Journal of Marine
Technology and Environment
DOI:10.53464/JMTE.03.2026.11

ISSN (Print): 1844-6116
ISSN (Online): 2501-8795
https://www. jmte.eu

CYBERATTACKS ON MARITIME PORT INFRASTRUCTURE: THREAT LANDSCAPE AND RESILIENCE STRATEGIES

Dragoș PĂTRAȘCU[1]

[1] "Alexandru Ioan Cuza" Police Academy, Aleea Privighetorilor 1-3, 014031 Bucharest, Romania

Abstract: Maritime port infrastructure represents one of the most critical and increasingly targeted categories of critical infrastructure in Europe. Ports such as Constanta — Romania's largest seaport and the busiest on the Black Sea — concentrate extensive digital systems managing cargo operations, customs processing, navigation, and supply chain logistics, creating a complex attack surface that adversarial actors have increasingly exploited through ransomware, operational technology attacks, and data breaches. This paper examines the evolving threat landscape facing maritime port infrastructure, analyses the specific vulnerability profiles of port digital systems, and evaluates the resilience frameworks required to protect these critical assets. Drawing on documented incident analysis and the requirements of the EU NIS2 Directive and ISPS Code, the paper proposes a four-layer resilience architecture that addresses governance, detection, protection, and response simultaneously.

Key words: maritime cybersecurity, port infrastructure, ransomware, OT security, NIS2, critical infrastructure.

1. INTRODUCTION

Maritime ports are the backbone of global trade, processing approximately 90% of international cargo by volume and generating economic value that makes them among the highest-priority critical infrastructure assets in any coastal nation. Constanta Port, handling over 60 million tonnes of cargo annually and serving as the primary gateway for Central European trade with the Black Sea and beyond, exemplifies both the economic significance and the cybersecurity exposure of major maritime port facilities. The digital systems that enable modern port operations — cargo management platforms, customs IT systems, SCADA-controlled cranes and loading equipment, vessel traffic management systems, and access control networks — collectively present an attack surface of extraordinary complexity that has attracted growing adversarial attention from both criminal and state-sponsored threat actors [1].

The trajectory of cyberattacks targeting maritime port infrastructure, illustrated in Figure 1, reveals a threat landscape that has intensified significantly since 2019 and accelerated further following Russia's invasion of Ukraine in 2022. Ransomware incidents, data breaches, and operational technology attacks have all grown at rates that exceed the general cybersecurity incident trajectory, reflecting both the increasing attractiveness of port infrastructure as a high-value target and the structural vulnerabilities that legacy operational technology systems create in an environment where cyber threats were not historically considered in system design [2].

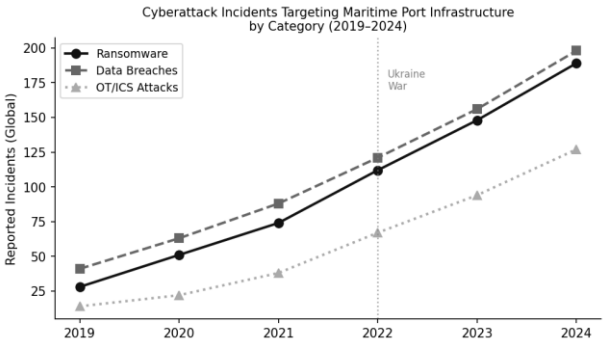


Figure 1 Cyberattack incidents targeting maritime port infrastructure by category (2019–2024). [1]

All three major attack vectors show sustained growth, with OT/ICS attacks showing the steepest relative increase — rising ninefold over the period. [1]

2. DOCUMENTED INCIDENT CASE STUDIES

The empirical record of cyberattacks on port infrastructure provides compelling evidence of both the diversity of threat vectors and the severity of operational consequences that successful attacks can produce. The 2017 NotPetya attack on Maersk — while not targeting port infrastructure directly — caused the shutdown of 17 Maersk port terminals globally, disrupting approximately

Creative Commons Attribution BY 4.0 International Licence (CC BY-4.0)

Journal of Marine
Technology and Environment
DOI:10.53464/JMTE.03.2026.11
ISSN (Print): 1844-6116
ISSN (Online): 2501-8795
https://www. jmte.eu

300 million tonnes of cargo handling capacity and costing an estimated $300 million in recovery costs and lost business. The incident demonstrated the cascading consequence potential of cyberattacks on interconnected maritime logistics systems: a single malware propagation event triggered a global operational paralysis that required weeks to resolve [2].

The 2021 ransomware attack on the Port of Houston provided a closer analogue to the specific threats facing European port infrastructure. Attackers used spear-phishing to gain initial access to the port's IT network, subsequently deploying ransomware that encrypted critical cargo management data and disabled multiple operational systems. While rapid incident response limited the operational impact, the attack revealed the inadequacy of network segmentation between IT and OT environments, which would have prevented malware propagation from administrative systems to operational technology controlling physical port infrastructure [3].

