sciendo

Land Forces Academy Review
Vol. XXX, No. 2(118), 2025

CYBERATTACKS ON PORT INFRASTRUCTURES: A DECADE OF TRENDS, INCIDENTS, AND MITIGATION STRATEGIES (2011-2024)

Minodora BADEA
University POLITEHNICA of Bucharest, Romania
badea.minodora@yahoo.com

Olga BUCOVEȚCHI
University POLITEHNICA of Bucharest, Romania
National Institute for Research & Development in Informatics – ICI Bucharest, Romania
olga.bucovetchi@upb.ro

Adrian V. GHEORGHE
Old Dominion University, Norfolk, Virginia, USA
University POLITEHNICA of Bucharest, Romania
agheorgh@odu.edu

Gabriel RAICU
Constanta Maritime University, Romania
gabriel.raicu@cmu-edu.eu

ABSTRACT

Port infrastructures are critical to global trade, handling over 80% of the world's cargo by volume. However, their increasing reliance on digital technologies has exposed them to a wide range of cyber threats. This paper provides a comprehensive analysis of cyberattacks targeting port infrastructures from 2011 to the present. We examine the types of attacks, geographical distribution, notable incidents, and underlying vulnerabilities. Additionally, we discuss mitigation strategies and future directions for enhancing cybersecurity in the maritime sector. Our findings highlight the urgent need for robust regulatory frameworks, advanced technological solutions, and collaborative efforts to safeguard critical port operations.

KEYWORDS: cybersecurity, port infrastructures, ransomware, DDoS, cyberwarfare, maritime security, mitigation strategies

1. Introduction

The growing dependence on interconnected digital systems in port operations has heightened cybersecurity risks, exposing seaports – key hubs in global trade – to increasingly advanced cyberattacks. This vulnerability demands a deep understanding of the shifting threat landscape, strong protective measures, and efficient response strategies to safeguard these critical infrastructures (Mawer et al., 2024; D'Amelio & Abuzneid, 2024;

DOI: 10.2478/raft-2025-0017

Patrick et al., 2024). As ports embrace digitalization, they face a rising tide of cyber incidents that disrupt operations and inflict substantial economic damage, underscoring the urgency for comprehensive cybersecurity solutions.

This study explores the cybersecurity challenges confronting port infrastructures in 2025, leveraging current research to pinpoint major threats, suggesting mitigation approaches, and identifying gaps needing further exploration. It examines the detection, prevention, and management of cyber threats, using existing literature to showcase practical examples and effective practices. With ports serving as essential conduits for international commerce, their digital evolution has made them prime targets for attacks like ransomware and state-backed cyber operations, necessitating a detailed review of attack patterns, real-world cases, and defensive strategies to bolster resilience.

2. Literature Review on Cyberattacks on Port Infrastructures

The expanding use of interconnected digital technologies in port operations has introduced significant cybersecurity weaknesses, making seaports – pivotal to global commerce – prime targets for increasingly complex cyberattacks. This trend calls for a thorough grasp of the changing threat environment, resilient defense tactics, and streamlined response protocols to protect these vital (Mawer et al., 2024; D'Amelio & Abuzneid, 2024; Patrick et al., 2024). As digital tools become integral to port functions, the surge in cyber incidents underscores the pressing need for fortified security measures to counter operational disruptions and financial setbacks.

This analysis investigates the cybersecurity obstacles facing port infrastructures in 2025, building on prior studies to highlight primary threats, recommend protective strategies, and point out areas warranting deeper research. It focuses on recognizing, countering, and resolving cyber risks, drawing from published works to present real-world insights and proven methods. Ports, essential to the flow of international goods, have seen a decade-long rise in attacks – from ransomware to state-orchestrated cyber campaigns – prompting a structured evaluation of threat trends, incident impacts, and countermeasures to strengthen their defenses.

The research is motivated by the growing frequency and sophistication of cyberattacks on ports, which have far-reaching implications for global trade and economic stability.

This analysis delves into critical aspects of port cybersecurity, identifying prevalent threats like ransomware, DDoS attacks, and state-sponsored cyberwarfare, driven by motives such as profit, geopolitics, and sabotage. It assesses the effectiveness of current defenses while proposing advanced solutions like real-time monitoring, threat detection, and rapid incident response. The study also examines best practices for incident response, emphasizing international coordination, business continuity planning, and the influence of regulations and standards on resilience. Additionally, it highlights research gaps, particularly around emerging technologies (e.g., IoT, AI) and the potential for global collaboration to strengthen defenses. By tackling these areas, the research aims to enhance understanding of port cybersecurity challenges, offering practical recommendations for operators, policymakers, and experts to protect vital infrastructure and sustain global trade.

2.1. Limitations

One of the primary limitations of this study is the lack of access to specialized databases such as Maritime Cybersecurity NL, which may contain valuable insights and case studies. Additionally, the rapidly evolving nature of cybersecurity threats means that some findings may become

outdated by 2025. Despite these limitations, the study provides a robust foundation for understanding and addressing cybersecurity challenges in port infrastructures.

3. Material and Methods

This research employs a mixed-methods approach, combining qualitative and quantitative analyses. The primary methodology involves a systematic literature review of scientific databases, including Web of Knowledge, Scopus, and Google Scholar. These databases were selected for their comprehensive coverage of peer-reviewed articles, conference papers, and technical reports related to maritime cybersecurity.

3.1. Data Collection

The literature review focused on identifying key cybersecurity threats to port infrastructures, existing mitigation strategies, and case studies of successful resolution of cyber incidents. Keywords such as "maritime cybersecurity", "port infrastructure" "cyber threats" and "2025 projections" were used to retrieve relevant publications.

3.2. Data Analysis

The collected data were analyzed thematically to identify common patterns, emerging trends, and gaps in existing literature. Case studies were selected based on their relevance to the 2025 threat landscape and their potential to provide actionable insights for port operators and policymakers.

