associated with shipboard OT systems (Table 1) are assessed based on assigned scores for the likelihood and severity (Table 2). The risk score is obtained by the product of the likelihood score and the severity score, which is assigned to each cyber risk of the OT systems. With the help of the 4 x 4 score matrix, the risk scores are established, which allow the classification of the cyber risks associated with the OT systems on the ship, being classified into three categories: high risk (score: 12÷16), medium risk (score: 3÷ 9) and low risk (score: 1÷2) (Table 3).

Table 3 Score matrix of cyber risks

Likelihood		Severity			
		Light (1)	Moderate (2)	Severe (3)	Critical (4)
Low	(1)	1	2	3	4
Medium-low	(2)	2	4	6	8
Medium-high	(3)	3	6	9	12
High	(4)	4	8	12	16

Based on the literature research, it appears that most shipboard OT systems on board the ship are high risk (red), their vulnerabilities can be exploited quite easily by hackers, thus disrupting the operations on the vessel. Shipboard OT systems, which present medium risk (yellow), can be attacked by hackers to a lesser extent, which leads to the unavailability of the resources and the network on board the ship. Low-risk systems (green) can be attacked, but with lower chances, these attacks affect both the safety of the vessel and that of the ship's crew/cargo. Each risk is evaluated based on the vulnerabilities of the systems, the flow of data between the systems, the degree of knowledge of the functionality of the systems, and the dependence on the Internet connection [12], [14]. Even if some cyber risks are common to several shipboard systems, the risk scores differ, due to the difficulty of exploitation, attack surfaces, and the level of participation in the OT and IT network, which varies from one system to another (Table 4) [1].

Table 4 Systems on board the ship and their classification in risk categories (processing according to [1])

OT systems	Risk level	Cyber risk type
ship ballast system, load control room, electronic chart display, and information system, radar system, global positioning system (GPS), automatic vessel identification system (AIS), satellite communication system, integrated communications, fuel supply and engine control systems	High	Malware attack via Phishing emails, Denial-of-Service (DoS) attack, Malware intrusion, Ransomware, GPS spoofing
satellite communication system, integrated communication system, wireless local area network (WLAN), global positioning system (GPS), automatic vessel identification system (AIS), radar system, global maritime safety system, navigation system integrity	Medium	Spoofing, Cross-site scripting, eavesdropping, Man-in-the-middle (MITM) attacks, exploiting vulnerabilities in old software versions
Propulsion and power control systems	Low	Man-in-the-middle (MITM) attack

Placing cyber risks in one of the three categories allows the definition of measures to mitigate these risks. According to the iTrust Center for Research in Cyber Security guidelines, mitigation actions can be applied to shipboard OT systems to manage cyber risks [6], [14], [15]. These mitigating actions come to the aid of ship owners, who can determine the cyber hygiene of their ships, based on three levels of security: level 1, which includes cyber security measures recommended for managing high risks (12÷16),

and which must be implemented on board the ships; level 2, includes cyber security measures recommended for the management of medium risks (3÷9), and which assume the existence on board the ship of the security controls mentioned for this level; level 3, which includes cyber security measures recommended for managing low-level risks (1÷2), and which are suggested to be implemented on board the ship.

5. CONCLUSIONS

The shipboard OT systems have an important role in the operation of the ships, they are permanently interconnected based on internet connections and therefore their protection from cyber-attacks becomes essential. Cyber risks identified for OT systems can be avoided by applying appropriate security controls and ensuring the cyber hygiene of ships. These risks are evaluated using the risk score matrix, depending on the probability the cyber risks occur and the impact caused by their occurrence. Depending on the risk score obtained, cyber risks fall into three categories: high risk, medium risk, and low risk, based on which measures to mitigate them can be defined. Through the periodic assessment of the cyber risks to which the OT systems on board the ship are subjected, ship owners understand how they can discover the vulnerabilities within these systems, thus have a better picture of the impact of these risks, being motivated to apply the security measures that are required for each case.

