TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 19
Number 3
September 2025
DOI: 10.12716/1001.19.03.03

Cybersecurity in Maritime Transport Systems: Threats, Trends, and Countermeasures in the Last Decade

R. Cichocki & P. Wójcik
Gdynia Maritime University, Gdynia, Poland

ABSTRACT: The increasing digitization and automation of maritime transport systems have introduced significant cybersecurity challenges across both vessel-based and port-based infrastructures. This paper provides a comprehensive overview of the current cyber threat landscape affecting the maritime domain, examining key vulnerabilities in modern maritime systems, including navigation, communication, and cargo handling technologies. It outlines recent trends such as the emergence of autonomous shipping and evaluates their implications for cybersecurity. A detailed classification of cyber threats—ranking from ransomware and phishing to advanced persistent threats and denial-of-service attacks—is presented alongside real-world case studies that illustrate the technical complexity and operational impact of cyber incidents. Furthermore, the paper analyzes the main risk factors contributing to cyber vulnerabilities in the maritime sector. Building on this, it explores state-of-the-art strategies and technologies aimed at mitigating these threats, including intrusion detection systems, blockchain applications, cybersecurity training protocols, and international regulatory efforts. The study concludes with key recommendations for strengthening cyber resilience in maritime operations, emphasizing a proactive and multilayered approach to securing this critical global infrastructure.

1 INTRODUCTION

The maritime transport sector is undergoing a profound transformation driven by the accelerated integration of digital technologies. From automated navigation systems aboard vessels to interconnected logistics platforms within ports, information and communication technologies (ICT) have become essential to ensuring operational efficiency, safety, and global connectivity. However, this digital shift has also exposed maritime infrastructure to a growing spectrum of cybersecurity threats. Unlike traditional risks, cyber threats are dynamic, asymmetrical, and often transnational, making them particularly challenging to detect, mitigate, and manage. As maritime systems become increasingly automated and data-driven, through the adoption of technologies such as the Automatic Identification System (AIS), Electronic Chart Display and Information System (ECDIS), and Supervisory Control and Data Acquisition (SCADA), the industry must simultaneously address the vulnerabilities that accompany this evolution. This chapter introduces the digital architecture of contemporary maritime systems and provides the foundational context for understanding the critical cybersecurity challenges that arise from their interconnected nature.

This paper presents a comprehensive analysis of cybersecurity in maritime transport, focusing on both shipborne and shore-based systems. It begins by characterizing the digital landscape of modern maritime infrastructure and identifying the technologies most susceptible to cyber threats. The

study then outlines current and emerging threat vectors, including ransomware, phishing, GPS spoofing, and advanced persistent threats, supported by real-world case studies from recent years. A critical examination of sector-specific risk factors follows, highlighting technical, human, and organizational vulnerabilities. The final sections are dedicated to exploring effective mitigation strategies, such as the implementation of intrusion detection systems, the use of blockchain for data integrity, and enhanced crew training protocols. By integrating technical insights with operational case studies, the article provides a practical and forward-looking perspective on strengthening cyber resilience in the maritime domain.

2 CHARACTERISTICS OF MARITIME TRANSPORT SYSTEMS

Modern maritime shipping uses many digital systems to support navigation, operations management, and communication, among other things. Electronic devices are present at every level of the maritime transport sector. Among the most important, commonly used systems are:

- Global Navigation Satellite Systems (GNSS) – satellite systems such as GPS, GLONASS, Galileo, or Compass. They enable precise determination of the ship's position and constitute the basis of modern navigation.
- Automatic Identification System (AIS) – a system enabling the exchange of navigation data, including the position, course and speed of a vessel. Its main task is the automatic exchange of information in order to avoid collisions and identify vessels.
- Automatic Radar Plotting Aid (ARPA) – a computer that automatically plots radar. It allows for simultaneous tracking of multiple objects and calculation of their basic parameters.
- Vessel Traffic Service (VTS) – a vessel traffic control system. It consists of a control center and observation and communication systems. It uses radars, ARPA systems and optionally vision cameras, and also processes information received from the AIS system.
- Electronic Chart Display and Information System (ECDIS) – electronic marine charts integrated with navigation data, supporting route planning and collision avoidance.
- Supervisory Control And Data Acquisition (SCADA) – IT systems supervising the course of technological or production processes. In the maritime sector, they are used both on ships and in ports, among others, to support the management of infrastructure, transshipment processes and power supply systems.
- Internet of Things (IoT) – a set of networked sensors that allow monitoring the technical condition of the ship, its equipment, cargo, as well as parameters such as weather conditions or fuel consumption.

2.1 *Trends in modern maritime transport systems*

Taking into account the latest trends, it should be assumed that the number of cyber systems in the described sector will gradually increase. The concept of autonomous or partially autonomous shipping is showing growing popularity. The practical implementation of this idea on a global scale will require the development and standardization of AI systems capable of full management and control of the ship.