4. Identifying Cybersecurity Threats to Port Infrastructures

Modern ports utilize a complex network of interconnected systems, including operational technology (OT) and information technology (IT) infrastructure, communication networks, and various software applications. This interconnectedness creates a large attack surface, making ports vulnerable to a wide range of cyber threats (Fenton, 2024; Avanesova et al., 2021).

These threats can be broadly categorized into several key areas:

- **Attacks on Critical Infrastructure and Election Support Systems**

The disruption of electric power operations can have catastrophic consequences for national security and the economy (Fenton, 2024). Ports, as critical infrastructure, are particularly vulnerable to attacks targeting their power grids, communication systems, and other essential services. A successful attack could lead to significant operational disruptions, financial losses, and potential safety hazards. The North American Electric Reliability Corporation (NERC) has established cybersecurity standards to address these vulnerabilities, but continuous monitoring and adaptation are crucial to stay ahead of evolving threats. The increasing reliance on interconnected systems necessitates a multi-faceted approach to security. Moreover, the interdependencies among computers, communication, and power infrastructures create complex challenges in meeting security and quality compliance. A systematic information security analysis of critical infrastructure is therefore essential (Farah et al., 2022).

- **Misinformation, Disinformation, and Malinformation (MDM) Campaigns**

The spread of MDM campaigns poses a significant threat to the integrity of port operations and the trust placed in them. These campaigns can be used to manipulate public opinion, sow discord, and undermine confidence in port authorities as stated by (Kamiski, 2021).

The impact of such campaigns can extend beyond simple misinformation, potentially influencing critical decision-making processes and disrupting supply chains. The sophistication of these campaigns is increasing, and their potential impact underscores the need for proactive measures to counter their spread.

This threat is particularly relevant in the context of elections, the disruption of electoral processes could have far-reaching consequences (Islam et al., 2021).

- **Espionage by Malicious Actors**

Ports handle vast quantities of sensitive data, including cargo manifests, financial transactions, and operational information. This data is attractive to malicious actors seeking to gain an economic or strategic advantage (Kamiski, 2021). Espionage activities can compromise the confidentiality, integrity, and availability of this data, potentially leading to significant financial losses, reputational damage, and national security risks. The potential for espionage highlights the need for robust data protection measures, including access controls, encryption, and regular security audits. The methods used by malicious actors are constantly evolving, requiring continuous adaptation and vigilance. The increasing reliance on technology in the maritime industry only amplifies this risk (D'Amelio & Abuzneid, 2024).

- **Attacks on Operational Technology (OT) Systems**

The increasing integration of OT systems in port operations presents new cybersecurity challenges (D'Amelio & Abuzneid, 2024). These systems control critical infrastructure and processes, and a successful attack could have severe consequences. Previous studies have indicated an underestimation of the possibility and impact of attacks on OT systems, highlighting the need for increased awareness and training among port personnel. The maritime industry's reliance on technology while enhancing efficiency creates a larger attack surface that necessitates comprehensive cybersecurity awareness training (D'Amelio & Abuzneid, 2024).

- **Vulnerabilities in Satellite Navigation Systems**

The reliance on satellite navigation systems, particularly GPS, for vessel navigation and port operations creates vulnerabilities to spoofing and jamming attacks. Such attacks could disrupt navigation, leading to accidents, delays, and significant economic losses. The need for multiple positioning, navigation, and timing (PNT) systems onboard vessels to complement GPS-only navigation is crucial. Exploring alternative navigation technologies and enhancing the resilience of existing systems are critical aspects of mitigating this threat (Avanesova et al., 2021).

5. Port Infrastructure Vulnerabilities

Port infrastructures, encompassing both physical and digital assets, are particularly vulnerable to cyberattacks due to their complex interconnectedness (Progoulakis et al., 2022; Weaver et al., 2021). These systems integrate operational technology (OT) and information technology (IT) systems, are creating dependencies that can be exploited by attackers (Farah et al., 2022; Weaver et al., 2021). Aging IT infrastructure in some areas further exacerbates the situation, increasing the likelihood of successful attacks (Fenton, 2024). The integration of Internet of Things (IoT) devices in ports expands the attack surface, while a lack of cybersecurity awareness among personnel compromises the human element of security (Fenton, 2024; D'Amelio & Abuzneid, 2024). This vulnerability is particularly pronounced in developing regions, where technological infrastructure and specialized skills may lag global standards (Patrick et al., 2024). Furthermore, the reliance on Global Navigation Satellite Systems (GNSS) for navigation and positioning introduces vulnerabilities that could be exploited to disrupt operations. Attacks on GNSS, such as spoofing or jamming, could lead to navigational errors, collisions, or even grounding (Farah et al., 2022; Androjna et al., 2020).

The potential for cascading disruption in congested waterways further underscores

the severity of these risks. The lack of adequate information sharing among stakeholders hinders effective threat response and proactive mitigation (Fenton, 2024).

Cybersecurity threats targeting port infrastructures are growing more complex and diverse, as attackers exploit vulnerabilities using advanced techniques, driven by the maritime industry's increasing dependence on technology and interconnected systems. Grasping the nature of these threats is essential for crafting robust mitigation and response strategies to protect critical operations.

5.1. Specific Vulnerabilities within Port Systems

A detailed examination reveals specific vulnerabilities within various port systems. For instance, access control systems, cargo management systems, check-in systems, and maritime traffic control systems are all potential targets for cyberattacks (Golgota & Erma, 2024). A successful attack could lead to data breaches, operational disruptions, or even physical damage (Avanesova et al., 2021). The complexity of these systems, coupled with the often-fragmented nature of security implementations, creates numerous opportunities for attackers to exploit weaknesses. The increasing use of SCADA in port operations further complicates the cybersecurity landscape systems (Kalogeraki et al., 2018). SCADA systems manage critical infrastructure, and a successful cyberattack could have far-reaching consequences. The lack of specific security requirements for control and monitoring devices, such as IoT platforms and satellites, presents a significant vulnerability. The interconnected nature of SCADA systems also means that a breach in one area could easily cascade to other parts of the infrastructure systems (Kalogeraki et al., 2018).

