Cyber Security as An Emerging Non-Traditional Threat to Maritime Security

Shivam Kumar Pandey[1], Deeksha Kathayat[2]
[1,2]*PhD Research Scholars, Rashtriya Raksha University*

Abstract -Throughout the extensive chronicle of maritime operations, the shipping industry has encountered a congregation of physical hazards, inclusive of arm robbery, terrorism, cargo theft, piracy, cargo theft, drug smuggling, illicit trafficking, and harm or annihilation of consignment else the vessel. The maritime industry has encountered a novel challenge as form of a 'cyber safety threat'[1] as an effect of the growing reliance on digitalization and technology. Until recently, the maritime sector has not encountered significant challenges with regards to cyber security for ships and ports. However, with the increasing integration of ships and their systems with the internet, the sector is now facing heightened vulnerability to cyber threats. The global community possesses extensive expertise in the reduction and prevention of such offences. However, the main concern is the "will" whether it is political will or legislative will to embark on such challenging yet fruitful task that would make the maritime sector the ideal trade mode.

Key words: Maritime Cyber risk, Cyber worthiness, shipping sector, Policy Instruments

INTRODUCTION

The shipping industry has encountered a number of physical hazards during the course of the long history of marine operations, including terrorism, cargo theft, piracy, drug smuggling, illegal trafficking, armed robberies, and destruction and damage of the ship or its cargo. However, as digitalization and technology have been more widely used in the marine industry, a new, unseen concern known as a "cyber security threat" has emerged. Up until recently, cyber security was not a significant concern for ports, ships, or the maritime industry as a whole. However, as systems onboard ships are progressively connected to the internet, increasing their vulnerability to cyber-related dangers.

Attacks by cybercriminals may have an impact on ports, businesses, and even individual ships. Business leaders must comprehend the significance of managing cyber risks and be ready to handle various cyberthreats. The hazards posed by cyber-attacks and the significance of minimising them should be understood by other parties who are directly engaged. The usage of technology in the marine industry has increased digitalization, making it considerably simpler for cybercriminals to hack ships' OT and IT systems. The most probable and dangerous assault against ships is to interfere with their navigational systems.

Attackers have the ability to change data in the ECDIS[2] by hacking into a ship's AIS[3] or GPS[4] systems. Modification of any ship's AIS data is very risky and might have disastrous results. There are several ways for the attacker to compromise or alter data. The most important details in this text are the potential attacks that can be carried out on a vessel. These attacks include modifying data regarding the vessel's position, course, cargo, speed, name, impersonating seaport personnel's, communicating with one another ships, and shutting down ship to ship communications or to seaport[5] or to vessels itself.

Nonetheless, the perpetrator has the capability to infiltrate the maritime vessel's information technology infrastructure and employ ransomware to encrypt it, thereby enabling the perpetrator to attain complete authority over the vessel until the demanded ransom is remitted. Furthermore, human beings constitute a significant vulnerability in cybersecurity frameworks, given that errors committed by users can readily compromise confidential data or establish entry points for

[1] Sanz Espinar G, "Https://Riull.Ull.Es/Xmlui/Bitstream/Handle/915/30978/C_22_%282022%29_28.Pdf?sequence=1&isAllowed=y" [2022] Çédille 513 <http://dx.doi.org/10.25145/j.cedille.2022.22.29>

[2] Electronic Chart Display and Information System
[3] Automatic Identification System
[4] Global Positioning System
[5] https://www.duo.uio.no/bitstream/handle/10852/92245/510.pdf?isAllowed=y&sequence=1

malicious actors. Furthermore, it is possible for passengers to procure corrupted files on the network or insert malware thumb drives on the server CPU designated for organizational administration, thereby granting the perpetrator entry to susceptible stored information. Ultimately, the perpetrator has the ability to disrupt the functionality of loading management systems and cargo. Digital systems[6] are utilised by the crew on the vessel for the purposes of control, management and cargo loading.[7]

The interfacing of these networks with diverse onshore systems may render them more susceptible to cyber incidents, thereby increasing their accessibility and vulnerability. The server networking threats on the Port of Antwerp serves as an illustration of how malevolent actors can penetrate computer networks and exploit them to their fullest potential. The June 2017 cyber-attack on A.P. Moller-Maersk proved to be a triumph, as it impacted the company's transportation and logistics operations. It is imperative for corporations to possess cyber resilience capabilities in order to effectively address and rebound from cyber security breaches. In order to increase cognizance of the possible hazards associated with cyber-attacks, the global community initiated the development of regulations and directives aimed at instructing and advising ship and business proprietors on the implementation of cyber risk management. Nevertheless, it is worth considering whether the existing rules, regulations, and strategies are sufficiently effective and unambiguous to ensure comprehension among stakeholders, whether they offer a compelling motivation for shipowners to comply, and whether they are legally enforceable.