The digital development of the maritime sector also applies to the land part. The idea of smart ports leads to the greatest possible automation of port processes, such as ship traffic management, cargo logistics and infrastructure maintenance. The existing solutions use modern methods of data transfer, big data analysis and AI support.

The trend developed along with the above concepts is the integration of individual systems in the maritime sector. The connection of ship and land systems into uniform digital ecosystems, enabling the exchange of data in real time between individual units, ports and shipowners, as well as enabling the automation of processes at an unprecedented level, will result in significant optimization of costs and times of task execution, as well as potentially improving the safety of navigation and port work.

However, the increasing digitization also brings with it threats. Every electronic system can be susceptible to errors, cyberattacks or problems resulting from insufficient training of the crew. The next chapter will analyze cyber threats related to the maritime sector. [1]

3 CURRENT CYBER THREATS IN THE MARITIME SECTOR

As mentioned earlier, any cyber system can be vulnerable to threats resulting from both intentional actions as well as unintentional human errors or hardware malfunctions. However, special attention in the general classification of digital threats is paid to cyber attacks. Below, we will present descriptions of individual types of malicious activities, as well as examples of attacks on maritime infrastructure from recent years. [2, 3, 4, 5]

3.1 *Cyber threat classification*

The types of attacks differ depending on the purpose, method and mode of action. The most common threats in the described sector are:

- Ransomware – one of the most popular types of cyberattacks. According to the 2023 Cyber Trends And Insights In The Marine Environment released in 2024 by Coast Guard Cyber Command, the number of incidents of this type increased by 80% between 2022 and 2023 and was one of the most common threats with the rate of 42% of all incidents. However, in the last year, the number of ransomware attacks has significantly decreased, although it still remains at a fairly high level. According to this year's edition of the aforementioned report, summarizing 2024, incidents of this type accounted for about 25% of registered incidents.
  A ransomware attack involves encrypting critical data or entire systems in order to force the victim to pay a ransom to unlock them. The maritime industry is particularly vulnerable to attempted

attacks of this type, due to the very high costs of delaying individual operations. [6,7,8,9]

- Phishing/Spoofing – the most common type of network threat globally, and one of the most serious problems in the maritime transport systems sector. Phishing involves an attempt to extort sensitive data using psychological manipulation in the form of fake emails, text messages or websites that clone the appearance of well-known services. Spoofing is a technique of falsifying one's identity by hiding or replacing a real email address, phone number or IP address. It is often used together with phishing to gain the victim's trust and increase the chance of stealing sensitive data. Attacks of this type are usually not targeted – they are directed to the widest possible group of recipients, some of whom will succumb, and some of the victims may provide the attacker with actually valuable data. Phishing can rely on both psychological methods and malware installed on victims' computers. [10,11]
- Disturbed Denial of Service (DDoS) – an attack that disrupts the operation of a selected system by artificially generating an unusually large amount of traffic on the server. A common example is the rapid flooding of the server with subsequent queries, which consequently causes the system to be overloaded. In the case of the maritime sector, this attack can disrupt communication, coordination of maritime traffic or port operations. [12]
- Domain Name System Attack – a type of attack that changes DNS settings so that it redirects known network addresses to servers chosen by the attacker – most often containing cloned versions of a given website, used to intercept sensitive data. [13]
- Man in the Middle (MitM) – this threat involves an attacker intercepting communication between two parties. This allows for information to be obtained and individual messages to be modified. Such an attack can be used to steal sensitive data, fraud, or further attacks of various kinds. [14,15]
- SQL Injection – this is an attack carried out on databases, consisting of injecting a malicious code fragment into an SQL query, allowing access to sensitive data or performing another type of attack. [16]
- Brute force – the most primitive type of attack, consisting of making successive attempts to crack a password by testing every possible combination of characters. This method is improved by checking the most popular passwords first. The level of threat depends on the quality of the passwords and the existence of accompanying security measures. Despite the simplicity of the attack, according to the report prepared by the Coast Guard Cyber Command in 2025, almost 47% of password cracking attempts made by Cyber Protection Team was successful. [7,17]
- Spyware – a threat in the form of software that allows the monitoring of user activity and potentially obtaining sensitive data. [18,19]

Additionally, the maritime industry is exposed to any combination of the above threats, aimed at disrupting supply chains, manipulating navigation data (for example, through GPS signal spoofing or AIS data falsification), or taking over control systems (for example, through attacks on SCADA systems or other Operational Technologies (OT)). [20,21]

3.2 *Examples of cyber threats incidents*

The most common types of digital threats are listed above. The individual incidents from the last few years are listed below, to point out the real scale and nature of the problem. The aftermath of the attacks includes financial loss, supply chain disruptions, safety threats and trust loss.