European ports have not been immune. The 2022 cyberattacks targeting oil terminal operators in Belgium, Germany, and the Netherlands — coinciding with the Ukraine conflict's disruption of energy supply chains — demonstrated the potential for geopolitically motivated actors to target maritime logistics infrastructure as an instrument of hybrid warfare. For Constanta Port, whose strategic significance has increased substantially in the context of its role as a transit hub for aid and military supplies to Ukraine, this threat dimension carries particular operational relevance.

3. VULNERABILITY ANALYSIS OF PORT DIGITAL SYSTEMS

Figure 2 presents vulnerability scores and security update rates for six categories of port digital systems, revealing a consistent and concerning pattern: the systems with the highest vulnerability scores — SCADA/ICS (84), communication networks (78), and cargo management (72) — also show the lowest patch and update rates (31%, 44%, and 48% respectively). This inverse relationship reflects the operational constraints of port environments: SCADA and ICS systems controlling physical infrastructure cannot be taken offline for updates during operational hours without disrupting cargo handling, and the extended update cycles that result create accumulating vulnerability exposure that adversaries actively probe [3].

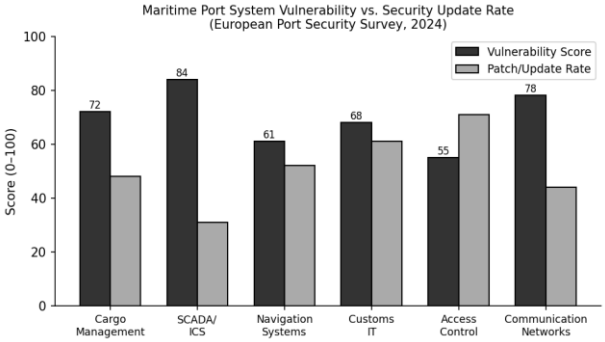


Figure 2 Vulnerability score vs. security update rate for six port system categories. [2]

The inverse relationship — highest-vulnerability systems showing lowest update rates — reflects the operational constraints of port environments and represents the central challenge for port cybersecurity management. [2]

The SCADA/ICS vulnerability profile deserves particular attention given its potential for physical consequence. Unlike IT systems whose compromise typically produces data and operational disruptions, OT system compromise can translate directly into physical damage: compromised crane control systems, manipulated container tracking, falsified weight measurements, or disrupted vessel traffic management can produce consequences ranging from cargo damage to vessel collisions. The 2021 Oldsmar water treatment facility attack — in which an attacker remotely accessed a SCADA system and attempted to increase chemical dosing to dangerous levels — illustrates the physical harm potential of OT system compromise in critical infrastructure contexts [4].

Communication network vulnerabilities create a second critical exposure category. Port operations depend heavily on real-time data exchange between vessels, terminals, customs authorities, and logistics partners, creating extensive network connectivity that expands the attack surface beyond the port's own perimeter. Software-defined radio systems used for vessel communications, AIS transponder networks, and port community systems connecting multiple stakeholders all represent entry vectors through which adversaries can gain initial access to port networks. The vulnerability score of 78 for communication networks combined with a 44% update rate suggests that this attack surface remains inadequately secured in most European port contexts.

4. RESILIENCE FRAMEWORK

Effective cybersecurity for maritime port infrastructure requires a comprehensive resilience architecture that addresses the threat landscape across four integrated layers, as presented in Figure 3. No single-layer approach — whether focused exclusively on technical protection, detection capability, or incident

Creative Commons Attribution BY 4.0 International Licence (CC BY-4.0)

Journal of Marine
Technology and Environment
DOI:10.53464/JMTE.03.2026.11
ISSN (Print): 1844-6116
ISSN (Online): 2501-8795
https://www. jmte.eu

response — can adequately address the complexity and adaptability of the threat actors targeting port infrastructure. The four-layer framework integrates governance, detection, protection, and response into a coherent system in which each layer reinforces the others.

The four-layer architecture ensures that governance requirements drive technical implementation, detection capability enables early threat identification, protection measures reduce attack surface, and response/recovery capabilities minimize harm when attacks succeed. Author's model based on ENISA Port Cybersecurity Guidelines [5].

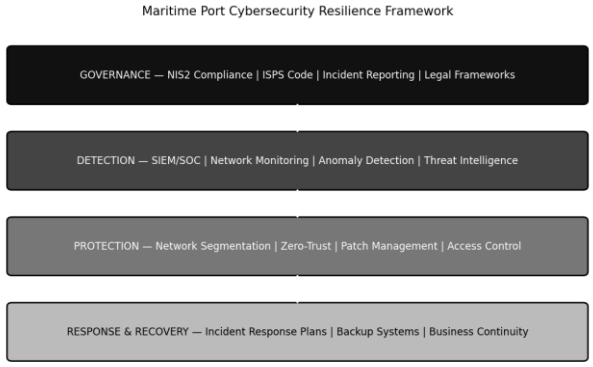


Figure 3 Maritime port cybersecurity resilience framework. [5]

The governance layer establishes the legal and organizational foundation for all other resilience activities. The EU Network and Information Security Directive (NIS2), which entered full application in October 2024 and classifies major maritime ports as essential entities subject to mandatory cybersecurity requirements, provides the primary legal framework. NIS2 requires essential entities to implement appropriate technical and organizational risk management measures, establish incident reporting procedures, and maintain business continuity plans — creating enforceable minimum standards that address the governance deficits historically characteristic of port cybersecurity. The International Ship and Port Facility Security (ISPS) Code provides a complementary framework specifically tailored to maritime security contexts, while the IMO's Maritime Cyber Risk Management guidelines offer operational guidance for vessel and port system risk assessment.