5.2. Types of Cyber Threats Targeting Maritime Ports

The range of cyber threats targeting maritime ports is diverse and ever evolving. These threats can range from relatively simple attacks, such as phishing or malware, to more sophisticated attacks, such as ransomware or denial-of-service attacks (Avanesova et al., 2021; Farah et al., 2022; Faria, 2020). State-sponsored actors and organized crime groups are increasingly active in the maritime domain, targeting both IT and OT systems for various purposes. These purposes may range from espionage and data exfiltration to disruption of operations and financial gain (Cichocki, 2023; Rohan, 2023; Avanesova et al., 2021). Opportunistic piracy remains a concern, potentially combining physical attacks with cyberattacks to maximize disruption. The increasing sophistication of cyberattacks necessitates a move beyond reactive measures towards a proactive, risk-based approach to security. The use of hybrid threats, combining cyberattacks with other forms of influence operations, further complicates the threat landscape. These attacks target both civilian and defense infrastructures, underscoring the need for robust and adaptable security frameworks (Fenton, 2024; Vasilescu & Preda, 2024).

5.3. Specific Threat Actors and Their Motives

While many cyberattacks remain attributed to "unknown" actors several studies point to the involvement of state-sponsored groups and organized crime. China, for instance, is identified as a significant threat actor, engaging in data exfiltration and other forms of cyber espionage. Other actors, such as Russia and Iran, are also implicated in maritime cyberattacks.

These attacks often target specific assets, such as shipping companies or ports, with the goal of disrupting operations or

gaining access to sensitive information. The motives range from economic gain to political influence, highlighting the diverse nature of threats facing the maritime industry (Rohan, 2023). The lack of detailed information on specific threat actors and their motives in some cases necessitates further research. Understanding the motivations and capabilities of these actors is crucial for developing effective mitigation strategies. An analysis of attack patterns and techniques is also essential for proactive security measures (Cichocki, 2023).

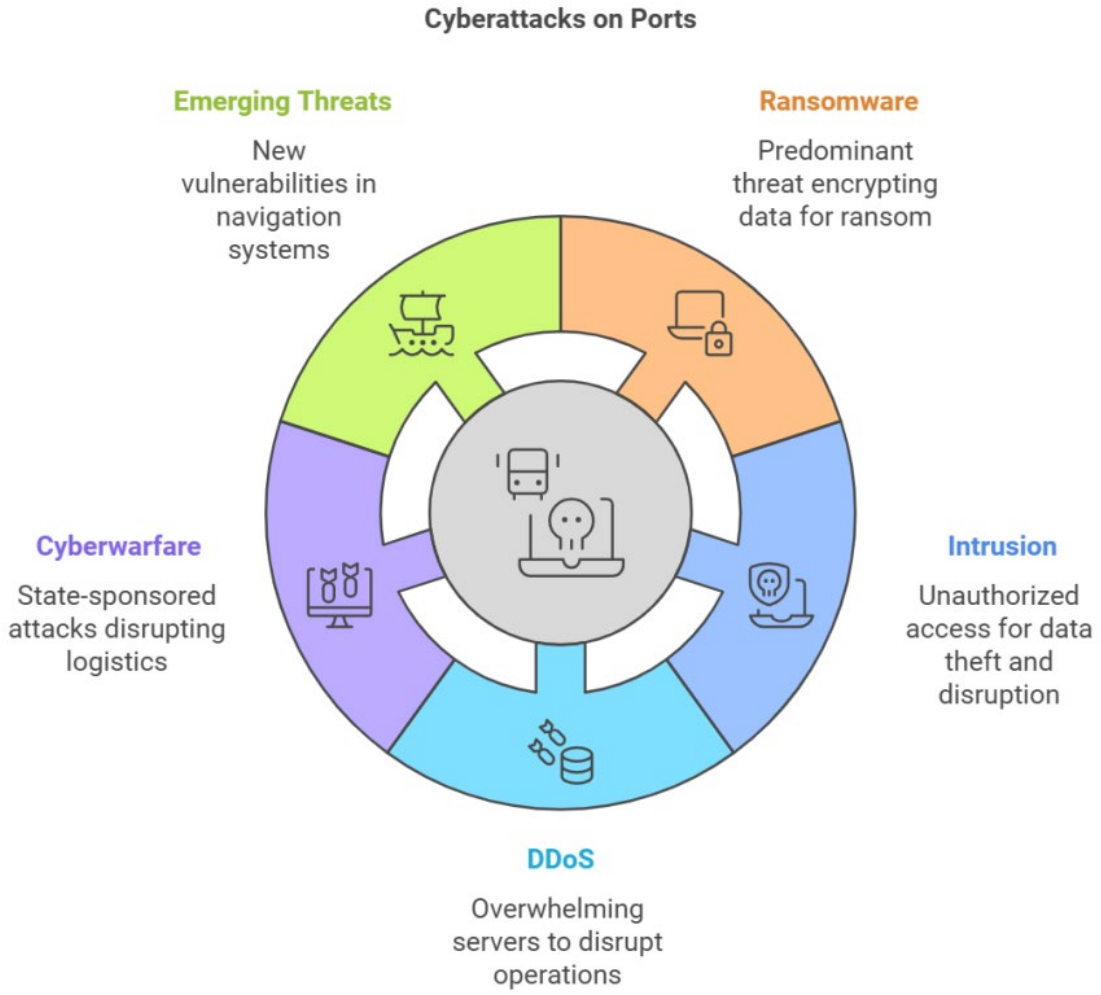

Figure no.1: *Cyberattacks on ports*

Ransomware remains the most prevalent threat, accounting for 69% of reported incidents. These attacks involve encrypting critical operational data and demanding ransom payments for decryption keys. The 2017 Petya attack on Maersk, which disrupted operations across 76 terminals worldwide and resulted in $300 million in losses, is a landmark example.