3.2.1 *Ransomware*

As mentioned earlier, the number of ransomware attacks is growing every year. The industry journals describe many incidents of this type. Of these, three cases that occurred no earlier than 2023 have been selected to provide a good example of the scale of the threat:

- Attack on Det Norse Varitas (January 2023) – DNV is the world's largest classification society and maritime software provider. On January 7, 2023, the company was hit by a ransomware attack. The exact target of the attack was the ShipManager software, used to manage fleet operations such as maintenance planning, logistics, and regulatory compliance. The attackers gained undisclosed access to the IT servers running the software, encrypted the data, and demanded a ransom. According to DNV, the incident was limited to the ShipManager servers, with no impact on the company's other services. Despite this, the attack affected 70 of the company's customers, affecting around 1,000 ships, which at the time represented 15% of the fleet served by the software. During the attack, all network functions of the system were down, leaving users with only limited offline functionality. No financial losses were made public, but the ShipManager server environment had to be rebuilt , an investigation had to be undertaken, and control and preventive measures had to be taken to protect customers. [22,23,24,25]
- Attack on Marinette Marine Shipyard (April 2023) – On April 12, 2023, the Fincantieri Marinette Marine shipyard, located in Wisconsin, USA was attacked. It is a key contractor for ships for the US Navy. Due to its military connections, the technical details of the attack have not been disclosed, but some sources indicate the work of a professional hacking group. The attackers managed to encrypt data on servers operating Computer Numerical Control machines (CNC) controlling production processes in the shipyard. The action was carried out in the early morning hours, which was probably intended to maximize the consequences of the production standstill. Ultimately, it managed to paralyze production processes for several days, delaying, among others, the construction of Constellation-class frigates and Freedom-class LCS ships. However, exact data on the number of delayed projects has not been made public. November 6, 2023 Fincantieri Marine Group confirmed that as a result attack leaked private data of 16,769 people. They included names and Social Security numbers. The company provided victims with two years of free credit monitoring services. [26,27]
- Nagoya Port Attack (July 2023) - Nagoya has the largest port in Japan, handling operations worth about $125 billion annually, or 10% of the country's trade. On July 4, 2023, it was hit by a ransomware attack that targeted the Nagoya Port Unified

Terminal System (NUTS). The system manages container loading and unloading operations. The attack began at 6:30 AM local time, halting the NUTS system. At the same time, a printer at the port printed a ransom message. The Japanese press suggested that the attack was carried out by the LockBit 3.0 group, known for attacks on critical infrastructure. It has not been confirmed how the hackers gained access to the system, but the most likely scenarios include phishing or a security hole. Ultimately, all transshipment operations at container terminals were suspended for almost 3 days. The precise amount of losses has never been published, but taking into consideration, the annually worth of handling operations it could exceed hundreds millions dollars. [28,29,30,31]

3.2.2 *Phishing / Spoofing*

As mentioned earlier, phishing is still one of the most common cyber threats, also in the maritime transport sector. In this industry, spoofing is an additional high risk, most often used to disrupt navigation processes by spoofing the GPS signal. Despite the scale of the phenomenon, it is difficult to obtain detailed information on specific attacks, because they often involve confidential data of individual companies. However, general information is often published in the industry press. Below, we will present selected incidents related to phishing and spoofing:

– spoofing attack on container ship MSC Antonia (May 2025) – On May 10, 2025, the over-300-meter-long container ship MSC Antonia, en route from the port of Marsa Bashayer in Sudan to the port of Jeddah in Saudi Arabia, went off course and ran aground near its destination. Analysis later in the day revealed that the incident was caused by GPS spoofing. According to Captain Steve Bomgardner, Vice President of Shipping and Offshore at Pole Star Global, the ship's AIS system was misled by false GPS signals. This led to the crew misrepresenting their positioning data and ultimately causing the vessel to go off course and run ground. Initial findings by Windward also suggested a GPS spoofing attack as the cause of the incident. The day before the incident, UK Maritime Trade Operations (UKMTO) reported multiple incidents of GPS signal disruptions in the Red Sea. The incidents involved multiple vessels and were recorded over several hours. As of May 23, 2025, the MSC Antonia ship was still grounded. [32,33,34,35]

Figure 1. Grounded MSC Antonia, Source: [32]

Figure 2. Satellite view of grounded MSC Antonia, Source: Pole Star Global

– SideWinder phishing attacks (2024) – In 2024, the SideWinder Group, most likely an Indian espionage group, intensified its activities. Over the past year, it has been carrying out targeted phishing attacks targeting the logistics and maritime transport sector in Africa and Asia. The attacks most often opposed of sending themed emails aimed at provoking the recipient to click on an infected document. It contained an exploit that used the Microsoft Office CVE-2017-1182 vulnerability known since 2017, which involves incorrect management of objects in memory. The SideWinder Group used this vulnerability to install the StealerBot toolkit, an advanced spyware. According to Kaspersky employees, SideWinder mainly attacked targets in Egypt, Djibouti, the United Arab Emirates, Bangladesh, Cambodia, and Vietnam in 2024. The group in question is most likely to rely on known vulnerabilities, old exploits , and easy-to-detect attacks, but experts say that a deeper analysis of the activities suggests that SideWinder may pose a more serious threat than it first appears. [36,37,38,39]

