30th
International
Maritime
Lecturers
Association
Conference
Split
Croatia
www.imla30.org

International Maritime Lecturers Association
FACULTY OF MARITIME STUDIES

CYBERSECURITY FOR SEAFARERS: HUMAN FACTOR RISKS AND TRAINING SOLUTIONS

Pallab Das[1*], Sanjampreet Singh[2]

Abstract. The ever-growing digitalisation of the maritime sector has increased cybersecurity risks for seafarers, positioning human factors as a weak point. Cyberattacks against onboard systems, crew, and shore-based operations threaten vessel security, cargo integrity, and crew safety. Despite improvements in cybersecurity technologies, the human factor remains a significant challenge due to low awareness, poor training, and behavioural failures. This research examines the human factor risks causing cybersecurity threats in the maritime industry and assesses the efficacy of training programs to counter these risks. The study employs a mixed-methods design involving a systematic review of past cybersecurity incidents, expert interviews with maritime cybersecurity experts, and a survey among active seafarers. A simulation-based assessment is also conducted to quantify the effect of cybersecurity training interventions. Initial findings show that phishing, social engineering, and human error misconfigurations are the most prevalent vulnerabilities targeted by cybercriminals. Survey results show that over 60% of seafarers have received little or no cybersecurity training, with many not knowing even the most basic cyber hygiene measures. Simulation tests show a 40% increase in threat response among participants who received focused cybersecurity training. They highlight the need to include cybersecurity awareness courses in obligatory maritime training programs. It concludes that seafarer training needs to take a systemic approach, embracing real-time simulations, behavioural risk ratings, and continuous learning courses. Enhancing seafarers' cybersecurity culture is essential to improving maritime cybersecurity resilience and mitigating human factor threats.

Keywords: Cybersecurity; Seafarers; Human Factor; Maritime Security; Cyber Threats; Training Solutions.

[1] Centurion University of Technology and Management, School of Maritime Studies, Ramchandrapur, Jatni, Bhubaneswar, Odisha 752050, India

[2] Centurion University of Technology and Management, School of Law, Ramchandrapur, Jatni, Bhubaneswar, Odisha 752050, India

* **Corresponding author:** pallab.das@cutm.ac.in

https://doi.org/10.7225/imla30.46

1. INTRODUCTION

Most of the world's trade happens in the sea, and various technologies have been developed to guarantee reliability and safety in navigation, management, and communication. These consist of a combination of onshore and maritime technologies. The interconnection between ships and onshore infrastructure has provided increased operational and physical safety, and contributed to the increase in cyberattacks. The European Network and Information Security Agency (ENISA) published a report on the maritime industry's cybersecurity problem in 2011, assuming that the industry relies on Information and Communication Technology (ICT) and thus is exposed to various cyberthreats.

The report identified that maritime cybersecurity is low to non-existent because the number of known cybersecurity incidents is small, they are not made public, and there is no mechanism to determine the incidents. In order to improve maritime cyber-security, the report recommends several actions, including conducting cyber-security campaigns and training for stakeholders, implementing security measures for maritime information and communication technologies (security by design), incorporating cyber-security into maritime policies, identifying and registering essential goods in the maritime sector, developing shared security policies for the International Maritime Organisation (IMO) and the European Union, and improving information sharing amongst stakeholders.

Nearly 80% of maritime casualties result from human actions, which applies to maritime cybersecurity. It requires training and sensitisation to counter cyberattacks and prepare shipping staff to detect and remove cyber threats. They surveyed 86 Greek maritime sector workers to study the human element's contribution to maritime cybersecurity and whether good practices and directives are adopted. The survey consisted of two pilot tests, a research paper offering a methodology for evaluating ship vulnerabilities based on their cybersecurity, the European Union's NIS Directive, and associated publications of vulnerabilities.

This research favourably advances a deeper understanding of the issues that require attention by raising broad awareness of cyber risk and assisting the marine community in strategically mitigating risks against known and potential attacks.