More recently, in April 2024, a coordinated ransomware attack targeted multiple maritime ports, crippling operations and manipulating Automatic Identification Systems (AIS) on ships, leading to significant delays and near-collisions.

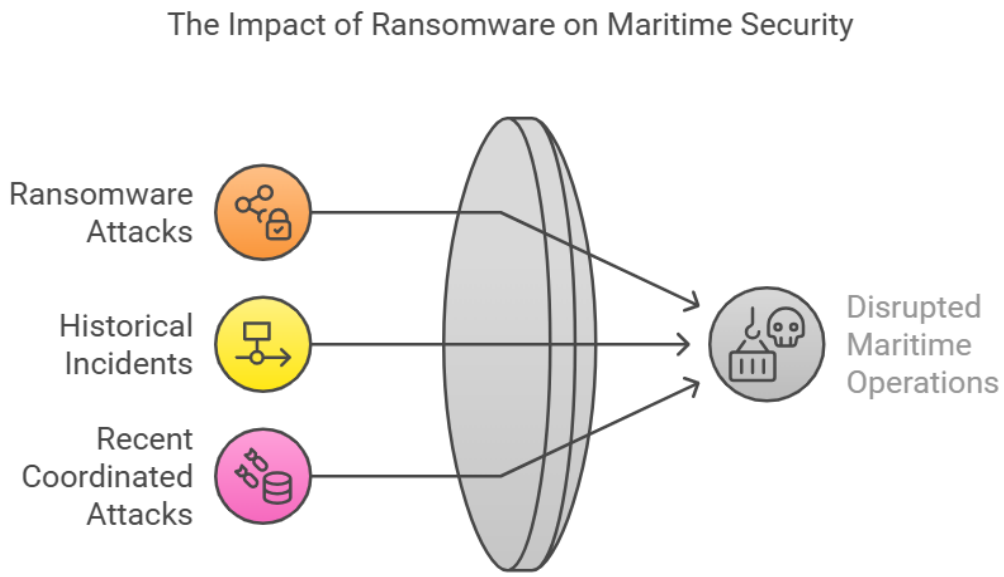

Figure no. 2: *The impact of Ransomware on Maritime Security*

Intrusion attacks, constituting 15% of incidents, involve unauthorized access to information networks. A notable case occurred in 2011 when a criminal drug cartel infiltrated the Port of Antwerp's container management system to facilitate drug smuggling. In 2023, a state-sponsored hacker group breached the Port of Lisbon's systems, exfiltrating sensitive data and disrupting operations.

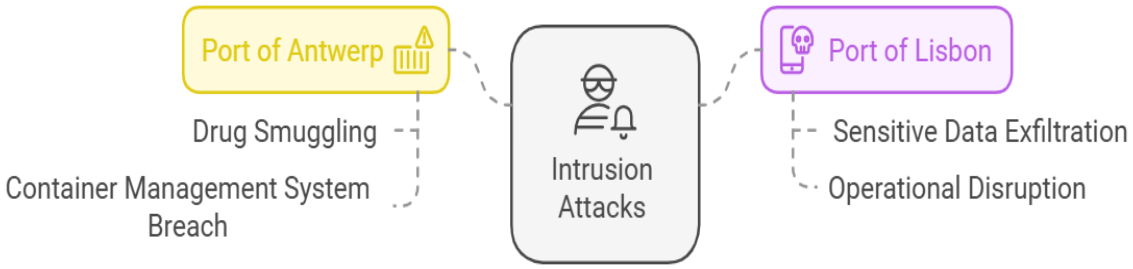

Figure no. 3: *Intrusion Attacks*

DDoS attacks, also making up 15% of incidents, aim to overwhelm servers and disrupt operations. In 2023, a surge in DDoS attacks was observed, particularly targeting ports supporting Ukraine amid the ongoing conflict with Russia.

These attacks disrupted communication systems and caused significant operational delays.

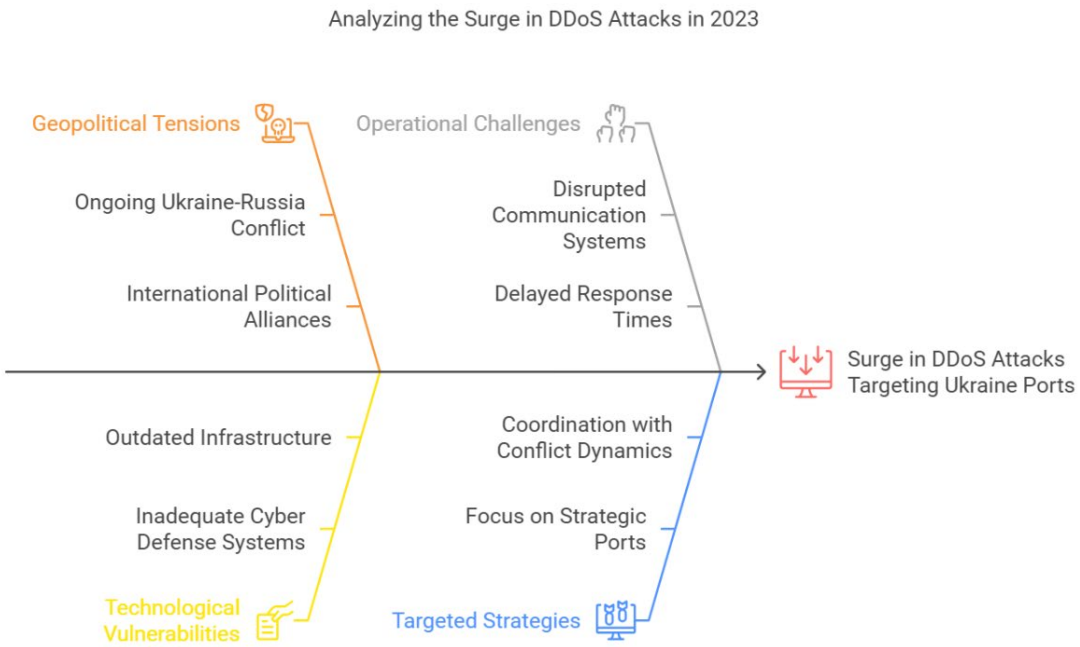

Figure no. 4: *Analyzing the surge in DDoS in 2023*

State-sponsored cyberattacks have targeted port infrastructures as part of broader geopolitical conflicts. For instance, in 2020, Israel launched a cyberattack on the Iranian Port of Shahid Rajaee in retaliation for earlier attacks on Israeli infrastructure. In 2024, Russian hacker groups targeted ports supporting Ukraine, using DDoS attacks to disrupt logistics and supply chains.