3.2.3 *Man in the Middle*

MitM incidents in the maritime sector are relatively poorly documented. This is due to the fact that such activities are usually just one stage of a larger attack, and the technical details are confidential data of individual companies. MitM is usually combined with phishing and spoofing attacks described in the previous points. An example of this is the attacks mentioned in the previous point, especially the actions of the SideWinder group. Successful use of the exploit mentioned earlier allowed for remote actions to be taken on infected computers, which in turn also made it possible to disrupt communication and carry out a typical man in the middle scenario. The StealerBot tool used later also enabled a wide range of hostile actions, including actions related to MitM. . [36,37,38,39]

Another example is the massive spoofing attacks carried out in the Crimea region on AIS systems. In previous years, there were reports of disruptions of the described system in the Black Sea basin, but in May 2023, such incidents escalated rapidly and took on specific characteristics. From May 14 to 21, 2023, many merchant ships operating near the southern coast of Ukraine experienced signal disruptions, redirecting their position in the AIS system to the area of Crimea occupied by Russia. The simulated locations of the ships were clearly arranged in the shape of the letter "Z", associated with Russian forces, which clearly

indicates deliberate and organized action by Russian services. [40,41,42]

Similar attacks took place on June 4, 2024, when the positions of almost 50 ships indicated their location at Simferopol Airport, and another 30 at Gelendzhik Airport, near the city of Novorossiysk. In addition to the positions, other AIS data, including speed, was also falsified. The attack targeted vessels of various types and sizes. There is no doubt that it was an element of the Russian-Ukrainian war, but the scale of the incident exceeds all previous actions of this type. [43]

Figure 3. Spoofing at Simferopol International Airport. Source: [43]

3.2.4 *DDoS*

DDoS attacks are most often used as a form of political protest or simple sabotage. As a result, they are not as dangerous as the other cases described. However, in maritime transport, they can disrupt the operation of key services, including communication systems, which can lead to significant delays or significant threats. Selected incidents from previous years include:

- Attack on Dutch ports (June 2023) – On June 6, 2023, the websites of Dutch ports were subject to a DDoS attack by a hacker group known as NoName057(16). The attack was allegedly motivated by the Dutch support for Ukraine during the ongoing war. As a result, the website of the port of Amsterdam remained unavailable for an hour, while Groningen Seaports experienced problems for the next two days. [44,45,46]
- Nagoya Port Attack (September 2022) – On September 6, 2022, the Nagoya Port website experienced a DDoS attack by Russian hacker group Killnet . The website remained unavailable for approximately 40 minutes. Along with the port website, other Japanese websites were also attacked. Killnet subsequently released a video on Telegram declaring that the attacks were a declaration of war against the Japanese government. [29,47,48]

DDoS attacks in Europe over the past year. In Spain alone, 72 incidents were recorded, occurring in March 2025 alone. The attacks mainly targeted key government services, although not exclusively. The previously described NoName057(16) group claimed responsibility for most of the incidents. The attacks are motivated by reasons related to actions supporting Ukraine in the political conflict that has been ongoing since February 2022. An increase in similar incidents is also being recorded in countries such as France and Italy. NoName057(16) has previously attacked port infrastructure, so there is a significant risk that similar incidents may occur this time too. [49,50]

3.2.5 *Brute force*

Brute technique force is the most primitive form of cyber-attack. Therefore, there are no single "major incidents" directly related to it and maritime transport. However, over the past years, it is possible to distinguish wide-scale actions, simultaneously targeting many sectors, including logistics companies.

An example of the mass use of the brute force technique may be the actions of Russian military intelligence. According to the American Cybersecurity Agency, the 85th Main Special Forces Center, part of the GRU, has been using military unit 26165 (also known online as APT28, Fancy Bear, Forest Blizzard or BlueDelta) to conduct intelligence operations based on cyberattacks since at least 2022. The main targets in the period described remain technology and logistics companies. The described group carried out mass attempts to guess the access data of attacked targets. To make it difficult to track, the attackers used VPN and the Tor network. Brute force was one of many forms of attack, including phishing, malware and the use of known vulnerabilities and exploits. Similar actions also took place before 2022. [51,52]

3.2.6 *Spyware*

Attacks using spyware have already been described in previous chapters. They are most often used in intelligence activities conducted by individual states. Direct examples are the previously described activities of Unit 26165 or the software installed by the SideWinder group on seized computers.