2. COMMON VULNERABILITIES

With the rapid digitization of the maritime sector, it is more vulnerable to cyberattacks. Incorporation of Information and Communication Technology (ICT) into navigation, cargo operations, communication, and operational systems, as much as it increases efficiency, has also opened up substantial security threats. Most maritime technologies were not designed with cyber security as an initial aspect, thus they are most vulnerable to being exploited. This is further exacerbated by obsolete software, a lack of adequate security measures, and industry-wide ignorance or standardization in cyber activities. Consequently, the industry is prone to many shared cybersecurity vulnerabilities, such as:

2.1. Electronic Chart Display and Information System – ECDIS

ECDIS's system displays navigational information; charts: ship's position, RADAR and AIS. It should comprise at least three sensors (compass, position, and speed) and be installed on the bridge's operating system. The internet or a USB may update it. The sophisticated, safety-related ECDIS system provides various integration and display options. Shipowners and operators, equipment manufacturers, chart publishers, training institutions, and hardware and software maintenance suppliers are all part of it. Regulations were phased out in 2011 following the International Maritime Organization (IMO) requirement of electronic charts for navigation in 2009. However, a six-station network simulation environment determined that ECDIS is a perfect platform for running malicious code, as it runs on old operating systems, which are soft targets.

2.2. Automatic Identification System – AIS

Since 2004, the International Maritime Organisation (IMO) has required the Automatic Identification System (AIS) on all passenger ships by the International Maritime Organisation (IMO), primarily for traffic control, collision avoidance, and accident search and rescue. The system delivers ship data, e.g., IMO number, departure, and arrival port, without constantly requiring the ship crew or seamen to monitor bridges or coastal stations. Nevertheless, the AIS protocols are unencrypted and thus subject to malicious users intercepting or sending deceptive messages with erroneous data. The effectiveness of the system depends on the provision of correct information.

2.3. Global Navigation Satellite System – GNSS

Global Navigation Satellite System (GNSS) is a satellite-based system that presents the ship's position and sends data to receivers. Its dependability is based on accuracy, integrity, continuity, and availability. However, it is rated the second most vulnerable system following the AIS since it was also subject to jamming

and spoofing attacks. Jamming attacks are possible through cheap hardware, whereas spoofing attacks need satellite signal simulation with higher power.

2.4. Navigation Telex – NAVTEX

NAVTEX is a global service for navigation and meteorological details on shore/sea zones concerning ships. It is automatically collected and printed directly from the telex, where each vessel must be equipped with a message receiving device. NAVTEX offers safety information on shipping and meteorological conditions, which can be accessed via web pages. Still, it is under threat from interference, storage devices, the internet, and other connected systems, resulting in erroneous message reception or service disruption.

2.5. Voyage Data Recorders – VDR

A Voyage Data Recorder, also known as a VDR, is vital equipment on ships for recording data on a vessel that can be utilized for accident investigation. The VDR system consists of input signals, processing, encoding, recording medium, playback equipment, power source, and standby power source. The VDR captures speed, direction, position, engine, fuel, and voice communications data for the past 12 hours. These data are saved securely and can be accessed, pertinent to ship condition, movement, physical status, and command and control before and after an incident. These data are utilized in safety investigations to determine an incident's cause(s). VDR may also be employed for preventive maintenance, monitoring efficiency of performance, analysis of heavy weather damage, accident prevention, and training to enhance safety and minimize running costs. It is better than airplanes' black boxes because it retains information for at least 12 hours, repeatedly overwritten by the newest inform ation. VDR is, however, vulnerable to harmful activities within the ship and is connected to a local area network (Ethernet) instead of the Internet. The security of VDR has vulnerabilities like poor encryption, insecure authentication, and antiquated firmware.

2.6. Sailing Directions

Sailing Directions (Pilots) are essential port entry and coastal navigation information for every class of ship. With 76 volumes, they account for the world's principal commercial sea routes and ports. Every volume contains data on navigational dangers, buoyage, regulations, and general comments on countries, port facilities, seasonal currents, ice, and climatic conditions: high-quality diagrams and photography help bridge crews interpret vital information when planning passage. Sailing Directions complement the Electronic Navigational Charts (ENC) employed by ECDIS, giving information that adds to the ship's safety concerning the route to be taken during its voyage.