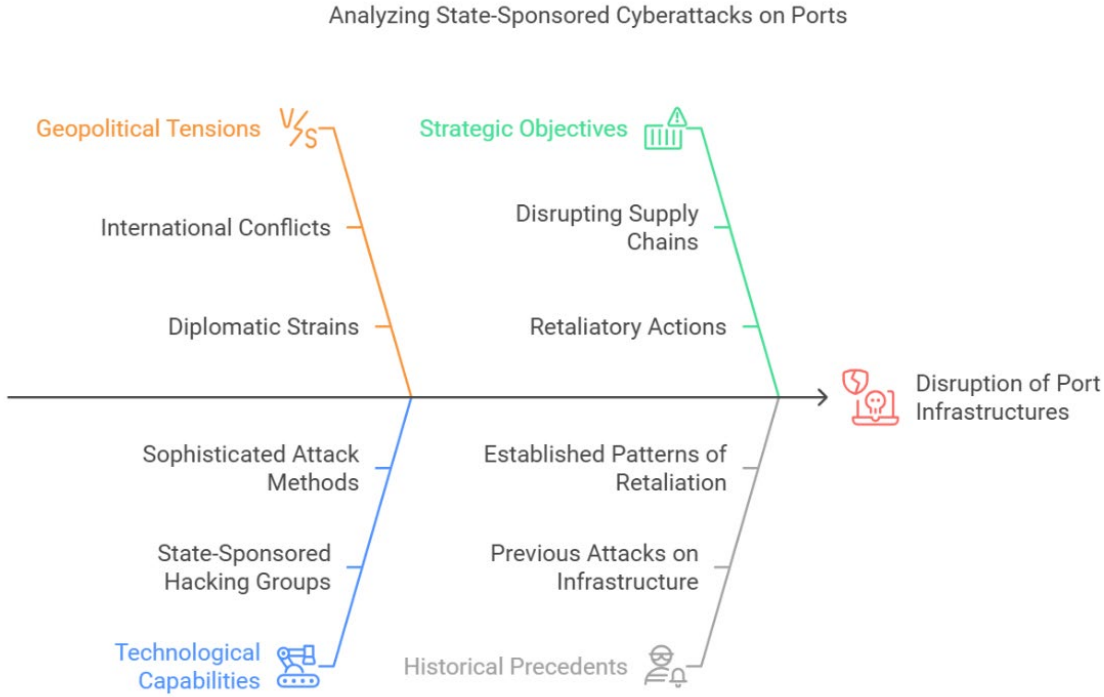

Figure no. 5: *Analyzing State-Sponsored Cyberattacks on Ports*

Emerging threats include GPS spoofing and AIS manipulation, which can lead to navigational errors and safety risks. In 2024, GPS interference was reported in the Strait of Hormuz, highlighting the vulnerability of maritime navigation systems. Additionally, the convergence of IT and OT systems has introduced new risks, such as the potential for cyber-physical attacks on ship navigation and propulsion systems.

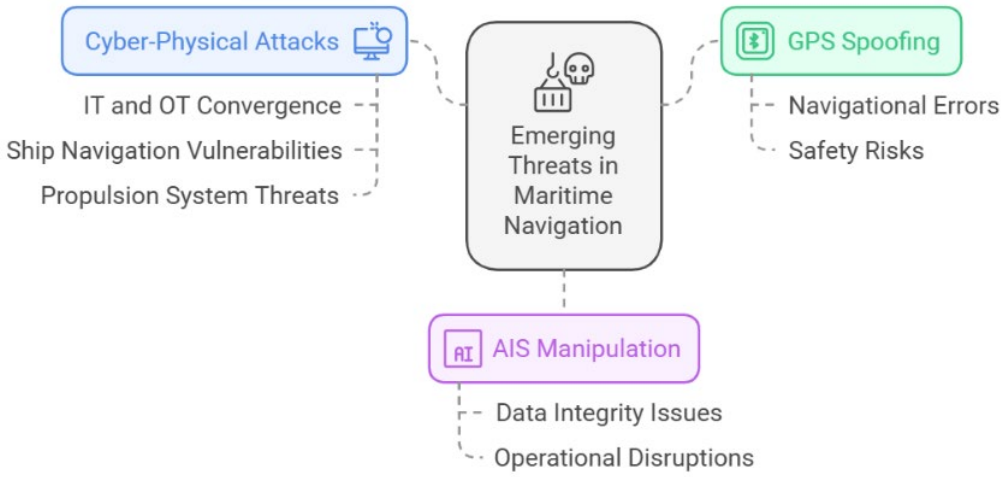

Figure no. 6: *Emerging Threats in Maritime Navigation*

6. Geographical Distribution on the Cyberattacks on Ports Analyzed

Cyberattacks on ports have been reported globally, with significant concentrations in Europe and North America. However, incidents have also been documented in Asia, Africa, and South America.

