Page 471 - 478 **DOI:** *https://doij.org/10.10000/IJLSI.112636*

INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 7 | Issue 3

2025

An Analyses of Legal Framework Relating to Cyber Risk in Maritime Industry

DIVYA BHARATHI M[1] AND MUHAMMED AMEEN[2]

ABSTRACT

Information and communication technologies (ICT), artificial intelligence, blockchain technology, big data, the internet of things, and other so-called end-to-end digital technologies are actively used in all facets of life, including maritime transportation, which is one of the key features of the modern world. An appropriate legal framework that can ensure cybersecurity in maritime transport is currently a challenge for the practical implementation of information technologies and autonomous vessels in the maritime industry. The cybersecurity concerns of maritime vessels' marine transport infrastructure facilities receive minimal attention1. Due to a lack of international collaboration and a common approach to the conceptual framework of cybersecurity, there is currently no appropriate legal framework for governing this field. Cyberattacks on ships will inevitably become the rule rather than the exception as hackers' strategies get more sophisticated. This article presents a comprehensive analysis of cyber-security frameworks and a classification of cyberattacks in the maritime industry. It also aims to identify the most effective approaches to enhance the current cyber security protection.

Keywords: *maritime, cyber risks, international law, new law*

I. INTRODUCTION

For many parts of the world, maritime transportation is essential to their economic viability. An ever-growing dependence on the sector is fueled by factors such as the expansion of the world's population, improvements in living standards, investment, and the removal of trade barriers. Maritime transportation is the backbone of both internal and international trade in regions with navigable rivers or those are made up of a group of islands. Furthermore, the marine industry handles 90% of all products transportation in markets that prioritize eco-friendly operations, low costs, efficient operations, and sustainable development. The transition to increasingly digitalized maritime infrastructures has been made possible by recent advancements in the Internet of Things (IoT), Big Data, and Artificial Intelligence.

There is an urgent need to safeguard the integrity of next-generation maritime facilities.

[1] Author is an Assistant Professor at Vels Institute of Science Technology and Advanced Studies, Chennai, India.
[2] Author is an Assistant Professor at Vels Institute of Science Technology and Advanced Studies, Chennai, India.

 [ISSN 2581-9453]

Infrastructure security is adversely affected by connectivity via navigation systems including Radio Detection and Ranging (RADAR), Automatic Identification System (AIS), and Global Navigation Satellite System (GNSS). Additionally, shipping corporations have been the target of new and extremely complicated cyberattacks that harm on-vessel core equipment and target in-port information systems.

A thorough analysis of cyber-security frameworks and a classification of cyberattacks in the maritime sector are presented in this article and an attempt is made to find the best ways the best ways to improve the cyber security protection that is currently in place.

II. MARITIME AND CYBER RISK

Malicious cyber activity directed at the digital systems of ships, ports, or associated maritime infrastructure constitutes a cyber-attack on ships. These assaults have the ability to jeopardize lives and cargo, interfere with operations, and compromise private data. It includes, snooping on schedules, injecting malicious software, tampering with ECDIS systems, changing ship positions, tracking navigational charts, triggering system alerts, Phishing and Social Engineering, Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks, Unauthorized Access, Supply Chain Compromises etc,.

In general, ships are susceptible to two types of cyber threats:

i. Untargeted attacks, in which the systems and data of a business or a ship are among numerous possible targets

ii. Targeted attacks, in which the systems and data of a business or a ship are the primary target or one of several targets.

Attackers will probably employ online tools and methods to find, identify, and take advantage of common weaknesses that might also exist in a business or on a ship. A few examples of instruments and methods that could be applied in these situations include

- Malware. Malicious software is intended to gain access to or harm a computer without the owner's knowledge.
- Water holing. Creating a phony website or compromising an authentic one in order to take advantage of unwary visitors.
- Scanning. Randomly searching vast swaths of the internet for exploitable flaws.
- Typo squatting. Also known as bogus URLs or URL hijacking.
- Social engineering. Potential cybercriminals employ this non-technical tactic, typically

but not always through social media contact, to coerce insiders into violating security protocols.

- Brute force. An attack that attempts a large number of passwords in the hopes of making a correct guess in the end. The hacker methodically looks through every potential password until they find the right one.
- Credential stuffing. Attempting to gain illegal access to a system or application by using credentials that have already been hacked or particular, frequently used passwords.
- Denial of service (DoS) stops authorized and legitimate users from obtaining data, typically by overloading a network with information. To carry out a distributed denial of service (DDoS) attack, several computers and/or servers are taken over.
- Phishing. Requesting specific bits of private or sensitive information over email to a huge number of possible recipients. Additionally, the email can have a malicious attachment or ask the recipient to click on a hyperlink to a phony website.
- Spear-phishing. Similar to phishing, however personal emails are used to target people and frequently contain links that download hazardous software automatically. SAT-C messages have occasionally been used to create a feeling of familiarity with the email address of a malevolent sender..
- Subverting the supply chain. Attacking a business or ship by compromising the software, hardware, or auxiliary services that are provided to the business or ship.