2.7. Global Maritime Distress and Safety System – GMDSS

The Global Maritime Distress and Safety System (GMDSS) is a global framework for maritime distress and safety communications, established in 1988 by the International Maritime Organization (IMO). It outlines the radiocommunications equipment required by ships, its maintenance and usage, and the context for establishing shore-based facilities to support GMDSS communications. Previously, distressed vessels relied on alerting other ships using their radio equipment. GMDSS changed this by requiring vessels to send their alert to shore, which then coordinates rescue efforts. This change was linked to the International Search and Rescue Convention (SAR Convention) and the Worldwide SAR Plan. GMDSS also improved ships' ability to declare distress and receive assistance from shore, and provided for the broadcast of essential safety-related information, Maritime Safety Information (MSI), which could be automatically received onboard ships at sea. However, vulnerabilities related to individual systems have been identified.

2.8. Long Range Identification and Tracking – LRIT

The Long-Range Identification and Tracking System (LRIT) (European Maritime Safety Agency (EMSA), 2009) provides information on the ship's identity. It offers comparatively safer data transport because satellite communications are the only means. Along with GMDSS, it is essential for search and rescue operations. The Denial of Service (DoS) assault is the most likely one that it could encounter.

2.9. Phishing

Phishing is a social engineering attack that steals users' information by fooling victims into opening malicious emails, instant messages, or text messages. The victim is deceived into opening a malicious link or file, resulting in malware installation, system freezing, or exposure of sensitive information. Email applications are critical in everyday shipping activities since they enable communication. Phishing is a human-related challenge that can only be effectively halted by humans, and there is no better means of avoiding threats from phishing attacks than through training. In the shipping industry, sailors and management utilise many applications, and email

applications have become an important aspect of day-to-day activities.

3. MARITIME CYBER-ATTACK INCIDENTS

There have been several assaults on ports, ships, and other data breaches throughout the years, proving that industry-specific cyberattacks are a reality. Hackers may be able to take over ship navigation and engine controls, access logistical software, and take advantage of financial records due to cyber threats and vulnerabilities. This section examines various cyberattacks that have occurred in the maritime sector in recent years:

3.1. Icefog

According to a Kaspersky assessment, an interactive espionage tool, advanced persistent threat (APT), has been operating since at least 2011. The technology, which malevolent people directly control, has targeted chiefly South Korean and Japanese government agencies and maritime corporations. Because of their persistence and capacity for evasion, APTs pose a serious threat to governments and organisations. The goal of spear phishing emails used in icefog targeted cyberattacks is to trick the target into visiting a harmful website or attachment. The first two vulnerabilities are exploited using Microsoft Office documents (Word and Excel) that drop and run the backdoor and show the victim a fake document. According to Kaspersky Lab (2013), these are often the attack tactics that attackers employ the most these days.

3.2. NotPetya

While some A.P. Moller-Maersk employees received notices that their essential files were being encrypted, others started receiving notifications in June 2017 that their file systems were being fixed. NotPetya's hacking into Maersk and several other multinational companies began at this point (Capano, 2021). NotPetya gave the attackers the access they needed to compromise the entire system by successfully breaking into a single Odessa computer. Consequently, vital elements essential to preventing ship capsizing, like port facilities, reservation systems, and container loading systems, were stopped. Maersk created an incident response team and set up a recovery centre to reduce the impact and aid recovery. The recovery operation included hundreds of employees working day and night worldwide. Maersk staff later found that they had a backup in their Ghana office. Fortunately, a power outage had disconnected the server from the network before the NotPetya attack, leaving one clean copy of the company's domain controller data behind. The recovery team was relieved by the discovery of this backup. Overall, the estimated attack cost to Maersk was between $250 million and $300 million (Capano, 2021).

