TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 18
Number 4
December 2024
DOI: 10.12716/1001.18.04.02

Cybersecurity in Maritime Industry

T. Neumann
Gdynia Maritime University, Gdynia, Poland

ABSTRACT: The maritime industry is increasingly adopting digital solutions to optimize operations, reduce costs, improve data processing speeds, promote sustainability, and enhance safety. Advances in information technology, particularly through satellite internet connections, have enabled seamless communication between IT and operational systems. However, these developments also introduce significant cybersecurity risks. To mitigate these challenges, international regulations, such as the IMO's Maritime Cyber Risk Management Resolution (2021), and guidelines have been implemented, emphasizing the integration of cybersecurity into Safety Management Systems (SMS). Effective cybersecurity management requires a top-down approach, beginning with executive leadership and fostering a culture of cybersecurity throughout organizations. Frameworks like those developed by the U.S. National Institute of Standards and Technology (NIST) complement IMO guidelines by providing tools to assess and manage cyber risks, especially in offshore operations experiencing rapid technological advancements. The offshore sector, vital to renewable energy and maritime economy growth, faces unique risks due to its dependency on interconnected systems. Comprehensive measures are necessary to safeguard navigation, protect infrastructure, and ensure personnel safety while adhering to evolving regulatory and technological standards. This paper highlights the need for robust cybersecurity frameworks to secure maritime operations against emerging threats, including data breaches, system manipulation, and cyberattacks, which pose challenges to global trade and maritime safety.

1 INTRODUCTION

Shipping is increasingly reliant on digital solutions, which have become essential for carrying out daily tasks. The rapid development of information technology, data processing and transmission speeds, as well as the growing volume of data, provides shipowners and other stakeholders in the maritime industry with enhanced opportunities for operational optimization, cost reduction, faster information processing, sustainable business practices, and improved safety. These changes are largely driven by improvements in communication channels, often through satellite internet connections, between servers, information technology (IT) systems, and operational technologies (OT). However, these advancements also increase potential vulnerabilities to threats and the risk of cyberattacks.

To address these challenges, international guidelines have been developed to define cyber threats, identify potentially unsafe behaviors, and outline how to manage cyber risks in the maritime sector. It is important to note that the process of managing cyber risk will depend on the specific characteristics of each organization. In addition to adhering to international requirements, companies

must also consider relevant national regulations and the laws of the flag state.

On January 1, 2021, the International Maritime Organization (IMO) Maritime Safety Committee (MSC) Resolution 428(98) on Maritime Cyber Risk Management came into force. The resolution states that the approved Safety Management System (SMS) should include cyber risk management in accordance with the objectives and functional requirements of the International Safety Management (ISM) Code [15].

In the same year, the IMO developed guidelines containing recommendations for maritime transport on managing cyber risks to protect shipping from current and emerging threats, as well as vulnerabilities in cybersecurity. As highlighted in the IMO guidelines, effective cyber risk management should begin at the executive management level. Subsequently, the ship's management should foster a culture of cybersecurity across all levels and departments of the organization and ensure a holistic and flexible cyber risk management system that operates continuously and is regularly assessed and verified through control mechanisms [5].

A notable organization that provides a professional approach to cybersecurity is the U.S. National Institute of Standards and Technology (NIST). It assists companies in adopting a comprehensive approach to risk assessment, helping them understand effective methods for managing potential cyber threats, both internal and external. The framework creates a "profile" that can help identify and prioritize actions to reduce cyber risks. This profile can also be used as a tool to align policy, business, and technological decisions in the context of risk management.

Figure 1. Cybersecurity framework. [26]

Sample framework profiles are publicly available for shipping, maritime operations, and passenger vessels. These profiles were developed by the U.S. Coast Guard and NIST's Cybersecurity Division. NIST frameworks can be used in conjunction with IMO guidelines to help the industry assess, prioritize, and mitigate cyber threats [26]. They can be particularly useful for the offshore sector, which has experienced significant growth in IT technology dynamics and information exchange over the years.

2 OFFSHORE ENVIRONMENT

Shipping is becoming increasingly dependent on digital solutions, which are essential for performing daily functions. The rapid development of information technologies, the speed of data processing and transmission, as well as the growing volume of data, provide seafarers and other stakeholders in the maritime industry with enhanced opportunities for improving efficiency, reducing costs, shortening data processing times, fostering sustainable business practices, and enhancing safety.