REFERENCES

[1]. Dumbala, R., Rajaram, P., Goh Voon Vei, M. and J. Zhou, "A Cyber Risk Study in Shipboard OT Systems". Society of Naval Architects and Marine Engineers Singapore 40th Annual Journal 2020/2021, Sustainable Development & Digital Innovation, 2021, pp.48-60.

[2]. International Maritime Organization, Guidelines on Maritime Cyber Risk Management, 2017. Accessed: Aug. 27, 2024. [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

[3]. American Bureau of Shipping. "Guide for Cybersecurity Implementation for the Marine and Offshore Industries ABS Cyber safety", Vol 2, 2021. Accessed: Aug. 27, 2024. [Online]. Available: https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/251-guide-for-cybersecurity-implementation-for-the-marine-and-offshore-industries---abs-cybersafety%C2%AE-volume-2/251-cybersafety-v2-cybersecurity-guide-aug23.pdf

[4]. BIMCO, Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners (INTERCARGO), InterManager, International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Union of . Insurance (IUMI), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass) and World Shipping Council (WSC), "The Guidelines on Cyber Security Onboard Ships", 2020Accessed: Aug. 27, 2024. [Online]. Available: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

[5]. Det Norske Veritas, DNV GL Cyber secure class notation, 2020. Accessed: Aug. 27, 2024. [Online]. Available: https://www.traficom.fi/sites/default/files/media/file/5.%20DNV%20GL%20Cyber%20secure%20Class%20Notation%20Information%20Day%20Finland%20handout.pdf

[6]. iTrust Centre for Research in Cyber Security. "Guidelines for cyber risk management in shipboard operational technology systems", 2022 Accessed: Aug. 27, 2024. [Online]. Available: https://itrust.sutd.edu.sg/research/projects/maritime-cyber/

[7]. National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity", 2018. Accessed: Aug. 27, 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

[8]. Det Norske Veritas, "Cyber Security Resilience Management for Ships and Mobile Off-

shore Units in Operation", 2016. Accessed: Aug. 27, 2024. [Online]. Available: https://www.dnv.com/siteassets/images/pdf-documents/dnv-gl-rp-0496.pdf

[9]. Boyes, H. and Isbell, R. "Code of Practice Cyber Security for Ships", 2017, Accessed: Aug. 27, 2024. [Online]. Available: https://www.safety4sea.com/wp-content/uploads/2017/09/UK-Cyber-Security-Code-of-Practice-for-ships-2017_09.pdf

[10]. Parka, C., Shib, W., Zhangb, W., Kontovas, C., Changa, C. H. "Cybersecurity in the maritime industry: a literature review", *Proceedings of the International Association ofMaritime Universities (IAMU) Conference*, 2019, pp.79-86.

[11]. Cassi, E., Scialla, P. and Cavanna, J.P. "Tackling complexity: Protecting against cyber risk in the marine industry". Lloyd's Register Group Resilience Engineering, pp. 1-14, 2018. Accessed: Aug. 27, 2024. [Online]. Available: https://www.ccr-zkr.org/files/documents/workshops/wrshp050919/Docs07_en.pdf

[12]. Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J. and Kusev, P. "Risk perceptions of cyber-security and precautionary behavior", *Computers in Human Behavior,* vol. 75, no. 1, pp.547-559, 2017.

[13]. Craigen, D., Diakun-Thibault, N. and Purse, R. "Defining cybersecurity", *Technology Innovation Management Review,* vol. 4, no.10, pp.13-21, 2014.

[14]. Svilicic, B., Kamahara, J., Rooks, M. and Yano, Y. "Maritime Cyber Risk Management: An Experimental Ship Assessment". *The Journal of Navigation*, vol.72, no.5, pp.1108- 1120, 2019.

[15]. Caponi, S. and Belmont, K. "Maritime cybersecurity: A growing threat goes unanswered", *Intellectual Property and Technology Law Journal*, vol. 27, no. 1, pp.16-18, 2015.

Paper received on October 27th, 2024