3.3. Port of Antwerp

Between June 2011 and June 2013, a Belgian organised crime organisation attempted a cyberattack against two companies situated in the Antwerp port. After successfully breaking into the targeted companies' computer networks, the group obtained private security data on the containers in the port. Because of this access, the organisation could steal cargo before the rightful owners could take possession. The thieves also used the port to smuggle drugs into the nation, taking advantage of the security flaw. When all containers went missing, port authorities realised there had been a breach. Authorities found more than a tonne of cocaine, worth 130 million pounds on the black market, and an equivalent amount of heroin during a police raid on the organisation (Bateman, 2013).

3.4. GPS Spoofing

False GPS signals are sent to a targeted system as part of a cyberattack known as GPS spoofing, which provides inaccurate navigational data. This can have hazardous consequences for the marine industry, including groundings, vessel collisions, and navigational errors (Lo, 2019). A recent event in the Black Sea demonstrated how standard GPS spoofing has grown as a hazard to the marine sector. At different points in late June 2017, several nearby ships reported anomalous GPS readings that misidentified their location at an airport. These incidents have raised concerns about cyberattacks and brought attention to the potential risks posed by GPS spoofing (Jones, 2017).

4. AWARENESS AND TRAINING

Training and sensitization onboard ships are prioritized in order to enhance cybersecurity through addressing vulnerabilities and minimizing the potential for cyber incidents. Company policy must be to train the crew at all levels, including shipboard staff, on topics like recognizing phishing emails, password hygiene, and reporting suspicious activity. There must be an effective incident response plan, which outlines what to do in the case of a cyber incident, e.g., communications, roles and responsibilities, containment, investigation, and recovery processes. Effective change management processes should be implemented to guarantee IT or OT system changes are tested, approved, and documented to avoid unauthorized changes that can potentially introduce vulnerabilities. Access control is also necessary, as it

limits user privilege levels and guarantees authorized personnel have access only to essential systems and information. Secure password policies, regular review of user privileges, and auditing of attempts at unauthorized access are some of the things included.

Regular security awareness training is necessary to raise employee knowledge of the value of cybersecurity and establish a security-conscious culture inside the company. Physical security measures must be implemented to prevent unauthorised access to Information Technology (IT) and Operational Technology (OT) infrastructure. These measures include guarding server rooms, limiting physical access to vital equipment, and appropriately discarding sensitive data.

Third-party management is also crucial because businesses must evaluate the cybersecurity capabilities of their third-party suppliers and service providers, perform due diligence investigations, and incorporate contractual requirements by the company's standards. Businesses can improve their cybersecurity posture and help reduce cyber incidents on ships by using such procedural protective measures.

4.1. Collaboration and Information Sharing

Det Norske Veritas (DNV) has identified the need for cooperation and exchange of information among government agencies, port authorities, ship owners/operators, and cybersecurity professionals to improve the maritime sector's cybersecurity stance. Nevertheless, just 31% of maritime industry professionals feel that organisations share effectively on cybersecurity threats, risks, and incidents (DNV, 2023). This failure to share information effectively prevents proper industry standards and best practices from being developed. DNV stresses improved information exchange and cooperation between maritime organisations, encouraging openness in discussion and exchange of experiences and difficulties. Knowledge sharing will assist in developing industry standards and best practices to create a robust cybersecurity stance. DNV also stresses acquiring a more risk-conscious workforce and a cybersecurity-aware culture, with hands-on training programs to keep employees adequately aware of cybersecurity risks and best practices. Collaboration, sharing of information, and training are DNV's main recommendations for the maritime sector to step up its cybersecurity capabilities and meet challenges.

4.2. Future Trends

Finally, a summary of the topic of cybersecurity may touch on new developments in the field that may affect cybersecurity, such as the rise in automation (autonomous ships), future Internet requirements, and other issues relating to automation. This review of cybersecurity in the marine business aims to give a concise, straightforward, and educational synopsis of the main factors and concerns surrounding cybersecurity in the maritime sector.