TYPES OF CYBER THREATS MARITIME INDUSTRY FACES

1. Malware: Violent malware that infects computer systems and prevents them from functioning normally. Malware can be used to shut down navigation systems or other crucial systems on board ships in the maritime sector, potentially causing accidents or other safety problems.
2. Phishing: Phishing is a sort of social engineering assault in which attackers try to convince victims to divulge private data, such as usernames and passwords. Phishing attacks can be used in the marine sector to obtain access to shipboard computer systems or port infrastructure.
3. Attacks known as denial of service (DoS) are attempts to prevent legitimate users from accessing computer systems by flooding them with traffic or requests. DoS assaults can be used to take down navigation systems or other vital systems on board ships in the maritime sector, which could result in accidents or other safety-related events.
4. Advanced Persistent Threats (APTs) are complex cyberattacks intended to infiltrate computer systems and go undiscovered for extended periods of time. APTs can be employed in the maritime sector to steal private data or obtain access to vital systems on board ships or at port facilities.

These are only a few instances of the various cyber dangers that the marine sector must deal with. In order to defend against these threats and maintain the safe and secure operation of ships and port infrastructure, it is crucial for organizations in the maritime sector to put into place robust cybersecurity measures.

INTERNATIONAL FRAMEWORK ADDRESSING MARITIME CYBER THREAT

- International Safety Management (ISM) Code[8]: Resolution A.741(18) saw the enforcement of the ISM Code[9] in 1993. The mandatory requirement was instituted upon the implementation of the 1994 amendments to the International Convention for the Safety of Life at Sea (SOLAS) on the first of July in 1998. The International Safety Management (ISM) Code acknowledges the inherent diversity among shipping companies and shipowners, as well as the varying operational contexts in which ships function. The statement acknowledges the fundamental importance of a strong safety management system (SMS) in ensuring optimal safety outcomes. It emphasises the need for a top-

[6] "Https://Inass.Org/Wp-Content/Uploads/2022/05/2022083131-2.Pdf" (2022) 15 International Journal of Intelligent Engineering and Systems <http://dx.doi.org/10.22266/ijies2022.0831.31>

[7] *Cyber-worthiness - duo.uio.no*. (n.d.). Retrieved April 25, 2023, from https://www.duo.uio.no/bitstream/handle/10852/92245/510.pdf?sequence=1

[8] International Management Code for the Safe Operation of Ships and for Pollution Prevention

[9] ibid

down approach to safety management, with senior leadership taking a proactive role in promoting a culture of safety. Additionally, it underscores the imperative for every organisation to establish, execute, and sustain an effective SMS. Notwithstanding, the ISM Code's security regulations do not incorporate any provisions pertaining to cyber-attacks.

In response to the absence of such provisions in the ISM Code, the International Maritime Organisation formulated Resolution MSC.428(98). This resolution mandates that shipowners and managers undertake an evaluation of cyber risk and execute appropriate measures throughout all aspects of their safety management system. The International Maritime Organisation (IMO) has reached a consensus that the integration of cyber risk management should be incorporated into the current management systems operating under the International Safety Management (ISM) Code and International Ship and Port Facility Security (ISPS) Code.

- IMO Resolution MSC 428(98)

Resolution MSC.428 (98) was adopted by the IMO[10] with the aim of increasing awareness of cyber vulnerabilities from threats, risk in order to promote secure and safe shipment. It mandates that each and every relevant partner engaged in maritime shipment organizations accelerate their efforts to protect shipping from existing and potential cyber risks and weaknesses. Additionally, it establishes a specific timeframe for flag states to guarantee that corporations have adequately addressed cyber risks. The Resolution mandates the implementation of cyber risk management protocols aboard ships, thereby motivating all maritime stakeholders to acknowledge the actuality of possible risk of cyber attackes as a significant risk to the maritme industry and necessitating their appropriate mitigation. IMO[11] has issued guidelines (MSC-FAL. 1/Circ.3) pertaining to the administration of network related cyber threats in the maritime industry. These guidelines offer a top-level recommendation for the effective solution to cyber risks in the maritime zone.

- Maritime Cyber Risk Management Guidelines by IMO (MSC-FAL.1/Cir.3)

The recommendations presented work as a guidance and therefore lack effective obligatory force. However, management of pertinent and possible threat is regarded as a crucial aspect for ensuring the secure and safe functioning of business operations in all organizations. The shipping industry's growing reliance on digitalization, network-based systems and automations, industrialization, has resulted in an escalating demand for cyber risk execution and management within the maritime sector. The Guidelines put forth five functional elements that facilitate efficient management of cyber risks:

1. risk Identification
2. Business asset protection
3. Threat detection
4. Quick response upon threat
5. Attack recovery

In a manner akin to the Resolution, the IMO Guidelines refrain from prescribing the specific means by which their high-level directions for maritime cyber threat administrations ought to be executed. Rather, they emphasise the significance of cyber risk management. Consequently, it proposes supplementary directives and criteria pertaining to the execution of computer networked threat management and alludes to:

1. Instructions for Cyber Security Onboard Ships (supported and produced by UIMI, OCIMF, BIMCO, ICS, CLIA, INTERTANKO, INTERCARGO)
2. IT Standards like ISO/IEC 27001.