The protection layer translates governance requirements into technical implementation. Network segmentation — creating isolated network zones for IT, OT, and externally connected systems with strict controls on inter-zone traffic — is the single most impactful technical control available for reducing the blast radius of successful intrusions. Zero-trust architecture principles, which eliminate the implicit trust assumptions that allow lateral movement within networks once initial access is achieved, provide a complementary approach particularly valuable for port community systems where multiple external organizations require network access. Patch management programs that accommodate the operational constraints of OT environments — through scheduled maintenance windows, virtual patching, and compensating controls for systems that cannot be updated — address the update rate gap identified in the vulnerability analysis.

5. IMPLICATIONS FOR CONSTANTA PORT AND ROMANIAN CRITICAL INFRASTRUCTURE

Constanta Port's elevated strategic significance in the current security environment — serving as a primary logistics hub for aid and military equipment transiting to Ukraine while simultaneously handling record cargo volumes driven by the rerouting of Black Sea trade — makes it a priority target for both criminal ransomware actors and state-sponsored threat actors with interest in disrupting NATO logistics flows. The port authority's cybersecurity investments must reflect this elevated threat profile, not the baseline risk assessment appropriate for a peacetime commercial port environment.

The Romanian National Directorate of Cyber Security (DNSC) has identified maritime port infrastructure as a priority critical infrastructure category under Romania's NIS2 implementation framework, designating Constanta Port as an essential entity subject to the Directive's enhanced requirements. Compliance with these requirements — including the mandatory risk management measures, incident reporting within 24 hours of significant incidents, and regular security audits — provides the regulatory foundation for resilience development, but effective protection requires investment beyond the minimum legal standard given the specific threat profile that Constanta's strategic position creates [5].

6. CONCLUSIONS

Cyberattacks on maritime port infrastructure represent a growing, increasingly sophisticated, and strategically significant security challenge that demands systematic resilience investment from port operators, national authorities, and their European partners. The combination of high-value operational concentration, legacy OT system vulnerability, complex multi-stakeholder connectivity, and elevated adversarial interest creates a threat environment that incremental security improvements cannot adequately address. The four-layer resilience framework proposed in this paper — integrating governance, detection, protection, and response into a coherent, mutually reinforcing architecture — provides a structured approach to closing

Creative Commons Attribution BY 4.0 International Licence (CC BY-4.0)

Journal of Marine
Technology and Environment
DOI:10.53464/JMTE.03.2026.11
ISSN (Print): 1844-6116
ISSN (Online): 2501-8795
https://www. jmte.eu

the most critical vulnerability gaps identified in the European port cybersecurity landscape. For Constanta Port and Romanian critical infrastructure authorities, the urgency of this investment is compounded by the current geopolitical environment: the window for orderly resilience development before a significant incident occurs may be shorter than comfortable planning timelines allow.

7. CREdit authors statement

Conceptualization: P.D.; Data curation: P.D.; Formal analysis: P.D.; Funding acquisition: not applicable; Investigation: P.D.; Methodology: P.D.; Project administration: P.D.; Resources: P.D.; Software: not applicable; Supervision: not applicable; Validation: P.D.; Visualization: P.D.; Writing – original draft: P.D.; Writing – review & editing: P.D..

8. REFERENCES

[1] European Union Agency for Cybersecurity (ENISA). Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector. ENISA, Athens, 2024.

[2] A. P. Dyryaviy. “NotPetya and its Impact on Maritime Logistics: Lessons Learned.” Journal of Cybersecurity, vol. 4, no. 1, pp. 1–18, 2018.

[3] BIMCO and INTERCARGO. The Guidelines on Cyber Security Onboard Ships. Version 4. BIMCO, Copenhagen, 2023.

[4] NATO Cooperative Cyber Defence Centre of Excellence. Cyber Threats to Maritime Critical Infrastructure. CCDCOE, Tallinn, 2023.

[5] Direcția Națională de Securitate Cibernetică. Ghid de securitate cibernetică pentru infrastructura critică maritimă. DNSC, București, 2024.

[6] C. Bueger and T. Edmunds. “Beyond Sea Blindness: A New Agenda for Maritime Security.” International Affairs, vol. 93, no. 6, pp. 1293–1311, 2017.

Creative Commons Attribution BY 4.0 International Licence (CC BY-4.0)