3.2.7 *The remaining types of attacks*

In recent years, the trade press has not reported any major attacks based solely on SQL injection or DNS attacks in the maritime sector, or they have not been made public. However, this does not mean that the threat does not exist. According to the European Cyber Report 2025 in 2024, SQL injection attacks accounted for 23%, while DNS-related incidents were included in the protocol point, accounting for 57% of attacks. [49]

3.3 *Risk factors*

The maritime transport sector faces several unique cybersecurity risk factors that distinguish it from other industries. These arise due to a combination of technological, organizational, and regulatory conditions that increase exposure to cyber threats.

Legacy systems and infrastructure - many vessels and port facilities continue to rely on outdated control systems and software, which are rarely updated or patched. These legacy systems are incompatible with modern cybersecurity tools, making them particularly susceptible to known exploits.

Low cybersecurity awareness among personnel - unlike other critical sectors, seafarers and port operators often lack specialized cybersecurity training. This human factor is significant—misconfigurations, weak passwords, or clicking on phishing links can introduce serious vulnerabilities. That situation is clearly visible throughout US Coas Guard Cyber Trends And Insights In The Marine Environment reports. In 2022 [53] 50% of CPT (Cyber Protection

Teams) mission gained initial access through Phishing campaigns and 59% success rate when Brute Force Cracking Password obtained in CPT missions. In 2023 [6] 66% phishing campaign was successful, 60,1% success rate in brute force cracking and 94,4% organizations has used default credentials. In 2024 [7] 53% successful credential harvesting through phishing campaigns and 46,9% success rate brute force cracking. All of those information clearly show that cybersecurity awareness in maritime organizations needs to be improved.

Increased system integration and remote access - As described in earlier sections, digital integration between ship and port systems is a growing trend. However, these connected infrastructures increase the attack surface, especially when remote access is granted for operational convenience or technical support without strong authentication protocols.

Limited onboard IT support - ships usually operate with minimal IT personnel, making real-time response to cyber incidents difficult. This creates a delay in detection, containment, and remediation of attacks.

Regulatory and standardization gaps - while several organizations (e.g., IMO, BIMCO, IACS) offer cybersecurity guidelines, they are often non-binding or outdated compared to the pace of cyber threat evolution. The absence of consistent enforcement results in varied levels of cybersecurity maturity across the industry.

4 STRATEGIES AND TECHNOLOGIES FOR COUNTERING THREATS

Mitigating cyber threats in maritime transport systems requires an integrated approach that combines technical solutions, personnel readiness, and regulatory compliance. Intrusion Detection and Prevention Systems (IDPS) are essential for real-time monitoring of vessel and port networks, detecting anomalies and enabling swift responses, particularly in SCADA and industrial control environments. Blockchain technology enhances data integrity in logistics and cargo handling by creating tamper-resistant, decentralized records of operational events. Addressing the human factor remains critical; regular, role-specific cybersecurity training and simulated threat scenarios improve awareness and response capability across crews and port staff. Artificial intelligence and machine learning contribute significantly to early threat detection by analyzing network behaviors and identifying irregularities, such as AIS spoofing or GPS manipulation. Regulatory frameworks like the IMO Guidelines and ISO/IEC 27001 ensure structured risk management and foster a consistent cybersecurity culture throughout the sector. Finally, network segmentation, strong access controls, encryption, and least-privilege policies serve to limit the spread and impact of potential intrusions, forming a vital foundation for resilient maritime cyber defense.

5 CONCLUSIONS AND RECOMMENDATIONS

The growing digitization of maritime transport systems has introduced substantial cybersecurity challenges, affecting both seaborne and port-based infrastructure. As demonstrated by numerous recent incidents, the maritime industry is increasingly vulnerable to cyberattacks ranging from ransomware and GPS spoofing to advanced persistent threats and coordinated denial-of-service campaigns. The complexity and interdependence of modern maritime systems, including navigation, logistics, and communication platforms, have expanded the sector's attack surface considerably. One of the most important conclusions is that cybersecurity in this domain is no longer a peripheral concern—it is now a core component of operational safety and business continuity. Many vulnerabilities stem not only from technical weaknesses but also from organizational gaps, such as outdated infrastructure, insufficient cyber awareness, or lack of standardized response procedures. The case studies presented in this paper highlight how even brief disruptions can result in cascading effects across supply chains, leading to significant financial losses and reputational damage. It is clear that as maritime operations become more integrated and data-driven, cybersecurity must evolve in parallel as a strategic priority.