These advancements largely rely on improving the quality of communication channels, often through satellite internet connections, between servers, information technology (IT) systems, and operational technologies (OT). However, this also increases potential vulnerabilities and the risk of cyberattacks.

To address these challenges, international standards have been established to define cyber threats, identify potentially unsafe behaviours, and outline methods for managing cyber risks in the maritime sector. It is important to remember that the process of risk management in the context of cybersecurity depends on the specifics of each project. In addition to international requirements, relevant national and public regulations must also be taken into account.

On January 1, 2021, the International Maritime Organization's (IMO) Maritime Safety Committee (MSC) Resolution 428(98) on Maritime Cyber Risk Management came into force. The document states that an approved Safety Management System (SMS) should include cyber risk management in accordance with the objectives and functional requirements of the International Safety Management (ISM) Code [15]. In the same year, the IMO developed standards containing recommendations for maritime transport and cyber risk management to protect ships from current and emerging cyber threats and vulnerabilities.

As highlighted in the IMO guidelines, effective cyber risk management must begin at the management level. Subsequently, ship management must implement a cybersecurity culture across all levels and departments of the organization and ensure a comprehensive and flexible cyber risk management system that operates continuously and is regularly assessed and verified through control mechanisms [5].

Another noteworthy organization that takes a professional approach to cybersecurity is the United States National Institute of Standards and Technology (NIST). It helps companies adopt a comprehensive approach to risk assessment by enabling them to understand the most effective methods for managing both internal and external cyber threats. The framework creates a "profile" that can identify and prioritize actions aimed at mitigating cyber threats. This profile can also be used as a tool to align policy, business, and technological decisions within the context of risk management. Template forms are publicly available for maritime transportation, offshore operations, and passenger vessels. These programs were developed by the United States Coast

Guard in collaboration with NIST's cybersecurity division. NIST profiles can be used alongside IMO guidelines to assist the industry in assessing, prioritizing, and mitigating cyber threats. They can be particularly useful for regions that have experienced significant advancements in information technology and data exchange dynamics over the years [26].

2.1 *Specifics of the offshore environment*

The offshore industry is one of the fastest-growing sectors of the maritime economy. It contributes to the creation of thousands of jobs for highly skilled specialists. According to estimates, wind energy contractors may require approximately 100,000 people over the next 20 years [26].

The scope of interests in the broadly understood coastal region is vast. Vessels are often constructed or modified specifically to perform a particular task. The term "offshore" can itself be defined as a range of activities and operations that take place both on land and at sea. It encompasses both fixed and mobile structures used for exploration, extraction, protection, processing, and exploitation of resources or facilities.

The dynamics of development bring numerous benefits to the regions themselves, including financial ones. Therefore, most countries with the opportunity to develop this maritime economy will likely seek to invest in it. A good example is Poland, which is driving discussions and analyses on the construction of offshore wind farms "from the ground up." Initiating such policies involves a broad economic perspective. Production, transportation, installation, port modernization, and the handling of the final product represent an opportunity for regional growth and a tangible chance to make a mark and establish a position in the market.

The development of offshore wind farms in Poland may be the best solution for reducing greenhouse gas emissions and meeting the strict requirements of the European Union. A promising step toward achieving this goal is moving away from traditional fossil fuels and exploring alternative, zero-emission sources of electricity. The discussions remain heated, and there is a possibility that Poland will establish its own dedicated institution for this purpose. Approved on February 2, 2021, Poland's Energy Policy until 2040 (PEP2040) outlines the development of renewable energy sources, including wind energy, as one of the key directions for change. According to the plan, wind energy capacity is expected to reach 5.9 GW by the end of 2030 and 11 GW by 2040 [29].

2.2 *The importance of safety of navigation and personnel involved in the construction, operation and decommissioning of offshore projects*

The dynamically developing coastal sector currently places significant emphasis on the broadly understood concept of safety. Every action, from planning to implementation, highlights the fundamental importance of safety for boats, the environment, and the people involved at all stages, from construction through operation to decommissioning. Safety is a crucial element impacting the durability of projects and the protection of the marine environment.