5. RECOMMENDATIONS AND FUTURE WORK

5.1. Recommendations for Enhancing Cybersecurity Awareness

The paper outlines the recommendations to improve cybersecurity awareness in the maritime sector. It recommends having an exhaustive training program on different areas of cybersecurity, such as phishing emails, strong passwords, potential threats, and suspicious activities reporting. Training sessions should be conducted periodically for all crew members, and new hires should be trained during onboarding. Open communication about cybersecurity concerns, reporting potential vulnerabilities, and rewarding good practices are encouraged. Regular assessments of cybersecurity vulnerabilities and risks should be conducted, evaluating the effectiveness of existing security measures and implementing necessary changes. Strong access controls and user permissions should be in place, and shipboard systems must be updated and patched regularly. Secure communication practices must be prioritized, including utilizing encrypted channels and not sharing sensitive information on unsecured networks. Crew members must be trained on secure communication procedures and equipped with the necessary tools and resources. An overall incident response plan should be created that defines procedures for the detection, containment, mitigation, and recovery from cybersecurity incidents. Stakeholder collaboration and information exchange must be facilitated, such as ship operators, port authorities, and cybersecurity professionals. Timely channels for cybersecurity alerts, advisories, and industry news must be provided. Drills and exercises can be regularly carried out to evaluate the efficacy of cybersecurity controls and prepare the crew to respond to cybersecurity breaches. The maritime sector can strengthen its overall cybersecurity stance and reduce cyberattack threats by adopting these proposals.

6. CONCLUSION

As shipping becomes more dependent on digital technologies, the threat of cyberattacks against ships, ports, and related systems has substantially increased.

This study emphasizes the importance of human factors in cybersecurity risks within maritime. Although improved cybersecurity technologies offer imperative protection, these are frequently compromised by a deficiency of awareness, inadequate training, and human error. Cyber attacks like phishing, social engineering, GPS spoofing, and malware target the weakest link of the security chain—the seafarer. With the use of a mix of literature review, expert interviews, surveys, and simulation-based tests, the research recognises the prevalence of human-derived vulnerabilities and measures the positive effect of targeted training programs. Significantly, more than 60% of the surveyed seafarers received little or no cybersecurity training, highlighting the imperative for reformation in education. Simulation exercises witnessed a notable 40% threat response improvement in individuals who undertook targeted training, supporting the efficacy of proactive learning programs.

In order to overcome these challenges, the paper recommends the incorporation of enhanced cybersecurity awareness and training into current maritime training and certification programs. Real-time simulation, behavioural evaluation, and ongoing upskilling should be adopted as best practices. Additionally, businesses need to formulate effective cybersecurity policies, incident response frameworks, and access control measures to lower exposure to cyber threats. Collaboration and sharing of information among maritime stakeholders—shipowners, port authorities, regulators, and cybersecurity specialists—are also crucial. Without a culture of transparency and cooperation, the industry cannot collectively develop resilience. Future studies will need to investigate the consequences of rising automation, the application of artificial intelligence, and the development of cyber-physical systems on board ships.

In summary, the creation of a cybersecurity-aware maritime labour force is not just a matter of operational need but one of strategic importance. Managing human factor threats through education, policy, and cooperation will be instrumental to the future security of maritime operations in a more digital world.

Conflict of interest: The authors declare that there is no conflict of interest regarding the publication of this paper.

REFERENCES

Awan, M. & Al Ghamdi, M., 2019. Understanding the vulnerabilities in digital components of an integrated bridge system (IBS). Journal of Marine Science and Engineering, 7(10).

BBC News, 2021. Police warning after drug traffickers' cyber-attack. [online] Available at: https://www.bbc.co.uk/news/world-europe-24539417 [Accessed 11 Nov. 2021].

BIMCO, 2018. The guidelines on cyber security onboard ships. [online] Available at: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships [Accessed Sep. 2020].

BIMCO, Chamber of Shipping of America, Digital Containership Association, INTERCARGO, InterManager, INTERTANKO and others, 2020. [pages 34–38].

DNV Det Norske Veritas, 2023. Maritime cyber priority 2023. [online] Available at: https://www.dnv.com/cybersecurity/cyber-insights/maritime-cyberpriority-2023.html [Accessed 27 May 2024].