To address these challenges, a proactive and multilayered approach to cybersecurity is necessary. Maritime stakeholders should invest in up-to-date technological safeguards while simultaneously cultivating a culture of cyber vigilance across all organizational levels. Regulatory frameworks must be implemented comprehensively and consistently, ensuring that risk management protocols are embedded in safety systems rather than treated as standalone policies. Industry-wide cooperation, including information sharing on emerging threats and response strategies, is essential to counter transnational risks effectively. Furthermore, targeted investments in crew training, system redundancy, and real-time threat detection capabilities can significantly improve resilience. Ultimately, cybersecurity must be regarded not merely as a compliance issue but as a dynamic and continuous process integral to the future of safe and efficient maritime operations.

ACKNOWLEDGEMENTS

This study was funded by the Gdynia Maritime University, under the research project: WN/2025/PZ/07.

REFERENCES

[1] Symes, S., Blanco-Davis, E., Graham, T., Wang, J., & Shaw, E. (2024). Cyberattacks on the Maritime Sector: A Literature Review. Journal of Marine Science and Application, 23(4), 689–706. https://doi.org/10.1007/s11804-024-00443-0

[2] Weintrit, A., Neumann, T. (2013). Marine navigation and safety of sea transportation: Maritime transport & shipping, 1-320, 978-131588312-0, CRC Press

[3] Weintrit, A., Neumann, T. (2013). Marine Navigation and Safety of Sea Transportation: Advances in Marine Navigation, 1-313, 978-131588301-4, CRC Press

[4] Weintrit, A., Neumann, T. (2015). Safety of marine transport introduction in: Safety of Marine Transport: Marine Navigation and Safety of Sea Transportation, 1-4, 978-131567261-8, CRC Press