The well-developed maritime infrastructure, one of the industry's strengths, requires careful protection to reduce the risk of maritime accidents and safeguard the personnel working in this environment. The utilization of conventional energy sector practices can be beneficial from an operational safety perspective, such as ensuring efficiency during normal operating conditions and in emergency situations.

While the high initial investment costs increase the need for safety investments, they also require specific strategies to avoid negatively impacting the profitability of projects. The permitting process, though complex, is the foundation of a safe and legally compliant business.

The concept of "maritime security" is defined on multiple levels and is used in legal, technical, organizational, and operational documents and publications to safeguard conditions at sea, including both ships and individuals, as well as to emphasize the importance of the maritime environment. The Strategic Concept of Maritime Security of the Republic of Poland defines "maritime security" as activities aimed at preventing or mitigating threats and challenges that are subject to subjective assessment and arise from human activities at sea. These threats may stem from technical, procedural, and personal deficiencies, which are further exacerbated by hydrometeorological conditions. Meanwhile, the term "maritime security" encompasses both maritime safety and national security at sea, defining a state of the world's waters where international and domestic laws are effectively enforced, freedom of navigation is ensured, and citizens, infrastructure, transport, the environment, and maritime resources are protected [18].

According to the works of J. Urbański, Z. Kopacz, and W. Morgaś, which represent a non-military approach to this issue, the term "maritime safety" should be understood as the proper and appropriate conditions for human activity at sea, which do not threaten life and property and do not harm the marine environment. Maritime safety encompasses the safety of life, security, and property against environmental and operational threats, as well as the protection of the marine environment from pollution caused by human activities at sea. Figure 2 illustrates the levels of maritime safety [8].

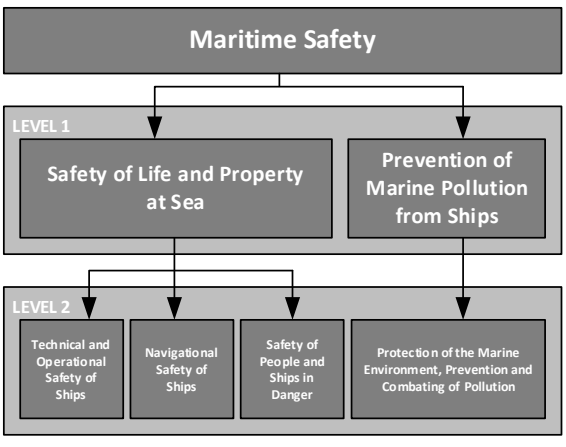

Figure 2. Maritime Safety. [8]

As shown in the figure above, maritime safety is defined as the state of conditions at sea in which the risk to health, life, property, and the marine environment is maintained at an acceptable level. The graphic depicts two levels of retention. The first step concerns the safety of life and property at sea and the prevention of pollution from the marine environment aboard ships. The second area of safety encompasses human activities at sea, which involve a higher level of abstraction [18].

2.3 *Cybersecurity in Maritime Law*

The concept of maritime safety is highly complex and appears in many legal acts governing today's work in the maritime sector. Unfortunately, this concept and the broadly understood principles associated with it were not always obvious. Until 1914, there was no international treaty establishing safety regulations. It was then that the SOLAS Convention was adopted, serving as a kind of response to the RMS Titanic disaster (which sank on the night of April 14–15, 1912). This was the first codification defining the framework for broadly understood safety in maritime operations. [17]

The increase in passenger and crew safety threats, which intensified in the 1980s, compelled the IMO to take decisive steps to legally address new forms of threats to the maritime sector. Incidents involving threats, intimidation, and the killing of passengers and crew members had to be codified, described, and defined to effectively combat them. The brutal necessity of such actions was highlighted by the events on the m/s Achille Lauro in November 1985. Acts of terrorism became a real problem and a significant threat to the maritime sector. IMO decided to adopt directive A 584(14) [11] regarding measures to prevent unlawful acts threatening the security of ships as well as the safety of their passengers and crew. In September 1986, the MSC issued circular MSC/Circ.443, addressing measures to prevent unlawful actions against passengers and crews onboard ships [12].