The examples listed above are not all-inclusive. Other cyberattacks techniques are developing, such as posing as a real shore-based employee of a shipping company in order to gather important data that can be utilized in a subsequent attack. The only thing limiting the potential quantity and complexity of tools and procedures used in cyberattacks is the creativity of the companies and individuals creating them.

III. LEGAL FRAMEWORK AND REGULATIONS GOVERNING MARITIME CYBER SECURITY: INTERNATIONAL LAW AND CONVENTIONS

The international maritime legal framework basically consists of the following key agreements:

- Convention on the High Seas (1958). The high seas are defined as the region outside of a state's territorial sea and internal waterways under the 1958 Geneva Convention on the

High Seas. It declares that no state can claim control over the high seas, which are open to all nations. The convention specifies a number of high seas freedoms, including as flying over them, fishing, building pipelines and subsurface cables, and navigating. It also highlights how states must use these liberties while taking other states' interests into account. The convention also covers topics including illegal drug trafficking, maritime pollution, and broadcasting from the high seas without permission.

- Convention on the International Regulations for Preventing Collisions at Sea (1972). Uniform guidelines for preventing collisions at sea are established by the 1972 Convention on the International Regulations for Preventing Collisions at Sea, or COLREGS. It addresses topics including safe speed, collision risk, and how vessels should behave in certain situations. All ships operating on the high seas and adjacent waterways are subject to the rules.
- International Convention for the Safety of Life at Sea or SOLAS (1974; Consolidated edition with amendments, dated January 1, 2020). One important international maritime agreement that establishes minimum safety requirements for merchant ships is the International Convention for the Safety of Life at Sea (SOLAS). To guarantee the safety of ships and people at sea, it specifies specifications for structure, machinery, and operation. One of the most significant international tools for maritime safety is SOLAS.
- The 1979 International Convention on Maritime Search and Rescue (SAR Convention). An international framework for coordinated maritime search and rescue operations was established by the 1979 International Convention on Maritime Search and Rescue (SAR Convention). By establishing SAR areas and rescue coordination centers, including joint centers for maritime and aeronautical services, it seeks to guarantee uniform and efficient SAR processes globally.
- The United Nations Convention on the Law of the Sea (UNCLOS, 1982), also known as the Law of the Sea Treaty, is an international agreement that establishes a legal framework for all maritime and marine activities. It defines the rights and responsibilities of nations in using the world's oceans, establishing rules for all uses of the oceans and their resources. UNCLOS divides the oceans into five zones: internal waters, territorial sea, contiguous zone, exclusive economic zone (EEZ), and the high seas, each with different legal statuses.
- International Convention on SALVAGE (1989), provides a precise and foreseeable legal framework for paying salvors for their assistance in rescuing endangered vessels or other

property. It created a "special compensation" to reward salvors who may not have received a reward based just on the value of the salved property but who had prevented or reduced environmental harm, replacing the previous Brussels Convention. The convention also addresses the responsibilities and rights of ship-owners, salvors, and other salvage operation participants.

- International Ship and Port Facility Security Code or ISPS Code (2002). Adopted in 2002, the ISPS Code is a collection of global maritime security guidelines intended to improve ship and port facility security. It is a component of the International Convention for the Safety of Life at Sea (SOLAS) and became required in 2004. In order to identify and discourage security issues, the ISPS Code seeks to create a framework for collaboration between governments and the maritime sector.

Since there was essentially no introduction of ICT in all areas of human life at the time these agreements were developed and adopted, there was no need to take into account the need to ensure cybersecurity at sea and its regulation. As a result, the norms of these conventions only interpret the general requirements for ensuring maritime security and have nothing to say about ensuring cybersecurity at sea.

The necessity of creating a unique international treaty and legal framework to deter crimes and cyberattacks on maritime transportation and guarantee its cybersecurity is confirmed by the reality of cybercrime and the threat it poses. The goal of the current international agreements on cybercrime, including the Arab Convention, the Budapest Convention on Cybercrime of 2001, and the Draft Convention on International Information Security of 2011, is to address the broader issues of fighting cybercrime. To ensure the safety of maritime navigation, the proposed special international treaty should therefore include provisions for both establishing and monitoring compliance with unified minimum standards and requirements for cyber systems as well as for prosecuting those responsible (perpetrators) for attacks on computer systems or computer information.