- Board of Ships Guidelines relating to Cyber Security

In order to delve deeper into the concept of managing cyber risks in the maritime industry, it is imperative to examine the "Guidelines on Cyber Security on Board of Ships" which pertains to the cyber security concerns that arise on vessels. These guidelines were formulated by prominent leaders in the shipping sector, namely CLIA, BIMCO, INTERCARGO, ICS, INTERTANKO, UIMI and OCIMF. Although the instructions by no means legally binding, some are crucial as it were formulated by representatives from the industry and offer valuable perspectives by means of plans to address computerized threats. The Guidelines provide a comprehensive overview of the management of various types of cyber risks, detailing the rationale and methodology behind their effective mitigation. It furnish a comprehensive overview of the procedure for conducting a risk

[10] International Maritime Organisation

[11] ibid

assessment. The document provides a comprehensive definition of threat actors, various types of cyber threats, and prevalent cyber vulnerabilities. The significance of assessing the probability of the risk and its potential consequences on the enterprise is underscored in the context of cyber risk management. The Guidelines offer crucial information for entities engaged in maritime shipping operations, including shipping companies, on examples of performing a thorough threat evaluation to safeguard their corporations against computerized threats.[12] However, as previously stated, the instructions in the form of guidelines were issued by industry heads are non-binding. The aforementioned are a set of instructions and principles that serve as a suggestion and a definitive framework for executing effective cyber risk management.

DOMESTIC LEGAL FRAMEWORK IN INDIA

The main piece of law addressing cybersecurity, data protection, and online crimes is the Information Technology (IT) Act, 2000[13]. It attempts to secure electronic data, information, and records, recognizes and protects electronic transactions and communications under the law, and forbids the unauthorized or illegal use of computer systems. The Indian Penal Code of 1860 and the Companies (Management and Administration) Rules 2014 are two more statutes that include provisions pertaining to cybersecurity. Sector-specific regulations published by regulators and agencies require regulated firms to uphold cybersecurity requirements.

CONCLUSION

The escalation of cybercrime in the shipping industry necessitates that shipowners adhere to a range of measures recommended by the global society to integrate protocols relating to cyber risk management systems into their existing security and safety management procedures. This is imperative to prevent, transfer, or alleviate all cyber-related hazards. It is pertinent to emphasize the three fundamental principles of the conventional notion of a ship's seaworthiness, as articulated in the framework of the Marine Insurance Law relating to Carriage of Goods[14]. The aforementioned principles encompass the vessel's physical fitness for navigating the sea, a proficient and capable crew, adherence to international and national standards for documentation and certification, and the ship's capability to transport cargo safely. The aforementioned elements necessitate safety and scrutiny within the framework of the present state of expertise in the field. The carrier is obliged to undertake all essential measures to safeguard the vessel (along with its cargo) from the customary hazards of the sea that may be encountered during its journey. The primary focus should pertains to the responsibility of shipowners to proactively mitigate the risk of cyberattacks that may occur during a voyage.

The Hague-Visby Rules in its Article VI enables ship owners to restrict their liability. The optimal probability of achievement for the ship liner is within the exemption codified in Article IV (2)(q). The aforementioned clause is commonly referred to as a "catch-all" exemption, which necessitates the individual invoking the exemption to demonstrate the absence of fault on the part of the carrier or its personnel. To mitigate the risk of unseaworthiness in their vessels, carriers are advised to adhere to the management standards established by the international community for the maritime cyber risk, impart adequate education and training to their personnel regarding the prospective hazards of cyber-prone risks, and ensure that suggested documentation is available on the vessel. Provided that the carrier can establish that they have taken reasonable care, they may not be deemed accountable for a violation of their duty and can therefore absolve themselves of responsibility.

---

[12] *Cyber-worthiness - duo.uio.no*. (n.d.). Retrieved April 25, 2023, from https://www.duo.uio.no/bitstream/handle/10852/92245/510.pdf?sequence=1

[13] Kient, "A Comparison of Cybersecurity Regulations" (*Law.asia*, October 19, 2022) <https://law.asia/comparison-cybersecurity-regulations/>

[14] *Cyber-worthiness - duo.uio.no*. (n.d.). Retrieved April 25, 2023, from https://www.duo.uio.no/bitstream/handle/10852/92245/510.pdf?sequence=1