2.4 *International Ship and Port Facility Security (ISPS) Code*

On July 1, 2004, a new maritime safety system was adopted under the SOLAS Convention, namely Chapter XI-2 on special measures to enhance maritime security, which covers ships and port facilities. The International Ship and Port Facility Security (ISPS) Code was introduced. It recognized the need and necessity of protecting international maritime cargo against the threat of terrorism. The IMO responded swiftly and decisively, promoting new requirements that result in cooperation among agencies, government bodies, local administrations, and the shipping and port industries [16].

2.5 *International Safety Management Code (ISM)*

In accordance with IMO Resolution A 741(18) from 1993, the International Safety Management Code (ISM Code) was adopted. Its purpose was to introduce a safe system for the management and operation of ships. This is a universal document that outlines general principles and objectives, identifying all hazards to both the ship and its crew, as well as the specific scope of activities for a particular shipowner. Based on this, specific targeted actions are determined to establish appropriate precautionary measures [14].

3 MARITIME CYBER THREATS

3.1 *The concept of cyber threat*

Cybersecurity threats include remote and unauthorized manipulation of telecommunication systems aimed at disrupting operations, gaining control, or intercepting data related to government services, public institutions, as well as merchants and individual users [1, 6, 23, 24].

Each country has its own services dedicated to protecting critical (relevant) infrastructure, conducts research in this field, and expands its protective capabilities in response to growing threats and technological advancements. Critical infrastructure is defined as buildings, structures, machinery, and services responsible for their functions, as well as computer systems essential to the security and well-being of the state and its efficient operation. The term "critical state infrastructure" includes energy systems, telecommunications, postal services, information systems, financial and banking services, water management, food and water supply, healthcare, transportation; services related to security and public order; ensuring the proper functioning of state structures and public administration during crises (including crisis management centers and command posts); and the protection of relevant critical industrial sectors, including defense.

Critical infrastructure has both public and private dimensions. So-called electronic attacks can be carried out by states with their own intelligence services and armed forces, but transnational entities are increasingly becoming significant aggressors. While these offensive and defensive actions align with the concept of traditional information strategy, they serve different purposes. However, cyberattacks are always deliberate and carefully planned actions.

Managing cybersecurity, particularly in terms of securing information and the systems that process it, has become one of the fundamental challenges of our times. Complex IT systems process massive amounts of data, making them attractive targets for criminals—ranging from intellectual criminals and amateur hackers to organized crime groups manipulated and trained by the military and police forces of various countries.

To effectively protect IT systems and the information they handle, several factors must be addressed, including identifying all the infrastructure requiring protection and determining the threats that an organization must prioritize defending against. Performing these basic duties presents significant practical challenges. These challenges pertain to the volume of hardware and IT systems, their complexity,

and the amount of data processed and operations to be conducted on them.

Thus, it is essential to organize information about these aspects, identify any gaps, and set work priorities. This approach eliminates the occasionally prevalent strategy of "everyone against everyone," which is not only economically unfeasible but also impossible to achieve.

3.2 *Cyberattacks at sea*

In times of increased digital dominance, the maritime sector finds itself in crisis. As dependency on technology grows, so does the risk of cyberattacks, creating unprecedented challenges for global trade. In recent years, the impact of digitization has been unparalleled: the replacement of legacy systems with smart devices and the connection of nearly everything to the Internet, from massive data centers to personal wearable devices. Energy infrastructure is also undergoing these changes, becoming increasingly interconnected. The use of smart devices, such as intelligent electronic devices (IEDs), IoT-enabled systems, and cyber-physical systems, along with the widespread adoption of Industry 4.0, has resulted in efficient resource utilization, reduced intervention, and increased convenience [27].

Marine assets such as ships, containers, port infrastructure, offshore wind farms, and drilling platforms can be connected to sensors and the Internet to collect and monitor data in real time. The Internet of Things (IoT) enables remote asset tracking, predictive maintenance, and improved operational efficiency. Cyber-physical systems (CPS) facilitate real-time remote command and control over on-site systems and equipment. Autonomous ships and smart port facilities, such as automated quay cranes, automated guided vehicles (AGVs) for moving vessels, and automated gate systems for efficient cargo clearance using technologies like machine learning, computer vision, and advanced navigation systems, allow for reduced human intervention and enhanced outcomes, resulting in increased profits [7, 33].