[5] Neumann, T. (2024). Cybersecurity in Maritime Industry. TransNav, International Journal on Marine Navigation and Safety Od Sea Transportation, 18(4), 765–774. https://doi.org/10.12716/1001.18.04.02
[6] Cyber Trends and Insights in the Marine Environment 2023. (2024). U.S. Coast Guard Cyber Command. https://www.uscg.mil/Portals/0/Images/cyber/CTIME_2023_FINAL.pdf
[7] Cyber Trends and Insights on the Marine Environment 2024. (2025). U.S. Coast Guard Cyber Command. https://www.uscg.mil/Portals/0/Images/cyber/CGCYBER%202024%20CTIME.pdf?ver=AgbTrQoh4Fs91HUmdhd_xA%3d%3d&timestamp=1747657640065
[8] Jaffe, J., & Floridi, L. (2024). Ransomware: Why It's Growing and How to Curb Its Growth. Applied Cybersecurity & Internet Governance, 3(2), 38–64. https://doi.org/10.60097/ACIG/192959
[9] Sindiramutty, S. R., Cen, T. Y., Raslan, M. A. H. bin M., Subramaniam, M. R., Xin, L. Y., Kin, S. J., Long, M. S., & Sindiramutty, S. R. (2024). In-Depth Analysis and Countermeasures for Ransomware Attacks: Case Studies and Recommendations. https://doi.org/10.20944/preprints202408.2261.v1
[10] Alhaji, U. M., Adewumi, S. E., & Yemi-peters, V. I. (2025). Classification of Phishing Attacks Using Machine Learning Algorithms: A Systematic Literature Review. Journal of Advances in Mathematics and Computer Science, 40(1), 26–44. https://doi.org/10.9734/jamcs/2025/v40i11960
[11] Jampani, S. K. (2025). Social Engineering 2.0 Deepfake and Deep Learning-based Cyber-attacks (Phishing). IJFMR - International Journal For Multidisciplinary Research, 7(1). https://doi.org/10.36948/ijfmr.2025.v07i01.35527
[12] DDOS Attacks and Analysis of Different Defense Mechanisms – IJSREM. (n.d.). Retrieved May 31, 2025, from https://ijsrem.com/download/ddos-attacks-and-analysis-of-different-defense-mechanisms/
[13] Afek, Y., Berger, H., & Bremler-Barr, A. (2025, January 23). POPS: From History to Mitigation of DNS Cache Poisoning Attacks. arXiv.Org. https://arxiv.org/abs/2501.13540v1
[14] Rolansa, F., Istiyanto, J. E., Afiahayati, A., & Frisky, A. Z. K. (2025). SMOTE tree-based autoencoder multi-stage detection for man-in-the-middle in SCADA. Indonesian Journal of Electrical Engineering and Computer Science, 38(1), Article 1. https://doi.org/10.11591/ijeecs.v38.i1.pp133-144
[15] Kandasamy, V., & Roseline, A. A. (2025). Harnessing advanced hybrid deep learning model for real-time detection and prevention of man-in-the-middle cyber attacks. Scientific Reports, 15(1), Article 1. https://doi.org/10.1038/s41598-025-85547-5
[16] Zhuo, Z., Cai, T., Zhang, X., & Lv, F. (2021). Long short-term memory on abstract syntax tree for SQL injection detection. IET Software, 15(2), 188–197. https://doi.org/10.1049/sfw2.12018
[17] College of Computers and Information Technology, Taif University, Taif, SA., Awadh, N., Zaid, H., College of Computers and Information Technology, Taif University, Taif, SA., Al-ajmani, Dr. S., & Department of Information Technology, College of Computer and Information Technology, Taif University, Taif, SA. (2025). A Robust Framework for Detecting Brute-Force Attacks through Deep Learning Techniques. International Journal of Recent Technology and Engineering (IJRTE), 13(5), 27–42. https://doi.org/10.35940/ijrte.E8182.13050125
[18] Mujtaba, A., Zulfiqar, M., Azhar, M. U., Ali, S., Ali, A., & Khan, H. (2025). ML-based Fileless Malware Threats Analysis for the Detection of Cyber security Attack based on Memory Forensics: A Survey. The Asian Bulletin of Big Data Management, 5(1), Article 1. https://doi.org/10.62019/abbdm.v5i1.289
[19] Guadarrama-Estrada, A. R., Osorio-Gordillo, G. L., Vargas-Méndez, R. A., Reyes-Reyes, J., & Astorga-Zaragoza, C. M. (2025). Cyber–Physical System Attack Detection and Isolation: A Takagi–Sugeno Approach. Mathematical and Computational Applications, 30(1), Article 1. https://doi.org/10.3390/mca30010012
[20] Transportation-Energy-Communication Integrated Management of Ship Cyber-Physical Systems Against Cyber Attacks. (n.d.). Retrieved May 31, 2025, from https://ieeexplore.ieee.org/document/10833774
[21] Swope, C., Bingen, K. A., Young, M., & Lafave, K. (2025). Space Threat Assessment 2025. Center for Strategic & International Studies. https://scispace.com/pdf/kinetic-weapons-nonkinetic-weapons-electronic-weapons-cyber-p1kxo3ufwf.pdf
[22] Greig, J. (2023, January 17). Ransomware attack on maritime software impacts 1,000 ships. https://therecord.media/ransomware-attack-on-maritime-software-impacts-1000-ships
[23] Kovacs, E. (2023, January 18). Ransomware Attack on DNV Ship Management Software Impacts 1,000 Vessels. SecurityWeek. https://www.securityweek.com/ransomware-attack-dnv-ship-management-software-impacts-1000-vessels/
[24] Page, C. (2023, January 18). Maritime giant DNV says 1,000 ships affected by ransomware attack. TechCrunch. https://techcrunch.com/2023/01/18/dnv-norway-shipping-ransomware/
[25] Cyber-attack on ShipManager servers – update. (2023, January 23). DNV. https://www.dnv.com/news/cyber-attack-on-shipmanager-servers-update-237931/
[26] LaGrone, S. (2023, April 20). Ransomware Attack Hits Marinette Marine Shipyard, Results in Short-Term Delay of Frigate, Freedom LCS Construction. USNI News. https://news.usni.org/2023/04/20/ransomware-attack-hits-marinette-marine-shipyard-results-in-short-term-delay-of-frigate-freedom-lcs-construction
[27] Ransomware attack on US Navy shipbuilder leaked information of nearly 17,000 people. (n.d.). Retrieved May 31, 2025, from https://therecord.media/fincantieri-shipbuilder-us-navy-wisconsin-ransomware
[28] Arghire, I. (2023, July 5). Japan's Nagoya Port Suspends Cargo Operations Following Ransomware Attack. SecurityWeek. https://www.securityweek.com/japans-nagoya-port-suspends-cargo-operations-following-ransomware-attack/
[29] Nagoya Port Cyber Attack Japan's Largest Port Paralyzed 2023. (2023, July 5). https://thecyberexpress.com/nagoya-port-cyber-attack-largest-japan/
[30] Wadhwani, S. (n.d.). Nagoya Port Ransomware Attack — Spiceworks. Spiceworks Inc. Retrieved April 27, 2025, from https://www.spiceworks.com/it-security/security-general/news/nagoya-port-ransomware-attack/
[31] Benjamin, J. (2023, July 11). OT Cybersecurity Breach Disrupts Operations at the Port of Nagoya, Japan | Dragos. https://www.dragos.com/blog/ot-cybersecurity-breach-disrupts-operations-at-the-port-of-nagoya-japan/
[32] Network, M. N. (2025, May 16). Intelligence Firm Confirms GPS Spoofing Responsible For MSC Antonia Grounding. Marine Insight. https://www.marineinsight.com/shipping-news/intelligence-firm-confirms-gps-spoofing-responsible-for-msc-antonia-grounding/
[33] Schuler, M. (2025, May 15). Pole Star Confirms GPS Interference Caused MSC ANTONIA Grounding. gCaptain. https://gcaptain.com/pole-star-confirms-gps-interference-caused-msc-antonia-grounding/
[34] MSC ANTONIA Current Position (Container Ship, IMO 9398216) — VesselFinder. (n.d.). Retrieved May 29, 2025, from https://www.vesselfinder.com/pl/?imo=9398216
[35] UKMTO Ops Centre w [@UK_MTO]. (2025, May 9). 20250509_UKMTO_ADVISORY_INCIDENT 015-25 https://ukmto.org/-/media/ukmto/products/20250509_ukmto_advisory_incident-015-25.pdf?rev=aaa78cfdab39445b8662a9c4232205e3