DNV. (2023, June 6). Maritime professionals warn of insufficient investment in cyber security as risks escalate in the era of connectivity. DNV. https://www.dnv.com/news/2023/maritime-professionals-warn-of-insufficient-investment-in-cyber-security-as-risks-escalate-in-the-era-of-connectivity-244153/

EC-Council, 2020. Certified Secure Computer User (CSCU). [online] Available at: https://www.eccouncil.org/programs/certified-secure-computer-user-cscu/ [Accessed Sep. 2020].

EMSA, 2009. How LRIT works. [online] Available at: http://www.emsa.europa.eu/lrit-main/lrit-home/how-it-works.html [Accessed Sep. 2020].

Enisa, 2011. Cyber security aspects in the maritime sector. [online] Available at: https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1 [Accessed Sep. 2020].

Enisa, 2016. Glossary: Phishing and spear phishing. [online] Available at: https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/phishing-spearphishing [Accessed Sep. 2020].

Enisa, 2017. Publications of the European Union Agency for Cybersecurity. [online] [Accessed Sep. 2020].

Greenberg, A., 2018. The untold story of NotPetya, the most devastating cyberattack in history. Wired. [online] Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Accessed 13 Sep. 2021].

IMO, 2000. Automatic Identification System (AIS). [online] Available at: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx [Accessed Sep. 2020].

IMO, 2002. Voyage Data Recorder (VDR). [online] Available at: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/VDR.aspx [Accessed Sep. 2020].

IMO, 2017. Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3). [online] Available at: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSCFAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf [Accessed Sep. 2020].

IMO GMDSS, 1992. Introduction and history of GMDSS. [online] Available at: http://www.imo.org/en/OurWork/Safety/RadioCommunicationsAndSearchAndRescue/Radiocommunications/Pages/Introduction-history.aspx [Accessed Sep. 2020].

IMO MSC, 2017. Resolution MSC.428(98) on Maritime Cyber Risk Management. [online] Available at: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf [Accessed Sep. 2020].

IMO SD, 1985. Navigation Charts. [online] Available at: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/Charts.aspx [Accessed Sep. 2020].

IOActive, 2016. Hacking into a Voyage Data Recorder (VDR). [online] Available at: https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr/ [Accessed Sep. 2020].

Kaspersky, 2016. Ship 'black boxes' vulnerability. [online] Available at: https://www.kaspersky.com/blog/ship-black-boxes-vulnerability/10957/ [Accessed Sep. 2020].

Kessler, G.C., Craiger, P. and 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), pp. 429–437.

Kevin Jones, K.T., 2018. Cybersecurity for maritime infrastructures. [online] Available at: https://www.c-mric.com/wpcontent/uploads/2018/06/Kevin_Cybersecurity2018.pdf [Accessed Sep. 2020].

LRIT, IMO, 1974. Long-Range Identification and Tracking (LRIT). [online] Available at: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/LRIT.aspx [Accessed Sep. 2020].

M., F., 2018. Foundations of GNSS spoofing detection and mitigation with distributed GNSS SDR receiver. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, 12(4).

NAVTEX, Hellenic Navy, 1986. Hellenic NAVTEX system. [online] Available at: https://www.hnhs.gr/en/2015-05-28-16-58-21/2015-05-28-16-59-41/navtex [Accessed Sep. 2020].

NIST, 2019. NIST IR 7298r3 Glossary of Key Information Security Terms. [online] Available at: https://doi.org/10.6028/NIST.IR.7298r3 [Accessed Sep. 2020].

Reports of Mass GPS Spoofing Attack in the Black Sea, 2024. Inside GNSS. [online] Available at: https://insidegnss.com/reports-of-mass-gps-spoofing-attack-in-the-black-sea-strengthen-calls-for-pnt-backup/ [Accessed 27 May 2024].

Svilicic, B., Bosnjak, D., Zec, D. and Skaramuca, D., (2019). Raising awareness on the cybersecurity of ECDIS. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, 13(1).

Tam, K. and Jones, K., (2019). MaCRA: A model-based framework for maritime cyber-risk assessment. WMU Journal of Maritime Affairs, 18, pp.129–145.

Wired, 2021. The Icefog APT: A tale of cloak and three daggers. [online] Available at: https://media.kaspersky.com/en/icefog-apt-threat.pdf [Accessed 11 Nov. 2021].