The maritime economy is changing rapidly. The number of embedded and interconnected systems, as well as those accessible and operable from land, is growing quickly. The term "marine" refers to ships, hulls, extraction structures, other floating objects, infrastructure, and everything that connects and integrates all of these elements into a business. Many organizations are currently migrating to the cloud for convenience [20]. For example, the shipping company "UASC" migrated to a secure system management solution via cloud computing. The "classic" way of organizing bunkering was cost-effective; therefore, "UASC" representatives took it a step further and partnered with "Shiptech" to create a secure cloud-based platform. Migration to the new "UASC" system enables better tracking of commodity prices from suppliers for communication, monitoring ship operations, and enhancing the defensive strategy for the entire fleet [25].

Maritime cyber risk refers to the extent to which a technological unit is exposed or vulnerable to a potential circumstance or event that results in operational failures, security or safety breaches related to navigation due to damage, loss of data, or systems. [13]

3.3 *The concept of maritime cyber threat*

The rapid digitization and automation of devices and systems on ships, in ports, and in remote equipment make maritime transport enterprises increasingly vulnerable to threats such as data theft, modification, or destruction. Maritime revenues have always played a key role in the economies of many countries. Today, in the era of globalization, it has become a crucial element of the supply chain, handling approximately 80% of global trade. As a driving force of the global economy, it requires constant protection against threats such as piracy, natural disasters, and cyberattacks. The latter emerged relatively recently and is primarily driven by the rapid digitization and automation of nearly all machines and systems used on ships, in ports, and by companies. Similar changes have already occurred in other sectors, such as finance and telecommunications, where the importance of cybersecurity was recognized many years ago, leading to the initial implementation of both recommendations and regulations [22].

3.4 *Types of cyber threats at sea*

The information received on the map is processed by the software and displayed in graphic and textual form on ECDIS, radar, and ARPA for navigational, collision-avoidance, and rescue purposes. Information from the terrestrial AIS system is used for monitoring and managing the ship market through vessel traffic management systems (VTMS) and online AIS providers. In the current situation, AIS has several weaknesses that need to be addressed before the introduction of autonomous ships.

The operating system can be attacked through the network used for updating electronic files or via USB memory for the same purpose. The consequences of such an attack are the same as for a personal computer, i.e., operating system failure, encryption and deletion of data, placement of malicious scripts, and the spread of malware within the connected network. As a result, ECDIS becomes unusable, and other instruments are infected. In such a scenario, a second ship should be equipped with ECDIS as a backup or with a chart for the intended voyage. Another form of attack involves GPS signal disruption or falsification of the ECDIS location. The issue can be easily detected when the system loses the entered position data and switches to dead reckoning mode. The GPS spoofing scenario is significantly worse. ECDIS plots a false location on the electronic chart from the GPS receiver, which is harder for the operator to detect and take appropriate action [3, 31].

The ship's position on the ECDIS screen has been shifted, and other parameters have been modified to make the officer on the bridge appear normal. The onboard AIS device provides the ship and information to protect coastal stations, nearby ships, and aircraft, receives information from other

transponders, tracks and monitors ship movements, and displays information transmitted by AtoN. The system uses two narrowband radio frequency (RF) channels in the maritime VHF band for communication [19]. The primary goal of communication is utility, which is free of charge. Inmarsat also offers paid communication services. Communication based on geostationary satellites in polar waters is limited due to the low elevation of satellites above the horizon.

Disruptions in communication prevent the ship's crew from accessing information essential for effective and safe navigation. They also make it impossible for the crew to control their vessel when attackers compromise navigation, control, and propulsion systems. To mitigate short-range communication issues when they are most critical, IALA has proposed the introduction of the VHF Data Exchange System (VDES).

3.5 *Types of threats to devices operating on the Internet*

3.5.1 *Most common cyberattacks*

The most common cyberattacks at sea include various methods and techniques that exploit the unique characteristics of the maritime environment and the technology used on ships and in ports. These attacks can lead to significant disruptions to the operations of vessels and port infrastructure, posing a threat to maritime safety. DDoS (Distributed Denial of Service) attacks are frequently used to disrupt IT systems in ports and on ships by overloading servers and communication networks. A Man-in-the-Middle (MitM) attack involves a hacker positioning themselves between two communicating parties, intercepting and potentially modifying the data being exchanged. This is particularly dangerous in maritime communication and navigation systems [21].