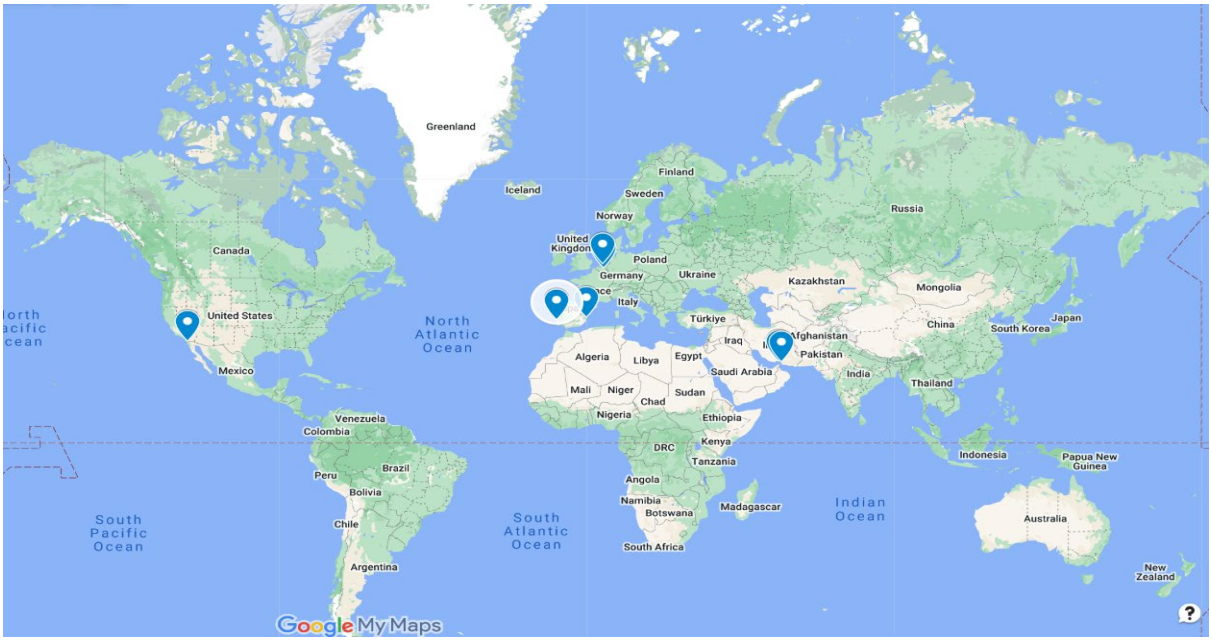

Figure no. 7: *Geographical distribution on the Cyberattacks on ports analyzed*
(Source: Authors' own elaboration)

Table no. 1 embeds the key incidents that highlight the evolving nature of cyber threats to port infrastructures:

Table no. 1

Case Studies of Cyberattacks on Port Infrastructures (2011-2024)

Year	Port/ Organization	Type of Attack	Hacker Category	Description	Impact
2011	Port of Antwerp, Belgium	Intrusion	Criminal Drug Cartel	Criminal group breached the container management system to facilitate drug smuggling.	Highlighted vulnerabilities in port security systems.
2017	Maersk (Global Terminals)	Ransomware (Petya)	Cybercriminal Group	Petya ransomware encrypted systems, disrupting operations at 76 ports worldwide.	$300 million in losses; significant operational downtime.
2018	Port of San Diego, USA	Ransomware (SamSam)	State-Sponsored (Iran)	Iranian hacker group launched a ransomware attack on port systems.	Disrupted port operations; attributed to geopolitical motivations.
2020	Port of Shahid Rajaee, Iran	Cyberwarfare	State-Sponsored (Israel)	Israel launched a cyberattack in retaliation for Iranian cyberattacks on Israeli infrastructure.	Temporarily disrupted port operations; part of ongoing cyber conflict.
2021	South African Ports	Ransomware	Cybercriminal Group	A ransomware attack disrupted operations at multiple South African ports.	Widespread operational disruptions; economic losses.
2023	Port of Nagoya, Japan	Ransomware	Unknown (Suspected Cybercriminals)	Suspected ransomware attack disrupted operations at Japan's largest port.	Operations halted for several days; significant economic losses.
2023	Port of Lisbon, Portugal	Intrusion	State-Sponsored (Suspected Russia)	State-sponsored hacker group breached systems, exfiltrating sensitive data.	Disrupted operations highlighted growing sophistication of cyber threats.
2023	Multiple Ports (Ukraine Support)	DDoS	State-Sponsored (Russia)	Russian hacker groups targeted ports supporting Ukraine amid the ongoing Ukraine War.	Surge in DDoS attacks; disrupted port operations and logistics.
2024	Port of Rotterdam, Netherlands	Ransomware	Cybercriminal Group	Coordinated ransomware attack targeted multiple maritime ports, manipulating AIS on ships.	Widespread disruptions; losses exceeding $500 million.

Year	Port/ Organization	Type of Attack	Hacker Category	Description	Impact
2024	Port of Singapore	DDoS	State-Sponsored (Suspected China)	DDoS attack delayed cargo handling and caused significant economic losses.	Operational delays; economic impact.
2024	Strait of Hormuz	GPS Spoofing	State-Sponsored (Suspected Iran)	GPS interference reported, leading to navigational errors and safety risks.	Highlighted vulnerabilities in maritime navigation systems.
2024	Port of Valencia, Spain	Cyber-Physical Attack	Academic/Research Simulation	Simulated attack on a container ship's rudder system demonstrated potential for high-impact disruptions.	Highlighted need for enhanced cybersecurity measures.

Global maritime infrastructure confronts increasingly sophisticated cyber threats, exhibiting pronounced regional disparities in vulnerability and response capacity, with Europe and North America notably impacted by significant incidents such as the 2017 Petya attack on Maersk terminals and the 2018 Port of San Diego ransomware event, revealing critical weaknesses in global supply chains that precipitate widespread operational disruptions and economic repercussions. In Asia, ports like Nagoya (2023 ransomware) and Singapore (2024 DDoS) exemplify escalating cybersecurity challenges, while Africa and South America report fewer incidents − likely due to underreporting and inadequate infrastructure rather than resilience – contrasting with China's opaque cybersecurity profile, where state-controlled measures obscure the true extent of threats, necessitating a cohesive global strategy encompassing advanced technology, real-time surveillance, international cooperation, and continuous personnel training to mitigate these dynamic digital risks.