#maritimesecurity #marsec https://t.co/khaYhYTInP [Tweet]. Twitter. https://x.com/UK_MTO/status/1920869477698191489
[36] SideWinder APT | StealerBot Campaign—CyberStash. (n.d.). Retrieved May 29, 2025, from https://www.cyberstash.com/sidewinder-apt-stealerbot-campaign/
[37] "SideWinder" Intensifies Attacks on Maritime Sector. (n.d.). Retrieved May 29, 2025, from https://www.darkreading.com/cyberattacks-data-breaches/sidewinder-intensifies-attacks-maritime-sector
[38] CVE-2017-11882—Security Update Guide—Microsoft—Microsoft Office Memory Corruption Vulnerability. (n.d.). Retrieved May 29, 2025, from https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882
[39] SideWinder APT | StealerBot Campaign. (2024, October). Cyber Stash. https://www.cyberstash.com/wp-content/uploads/2024/10/SideWinder-APT-StealerBot-Campaign.pdf
[40] Dixon (g_dixon), G. (2023, May 25). Ship AIS data spoofed to draw pro-war Russian Z symbol in Black Sea. TradeWinds | Latest Shipping and Maritime News. https://www.tradewindsnews.com/technology/ship-ais-data-spoofed-to-draw-pro-war-russian-z-symbol-in-black-sea/2-1-1456329
[41] Spoofed AIS Signals Form Symbol of Russian Invasion. (n.d.). The Maritime Executive. Retrieved May 30, 2025, from https://maritime-executive.com/article/spoofed-ais-signals-form-symbol-of-russian-invasion-off-crimea
[42] Courtnell, J. (2023, October 2). AIS Spoofing Research Unveils 4 Main Typologies: A Complete Guide. Pole Star Global. https://www.polestarglobal.com/resources/ais-spoofing/
[43] Mass AIS Spoofing Event "Moves" Dozens of Ships to Crimean Airport. (n.d.). The Maritime Executive. Retrieved May 30, 2025, from https://maritime-executive.com/editorials/mass-ais-spoofing-event-moves-dozens-of-ships-to-crimean-airport
[44] Rotterdam: Europe's Largest Port Targeted in Cyberattack Linked to Pro-Russian Hackers. (2023, June 14). Tech Times. https://www.techtimes.com/articles/292580/20230614/rotterdam-europe-largest-port-cyberattack-pro-russian-hackers.htm
[45] Port of Rotterdam Targeted in Cyberattack—Maritime Gateway. (n.d.). Retrieved May 30, 2025, from https://www.maritimegateway.com/port-of-rotterdam-targeted-in-cyberattack/
[46] Dutch ports' websites offline for hours, days due to pro-Russian cyber attacks | NL Times. (2023, June 14). https://nltimes.nl/2023/06/14/dutch-ports-websites-offline-hours-days-due-pro-russian-cyber-attacks
[47] Dark Web Profile: Killnet - Russian Hacktivist Group. (2022, December 16). SOCRadar® Cyber Intelligence Inc. https://socradar.io/dark-web-profile-killnet-russian-hacktivist-group/
[48] Major Cyber Attacks Targeting Transportation & Logistics Industry. (2025, March 28). SOCRadar® Cyber Intelligence Inc. https://socradar.io/major-cyber-attacks-transportation-logistics-industry/
[49] EUROPEAN CYBER REPORT. (2025). Link11. https://www.link11.com/wp-content/uploads/2025/03/Link11_European_Cyber_Report_EN_2025-2.pdf
[50] Desk, iHLS N. (2025, May 8). Massive Surge in DDoS Attacks Targets Spain and Europe Amid Rising Hacktivist Campaigns. iHLS. https://i-hls.com/archives/129199
[51] Russian GRU Targeting Western Logistics Entities and Technology Companies | CISA. (2025, May 21). https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a
[52] Greenberg, A. (n.d.). Russian Hackers Are Trying to Brute-Force Hundreds of Networks. Wired. Retrieved May 30, 2025, from https://www.wired.com/story/fancy-bear-russia-brute-force-hacking/
[53] Coast Guard Cyber Command. (2023). 2022 Cyber Trends and Insights in the Marine Environment (CTIME) Report. United States Coast Guard. https://www.uscg.mil/Portals/0/Images/cyber/2022CTIMEReport_Final.pdf?ver=lFYiLZqt4dbVf2RFTgL15g%3d%3d&timestamp=1685643398263