A popular method of attack is phishing, which targets maritime personnel to obtain login credentials or other confidential information through fake addresses or websites that appear credible. ARP spoofing (Address Resolution Protocol) enables hackers to intercept traffic within a ship's local network.

Figure 3. Pictogram of ARP spoofing

3.5.2 *Cross-site scripting (XSS)*

An attack involving the injection of malicious scripts into other benign and trusted websites. These scripts run in end users' browsers, potentially leading to the theft of cookies, session tokens, or other sensitive information, which can result in identity theft [2].

Figure 4. Pictogram of Cross-site scripting

3.5.3 *Botnet: infected computers*

Botnet – refers to a network of private computers infected with malicious software and controlled by a group without the owners' knowledge. Botnets can be used for distributed denial-of-service (DDoS) attacks, data theft, or sending spam [30].

Figure 5. Pictogram of Botnet

3.5.4 *Phishing*

Phishing – this type of attack involves tricking people into providing confidential information, such as personal data, banking details, credit card information, and passwords. It is usually carried out through fake emails or websites [10].

Phishing is the most common form of cybersecurity incident. These attacks can be divided into two categories: the first is called social engineering, and the second relies on malware. On social media, attackers attempt to cause harm through emails that appear harmless at first glance or through fake websites. On the other hand, malware-based attacks use malicious software installed on the victim's computer. Such threats are common in email-based scams. Typically, the email contains a hyperlink to a fake website where the user, either out of carelessness or ignorance, enters personal data such as usernames and passwords to access an account. This often happens when individuals are distracted and fail to pay attention to the content of the email or hyperlink due to a busy schedule.

Figure 6. Pictogram of Phishing

3.5.5 *Boneypot*

Boneypots are typically security devices that, in an attack scenario, can be considered decoys configured to detect, distract, or study attempts to gain unauthorized access to IT systems [37].

Figure 7. Pictogram of Boneypot

3.5.6 *Brute force*

Brute force – a method of attack that involves systematically trying all possible passwords or passphrases until the correct one is found. This method of attack is fairly simple but can be very effective depending on the complexity of the password [28].

Figure 8. Pictogram of Brute force

3.5.7 *Sniffing*

Sniffing involves intercepting and recording traffic passing through a digital network or a part of it. Attackers can capture sensitive information, such as passwords and authentication data [32].

Figure 9. Pictogram of Sniffing

3.5.8 *Null session attack*

Null session attack— the attacker exploits a vulnerability in the NetBIOS session service to gain access to an unauthorized system, potentially accessing sensitive data without a valid username and password [75].

Figure 10. Pictogram of Null session attack

3.5.9 *Attack DDoS (Distributed Denial of Service)*

DDoS (Distributed Denial of Service) – this attack aims to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of internet traffic [34].

Figure 11. Pictogram of Distributed Denial of Service

3.5.10 *Attack DNS (Domain Name System)*

DNS Attack (Domain Name System) – vulnerabilities in the DNS system are exploited to redirect traffic from legitimate servers to fake ones, often with the aim of stealing data or delivering malicious software [75].

Figure 12. Pictogram of Domain Name System

3.5.11 *Attack Man in the Middle*

A Man-in-the-Middle (MitM) attack occurs when attackers secretly relay and potentially alter messages between two parties who believe they are directly communicating with each other. "Man in the Middle" (MITM/MIM) is a type of malware that exploits weaknesses in the SSL/TLS protocol in response to communication between two network users, which is rarely accessible [4].

Figure 13. Pictogram of Man-in-the-Middle

3.5.12 *Attack ARP (Address Resolution Protocol)*

ARP spoofing – this is a type of attack in which the attacker sends false ARP messages to the local network. This results in associating the attacker's MAC address with the IP address of a legitimate computer or server in the network [35].

Figure 14. Pictogram of ARP Spoofing

3.5.13 *Attack SQL*

SQL Injection – inserting malicious SQL statements into an input field to execute them (e.g., to dump the contents of a database for the attacker) [36].

Figure 15. Pictogram of SQL Injection

3.5.14 *Spyware attack*

Spyware attack - spyware is software that allows a user to obtain confidential information about the operation of someone else's computer by secretly transmitting data from the hard drive [9].