IV. CHALLENGES AND WAYS FOR DEVELOPING INTERNATIONAL LAW FOR MARITIME CYBERSECURITY

A new International shipping legislation will serve as the broad framework for the development of the new maritime cybersecurity rule. National legislation and industry standards for execution are intertwined with international law, especially IMO legal instruments. As a result, cooperation between various actors—including between the government and the industry—is required. The IMO has always been dominated by western nations with significant marine

industries. It is crucial that emerging nations actively participate in any future cybersecurity legislation. The world's technological and geopolitical landscape is evolving. This also applies to the maritime industry. Some of the top developing nations may now innovate, use maritime technologies, and have a significant impact.

The IMO's legislative procedure is increasingly more convoluted and contentious. However, it is mostly impacted by a few prominent maritime countries and significant industry participants. Given the technical complexity, the involvement of nonstate players, such as the pertinent industries, is also necessary for the regulatory reform to succeed in the future. Future international legislation for marine cybersecurity must take this shifting techno-geopolitical and economic environment into account. In addition to the internal intricacies of the IMO, maritime cybersecurity may entail collaborative efforts with other global institutions like the United Nations Office on Drugs and Crime, the World Telecommunication Union, and the WCO. Future IMO developments should also be in line with ongoing UN negotiations to create a new worldwide legal framework for cybercrimes.

Despite the disparities and divides among participants, a cooperative approach to an efficient legislative framework for maritime cybersecurity is feasible. All parties involved in a more secure maritime transportation system—the backbone of the world economy—stand to gain from it, making this feasible. Additionally, maritime cybersecurity takes into account some more general aspects of international law as well as a number of IMO requirements, such as safety, security, and the ease of maritime trade. While an IMO code on maritime cybersecurity would be useful, various IMO legal instruments need to be changed in order to guarantee clarity, consistent application, and deterrent punishment through the member states' national administrative and judicial systems.

V. CONCLUSION AND SUGGESTIONS

Maritime safety has been and continues to be a major concern. Modern issues, cyberattacks, and threats to cybersecurity in maritime transportation related to the advancement and application of ICTs necessitate the progressive codification of international legal norms and the development of international law in order to combat cybercrime and guarantee cybersecurity in maritime transportation. To guarantee cybersecurity in maritime transportation, states should focus their efforts on developing unique standards and establishing a global, regional, and universal method. To protect cyberspace from the threats that come with the growth of information technologies and their application in the maritime sector, special management is required.

Promoting a cybersecurity culture across all sectors, especially the maritime sector, is crucial. Recognizing cybersecurity as an essential component of both domestic and global security is an issue of principle. The development of a comprehensive international legislative framework for collaboration in the areas of cybersecurity and cybercrime may be based on the Russian initiative to approve the UN Convention on Cooperation in Combating Information Crime. In order to effectively provide cybersecurity at sea, the international community must work together to create a single conceptual framework that includes a universal definition of cybersecurity and further codification of the term, as well as international standards that specify the types and indicators of cybercrime at sea.

Due to the absence of a common standard for safeguarding cyberspace in general and a united approach to the idea of cybersecurity, the majority of states are currently ill-prepared to recover from significant cyberattacks in the maritime sector. States, international organizations, and the private sector must, however, agree on the necessity of regulating their activities in cyberspace and adopt a suitable international treaty that will act as a model for the adoption of national regulations in this area if these detrimental factors are to be eliminated. Adopting such a treaty might resolve disputes and create a common conceptual foundation for cybersecurity as a whole.

There is no particular law for maritime cyber threats or maritime security in India, where maritime law has developed gradually. Even though there aren't any cyberattacks in India, regulations can be made to address marine cyber threats in the future by adopting conventions like the SUA Convention, SOLAS Convention, and ISM Code, as well as guidelines like BIMCO. Additionally, the Admiralty Act of 2017 could be amended to allow claims for damages resulting from cyberattacks, which include both monetary loss and fatalities.

*****

 [ISSN 2581-9453]

VI. BIBLIOGRAPHY

A. PRIMARY SOURCES

1. UNCLOS,1982
2. Suppression of Unlawful Acts against the Safety of Maritime Navigation,1988 and 2005
3. International Convention for the Safety of Life at Sea (Solas),1974 IV. International Safety Management Code (ISM) 1993.

B. SECONDARY SOURCES

1. Cyber security in marine transport: opportunities and legal challenges by Naser Abdel Raheem Al Ali, Anna A. Chebotareva, Vladimir E. Chebotarev
2. Defending the Cyber Sea: Legal Challenges Ahead-VA Greiman
3. Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat? - Md Saiful Karim
4. Maritime Hacking: The International and Criminal Law Framework - Belma Bulut, Aref Fakhry

*****