Cyberattacks on ports, such as ransomware and DDoS, threaten global trade due to their interconnected nature, causing widespread operational and economic disruptions. No region is safe, and poor transparency in reporting, especially in Africa, South America, and China, hides the true scale of the issue, amplifying risks of delays, losses, and reputational harm. Ports must adopt advanced cybersecurity tools – real-time monitoring, threat detection, and rapid response – while fostering international collaboration and transparent reporting. Robust business continuity and disaster recovery plans are essential to mitigate impacts and ensure trade resilience.

7. Mitigation Strategies and Cybersecurity Best Practices

Addressing the cybersecurity challenges facing maritime ports requires a multi-faceted approach encompassing technological, procedural, and human elements (Fenton, 2024; Patrick et al., 2024). Technological solutions include strengthening IT and OT infrastructure, implementing robust access control measures, and deploying advanced threat detection and response systems (Fenton, 2024; Progoulakis et al., 2022; Golgota & Erma, 2024; Jacq et al., 2018). Regular security audits and vulnerability assessments are crucial for identifying and addressing weaknesses before they can be exploited (Progoulakis et al., 2022; Melnyk et al., 2023). The implementation of international standards and regulatory frameworks provides a baseline for security practices (Fenton, 2024; Vasilescu & Preda, 2024).

Figure no. 8: *Vulnerabilities and Challenges in Port Security*

The growing adoption of IoT and connected systems in ports has significantly increased their exposure to cyber threats, further exacerbated by the continued reliance on legacy infrastructure and the human factor, including vulnerabilities to phishing and social engineering attacks (Cîrnu et al., 2018). To address these risks, it is crucial to improve information sharing among stakeholders, develop comprehensive incident response strategies, and strengthen supply chain security measures (Fenton, 2024; Patrick et al., 2024). Additionally, regular cybersecurity drills and targeted training programs are essential to enhance staff awareness and resilience against evolving cyber threats (Avanesova et al., 2021; D'Amelio & Abuzneid, 2024).

8. Research Gaps and Future Directions

As ports continue to modernize, cybersecurity remains a paramount concern, with emerging technologies such as artificial intelligence (AI) and blockchain being explored to improve threat detection and prevention. However, the industry must address challenges including outdated systems, fragmented infrastructures, and the human element to ensure a resilient cybersecurity future. Despite the growing body of research in maritime cybersecurity, significant gaps persist, particularly regarding understanding threat actors' motivations and capabilities, enhancing threat detection and response mechanisms, and improving port infrastructure resilience to cyberattacks (Jacq et al., 2018; Hopcraft, 2021; Weaver et al., 2021; Rohan, 2023; Vasilescu & Preda, 2024). Furthermore, the development of standardized cybersecurity competencies for seafarers, tailored to specific company and operational risk management practices, is essential for future advancements.

Research into the economic impact of cyberattacks is also crucial to inform risk assessments and investment decisions (Jacq et al., 2018; Hopcraft, 2021; Weaver et al., 2021; Rohan, 2023; Vasilescu & Preda, 2024). A proposed multicriteria approach could facilitate the development of adaptable theoretical models that address regional cybersecurity challenges, integrate blockchain technology for enhanced security, and create specific cybersecurity measures for autonomous vessels, considering regional technological,

regulatory, and infrastructural differences (Vevera et al., 2022; Adeshina et al., 2024). Additionally, research into blockchain integration in the maritime sector offers innovative solutions for improving security, transparency, and efficiency, requiring a comprehensive examination of the current network infrastructure in ports and vessels to understand the challenges and opportunities for successful implementation (Farah et al., 2024). Finally, developing tailored cybersecurity measures for autonomous vessels, given their increased connectivity and autonomy, is a critical area for future research (Tabish & Chaur-Luh, 2024).

9. Conclusions

Maritime cybersecurity, particularly concerning port infrastructures, is a complex and evolving challenge. The interconnected nature of modern maritime systems, coupled with the increasing sophistication of cyber threats, necessitates a proactive and multi-faceted approach to security. While significant progress has been made in understanding the vulnerabilities and threats, significant research gaps remain. Addressing these gaps through collaborative efforts between academia, industry, and governments is crucial for ensuring the safety, security, and resilience of the maritime sector in the face of growing cyber risks. The development of robust cybersecurity frameworks, coupled with enhanced training and awareness programs, is essential for mitigating the risks and protecting the critical infrastructure that underpins global trade and economic activity. Cyberattacks on port infrastructures pose significant risks to global trade and security. This paper has provided a comprehensive overview of the trends, incidents, and vulnerabilities observed over the past decade. By adopting robust mitigation strategies and fostering collaboration, the maritime sector can enhance its resilience against evolving cyber threats.

REFERENCES

Adeshina, F., Adelani, F.A., Olatunde, T.M., & Oliha, J.S. (2024). Theoretical perspectives on cybersecurity challenges in critical water infrastructure: insights from Africa and the United States. *International Journal of Frontiers in Engineering and Technology Research*. Available at: https://doi.org/10.53294/ijfetr.2024.6.2.0029.

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity Challenges in the Maritime Sector. *Network, 2(1),* 123-138. Available at: https://doi.org/10.3390/network2010009.

Alcaide, J.I. & Llave, R.G. (2020). Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia, 45*, 547-554. Available at: https://doi.org/10.1016/j.trpro.2020.03.058.

Avanesova, T., Gruzdeva, L., Iuskaev, R.A., Gruzdev, D.Y., & Somko, M.L. (2021). Analysis of cyber-security aspects both ashore and at sea. *IOP Conference Series Earth and Environmental Science, 872(1)*. Available at: https://doi.org/10.1088/1755-1315/872/1/012024.

Cîrnu, C.E., Rotună, C.I., Vevera, A.V., & Boncea, R. (2018). Measures to Mitigate Cybersecurity Risks and Vulnerabilities in Service-Oriented Architecture. *Studies in Informatics and Control, ISSN 1220-1766, 27(3)*, 359-368. Available at: https://doi.org/10.24846/v27i3y201811.