Figure 16. Pictogram of Spyware attack

4 CONCLUSIONS

Briefly, the development of digital technologies in the maritime sector brings numerous benefits but requires the simultaneous advancement of strategies and tools to counter cyber threats. Implementing IMO

guidelines, collaborating with institutions such as NIST, and promoting a culture of security are key to ensuring the protection of infrastructure and operations in the maritime environment.

REFERENCES

1. Afenyo, M., Caesar, L.D.: Maritime cybersecurity threats: Gaps and directions for future research. Ocean & Coastal Management. 236, 106493 (2023). https://doi.org/10.1016/j.ocecoaman.2023.106493.
2. Alanda, A. et al.: Cross-Site Scripting (XSS) Vulnerabilities in Modern Web Applications. In: 2024 11th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI). pp. 270–276 (2024). https://doi.org/10.1109/EECSI63442.2024.10776461.
3. Androjna, A. et al.: Assessing Cyber Challenges of Maritime Navigation. Journal of Marine Science and Engineering. 8, 10, 776 (2020). https://doi.org/10.3390/jmse8100776.
4. Benton, K., Bross, T.: Timing Analysis of SSL/TLS Man in the Middle Attacks. CoRR. abs/1308.3559, (2013).
5. Bimco: The Guidelines on Cyber Security Onboard Ships, https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/guidelines-on-cyber-security-onboard-ships-v4.ashx?rev=e86ee4330cce44d7b90ad718e8af3c2e, last accessed 2024/12/03.
6. Cichocki, R.: State-Sponsored and Organized Crime Threats to Maritime Transportation Systems in the Context of the Attack on Ukraine. TransNav Int. J. Mar. Navig. Saf. Sea Transp. 17, 3, 717–721 (2023). https://doi.org/10.12716/1001.17.03.24.
7. De Alwis, N., Nam, H.-S.: A way towards port automation: challenges and implications. WMU Journal of Maritime Affairs. (2024). https://doi.org/10.1007/s13437-024-00350-9.
8. Dyrcz, C.: Bezpieczeństwo morskie a nawigacja. Nautologia. 158, 1–10 (2021).
9. Forte, D.: Spyware: more than a costly annoyance. Network Security. 2005, 12, 8–10 (2005). https://doi.org/10.1016/S1353-4858(05)70312-3.
10. Gupta, B.B. et al.: Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommun Syst. 67, 2, 247–267 (2018). https://doi.org/10.1007/s11235-017-0334-z.
11. IMO: Directive A 584(14) Measures to prevent unlawful acts which threaten the safety of ships and the security of their passengers and crew, https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20A.584(14).pdf, last accessed 2024/12/03.
12. IMO: MSC/Circ.443 Measures to prevent unlawful acts against passengers and crews on board ships, https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC.Circ.443.pdf, last accessed 2024/12/03.
13. IMO: MSC-FAL.1/Circ.3/Rev.2 Guidelines on maritime cyber risk management, https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf, last accessed 2024/12/03.
14. IMO: Resolution A 741(18) International management code for the safe operation of ships and for pollution prevention (International Safety Management (ISM) code). (2017).
15. IMO: Resolution MSC 428(98). Maritime Cyber Risk Management in Safety Management Systems. (2017).
16. IMO: SOLAS XI-2 and the ISPS Code, https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx, last accessed 2024/12/03.
17. Johansen, K., Gudmestad, O.T.: Revisiting Unsinkable Ships: From Titanic to Helge Ingstad, the Long-Standing Issues and Persistent Risks of Ship Disasters. TransNav Int. J. Mar. Navig. Saf. Sea Transp. 18, 1, 95–106 (2024). https://doi.org/10.12716/1001.18.01.08.
18. Kopacz, Z. et al.: Formalne i nieformalne oceny bezpieczeństwa morskiego. Zeszyty Naukowe Akademii Marynarki Wojennej. R. 46 nr 3 (162), 51–67 (2005).
19. Koshevyy, V., Shishkin, A.: Developments of Interface for VHF, MF/HF Communication Using DSC in GMDSS Services in the Framework of E-navigation Concept. TransNav Int. J. Mar. Navig. Saf. Sea Transp. 15, 3, 593–600 (2021). https://doi.org/10.12716/1001.15.03.12.
20. Lind, M. et al. eds: Maritime Informatics. Springer International Publishing, Cham (2021). https://doi.org/10.1007/978-3-030-50892-0.
21. Linh Vu et al.: A Cyber-HIL for Investigating Control Systems in Ship Cyber Physical Systems Under Communication Issues and Cyber Attacks. IEEE Transactions on Industry Applications. 60, 2, 2142–2152 (2024). https://doi.org/10.1109/TIA.2023.3311429.
22. Martínez, F. et al.: Maritime cybersecurity: protecting digital seas. Int. J. Inf. Secur. 23, 2, 1429–1457 (2024). https://doi.org/10.1007/s10207-023-00800-0.
23. Melnyk, O. et al.: Review of Ship Information Security Risks and Safety of Maritime Transportation Issues. TransNav Int. J. Mar. Navig. Saf. Sea Transp. 16, 4, 717–722 (2022). https://doi.org/10.12716/1001.16.04.13.
24. Mohsendokht, M. et al.: Decoding dependencies among the risk factors influencing maritime cybersecurity: Lessons learned from historical incidents in the past two decades. Ocean Engineering. 312, 119078 (2024). https://doi.org/10.1016/j.oceaneng.2024.119078.
25. Mraković, I., Vojinović, R.: Maritime Cyber Security Analysis – How to Reduce Threats? Transactions on Maritime Science. 8, 1, 132–139 (2019). https://doi.org/10.7225/toms.v08.n01.013.
26. NIST: Releases Version 1.1 of its Popular Cybersecurity Framework, https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework, last accessed 2024/12/03.
27. Onishchenko, O. et al.: Ensuring Cyber Resilience of Ship Information Systems. TransNav Int. J. Mar. Navig. Saf. Sea Transp. 16, 1, 43–50 (2022). https://doi.org/10.12716/1001.16.01.04.
28. Paar, C., Pelzl, J.: Understanding Cryptography: A Textbook for Students and Practitioners. Springer, Berlin, Heidelberg (2010). https://doi.org/10.1007/978-3-642-04101-3.
29. Polish Government: Poland's energy policy until 2040, https://www.gov.pl/web/klimat/polityka-energetyczna-polski, last accessed 2024/12/03.
30. Schiller, C.A. et al.: Chapter 2 - Botnets Overview. In: Schiller, C.A. et al. (eds.) Botnets. pp. 29–75 Syngress, Burlington (2007). https://doi.org/10.1016/B978-159749135-8/50004-4.
31. Spravil, J. et al.: Detecting Maritime GPS Spoofing Attacks Based on NMEA Sentence Integrity Monitoring. Journal of Marine Science and Engineering. 11, 5, 928 (2023). https://doi.org/10.3390/jmse11050928.
32. Trabelsi, Z. et al.: Malicious sniffing systems detection platform. In: 2004 International Symposium on Applications and the Internet. Proceedings. pp. 201–207 (2004). https://doi.org/10.1109/SAINT.2004.1266117.
33. Yang, Y. et al.: Internet of things for smart ports: Technologies and challenges. IEEE Instrumentation & Measurement Magazine. 21, 1, 34–43 (2018). https://doi.org/10.1109/MIM.2018.8278808.
34. Zeb, K. et al.: DDoS attacks and countermeasures in cyberspace. In: 2015 2nd World Symposium on Web

Applications and Networking (WSWAN). pp. 1–6 (2015). https://doi.org/10.1109/WSWAN.2015.7210322.
35. Zhao, Y. et al.: ARP Spoofing Analysis and Prevention. In: 2020 5th International Conference on Smart Grid and Electrical Automation (ICSGEA). pp. 572–575 (2020). https://doi.org/10.1109/ICSGEA51094.2020.00130.
36. Zhuo, Z. et al.: Long short-term memory on abstract syntax tree for SQL injection detection. IET Software. 15, 2, 188–197 (2021). https://doi.org/10.1049/sfw2.12018.
37. Zobal, L. et al.: Current State of Honeypots and Deception Strategies in Cybersecurity. In: 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT). pp. 1–9 (2019). https://doi.org/10.1109/ICUMT48472.2019.8970921.