Cichocki, R. (2023). State-sponsored and organized crime threats to maritime transportation systems in the context of the attack on Ukraine. *TransNav: the International Journal on Marine Navigation and Safety of Sea Transportation, 17(3),* 717-721. Available at: https://doi.org/10.12716/1001.17.03.24.

D'Amelio, E. & Abuzneid, S. (2024). All hands-on tech: effectively addressing maritime operational technology risks through cybersecurity awareness training. *2024 IEEE Long Island Systems, Applications and Technology Conference.* Available at: https://doi.org/10.1109/LISAT63094.2024.10808032.

Farah, M.A.B., et al. (2022). Cyber security in the maritime industry: a systematic survey of recent advances and future trends. *Information, 13(1),* 22. Available at: https://doi.org/10.3390/info13010022.

Farah, M.A.B., et al. (2024). A survey on blockchain technology in the maritime industry: challenges and future perspectives. *Future Generation Computer Systems, 157*, 618-637. Available at: https://doi.org/10.1016/j.future.2024.03.046.

Fenton, A.J. (2024). Preventing catastrophic cyberphysical attacks on the global maritime transportation system: a case study of hybrid maritime security in the straits of Malacca and Singapore. *Journal of Marine Science and Engineering, 12(3),* 510. Available at: https://doi.org/10.3390/jmse12030510.

Golgota, A. & Erma, U. (2024). Securing Durres port's digital transformation: cybersecurity strategy for maritime industry. *13th Mediterranean Conference on Embedded Computing,* 1-4. DOI:10.1109/MECO62516.2024.10577771.

Hopcraft, R. (2021). Developing maritime digital competencies. *IEEE Communications Standards Magazine, 5(3)*, 12-18. Available at: https://doi.org/10.1109/mcomstd.101.2000073.

Ige, A.B., Kupa, E., & Ilori, O. (2024). Best practices in cybersecurity for green building management systems: protecting sustainable infrastructure from cyber threats. *International Journal of Science and Research Archive, 12(01)*, 2960-2977. Available at: https://doi.org/10.30574/ijsra.2024.12.1.1185.

Jacq, O., Boudvin, X., Brosset, D., Kermarrec, Y., & Simonin, J. (2018). Detecting and hunting cyberthreats in a maritime environment: specification and experimentation of a maritime cybersecurity operations centre. *2018 2nd Cyber Security in Networking Conference (CSNet)*, 1-8. Available at: https://doi.org/10.1109/CSNET.2018.8602669.

Kalogeraki, E., Papastergiou, S., Mouratidis, H., & Polemi, N. (2018). A novel risk assessment methodology for SCADA maritime logistics environments. *Applied Sciences, 8(9)*, 1477. Available at: https://doi.org/10.3390/app8091477.

Kamiski, M. (2021). Cyber security requirements for port infrastructure. *Cybersecurity & Cybercrime 1(1)*, 85-99. Available at: https://doi.org/10.5604/01.3001.0053.8012.

Mawer, T., Solms, S.V., & Meyer, J. (2024). Identifying the scope of cybersecurity research conducted in the maritime industry: 2003-2023. *Proceedings of the 19th International Conference on Cyber Warfare and Security, 19(1)*. Available at: https://doi.org/10.34190/iccws.19.1.2037.

Melnyk, O., Onyshchenko, S., Onishchenko, O., Lohinov, O., & Ocheretna, V. (2023). Integral approach to vulnerability assessment of ships critical equipment and systems. *Transactions on Maritime Science, 12(1).* Available at: https://doi.org/10.7225/toms.v12.n01.002.

Progoulakis, I. & Rohmeyer, P. (2021). Cyber physical systems security for maritime assets. *Journal of Marine Science and Engineering, 9(12)*, 1384. Available at: https://doi.org/10.3390/jmse9121384.

Progoulakis, I., Dalaklis, D., & Yaacob, R. (2022). Cyber-physical security for ports infrastructure. *The International Maritime Transport and Logistic Journal, 11*, 105. Available at: https://doi.org/10.21622/marlog.2022.11.105.

Ribeiro, A. (2023, August 13). *Navigating rising storm of maritime cyber threats, as cyber adversaries strike port systems and networks*. Industrial Cyber. Available at: https://industrialcyber.co/features/navigating-rising-storm-of-maritime-cyber-threats-as-cyber-adversaries-strike-port-systems-and-networks/.

Rohan, R.S. (2023). Identifying commonalities of cyberattacks against the maritime transportation system. *Proceedings of the 18th International Conference on Cyber Warfare and Security, 18(1)*. Available at: https://doi.org/10.34190/iccws.18.1.965.

Senarak, C. (2024). Port cyberattacks from 2011 to 2023: a literature review and discussion of selected cases. *Marit Econ Logist, 26,* 105-130. Available at: https://doi.org/10.1057/s41278-023-00276-8.

Tabish, N. & Chaur-Luh, T. (2024). Maritime autonomous surface ships: a review of cybersecurity challenges, countermeasures, and future perspectives. *IEEE Access, 12,* 17114-17136. Available at: https://doi.org/10.1109/ACCESS.2024.3357082.

Vasilescu, A.B. & Preda, M. (2024). Cyber resilience under the EU framework: insights from an applied case study on critical sectors. *International Journal of Information Security and Cybercrime, 13(2), 18-32*. Available at: https://doi.org/10.19107/ijisc.2024.02.02.

Vevera, A.-V., Cîrnu, C.E., & Rădulescu, C.Z. (2022). O abordare multi-criterială pentru calculul unui indicator complex de Securitate Cibernetică și Dezvoltare Digitală. *Revista Română de Informatică și Automatică, ISSN 1220-1758, 32(4),* 19-32. Available at: https://doi.org/10.33436/v32i4y202202.

Weaver, G., Feddersen, B., Marla, L., Wei, D., Rose, A., & Moer, M.V. (2021). Estimating economic losses from cyber-attacks on shipping ports: an optimization-based approach. *Social Science Research Network*. Available at: https://doi.org/10.2139/ssrn.3816659.