Cybersecurity Recommendations for Planning and Securing Port 4.0 and Maritime Industry against Cyberattacks

Nitesh Bharot*, Priyanka Verma†, Rutvij H. Jhaveri‡, John G. Breslin*
*Insight Research Irealnd Centre for Data Analytics, University of Galway, Galway, Ireland
†School of Computer Science, University of Galway, Galway, Ireland
‡Department of Computer Science and Engineering, Pandit Deendayal Energy University, Gandhinagar, India

2025 IEEE 12th International Conference on Data Science and Advanced Analytics (DSAA) | 979-8-3315-1179-1/25/$31.00 ©2025 IEEE | DOI: 10.1109/DSAA65442.2025.11248031

***Abstract*—The global maritime industry is undergoing a digital transformation driven by the Fourth Industrial Revolution, which gives rise to "smart ports" or "Port 4.0" environments. These ports leverage smart technologies, and thus increase exposure to cyber threats that have seen dramatic growth in recent years. This paper presents four key contributions to strengthen cybersecurity in smart Port ecosystems. First, it maps the current cyber-threat landscape across both Information Technology (IT) and Operational Technology (OT) systems used in the smart Port environment, highlighting critical vulnerabilities. Then, it analyzes existing regulatory and standard frameworks such as the International Maritime Organization (IMO) guidelines, ISO/IEC 27001, and the National Institute of Standards and Technology (NIST) cybersecurity framework, identifying alignment gaps with maritime operational realities. Further, this paper also provides structured, Port-specific cybersecurity recommendations tailored to the complex interplay of legacy OT systems and modern digital technologies. Finally, the paper discusses AI-assisted cybersecurity solutions available in the literature, highlighting how advanced AI-based analytics, predictive modeling, and automated incident response can be incorporated. The insights presented are intended to help Port authorities build resilient, adaptive cybersecurity postures in an increasingly interconnected maritime domain.**

***Index Terms*—Maritime, Port 4.0, Cybersecurity, AI, IT, OT, IoT, Security recommendations**

I. Introduction

In the wake of the Fourth Industrial Revolution, the global maritime transportation industry has entered an era defined by unprecedented digitalization and interconnectivity [1]. From the integration of Internet of Things (IoT) sensors on container cranes to cloud-based terminal operating systems, ports have embraced the nine pillars of Industry 4.0 autonomous robots, big data analytics, horizontal and vertical systems integration, and more to forge so-called "Port 4.0" or "smart Port" environments [2]. While these advances have driven significant gains in operational efficiency, throughput, and real-time responsiveness, they have also widened a "digital divide" among Port facilities worldwide, creating disparate levels of maturity in both technological adoption and cyber-resilience [3].

Regardless of a Port's position on this digital spectrum, the very convergence of Information Technology (IT) and Operational Technology (OT) in increasingly complex, networked ecosystems has amplified its exposure to cyber risk [4]. Recent industry reports indicate that phishing campaigns, the exploitation of unpatched Internet facing infrastructure, and targeted attacks on OT controllers have surged, with a four-fold increase in overall incidents and a 900% rise in OT specific compromises over a three-year period [5]. These trends underscore a stark reality: no Port, however "smart", can afford to overlook cybersecurity as a core element of operational resilience.

Port authorities occupy a uniquely critical role in the maritime ecosystem. They not only orchestrate the safe and efficient movement of goods, but also serve as the nexus for multiple stakeholders including terminal operators, shipping lines, customs agencies, and hinterland transport providers whose systems and processes are deeply interwoven. A single successful cyber-attack against a Port authority's network or control system can cascade through this ecosystem, triggering disruptions in global supply chain, eroding stakeholder trust, and imposing severe economic and reputational cost [6].

Against this backdrop, there is an urgent imperative for Port authorities to develop, adopt, and continuously refine a set of cybersecurity recommendations tailored specifically to maritime applications [7]. These guidelines must bridge the gap between high level standards such as the International Maritime Organization (IMO) [8] to integrate cyber risk into Safety Management Systems, ISO/IEC 27001 [9], and NIST's Cybersecurity Framework [10] and the practical realities of Port operations, where legacy OT equipment, complex third-party software environments, and 24/7 operational demands often collide. The major contribution of this paper are:

- Map the cyber-threat landscape affecting modern Port environments, with a focus on both IT and OT

centric attack vectors in Port 4.0.
- Assess regulatory and standard frameworks, identifying areas of alignment and divergence among IMO, ISO, NIST, and industry-specific guidelines (e.g., BIMCO, MTS-ISAC).
- This research also contributes to structured cybersecurity recommendations, specifically designed to address the complex interplay between Operational Technology (OT) and Information Technology (IT) systems in modern smart Port and Maritime Industry.
- This work also discusses some of the AI-assisted cybersecurity solution which could be utilized in Port 4.0 environment. By integrating advanced data analysis, predictive modeling, and automated incident response mechanisms, will help in addressing the emerging cyberattack challenges associated with interconnected Port and Maritime Industry.

The rest of the paper is organized as: Section II presents the need for cybersecurity awareness in the Port and Maritime Industry, while Section III discusses the cyber-threat landscape. Section IV shows the analysis of regulations and standards related to cybersecurity, followed by section V presenting security recommendations in the Port and Maritime Industry. Finally section VI discusses the AI assisted solutions to secure ports against cyberattacks, and section VII concludes the paper.

II. Need for Heightened Cybersecurity Awareness in Port and Maritime Industry

Ports and terminals have become prime targets for cyber-attackers due to their status as critical infrastructures supporting global trade. Their highly interconnected systems and the severe consequences of a breach can inflict not only locally but throughout supply chains. Some of the major reasons highlighting the need for cybersecurity awareness in Port 4.0 and Maritime Industry are:

- Ports as Critical Infrastructure: Seaports and terminals are categorized alongside transport, energy, and telecommunications networks as national critical infrastructures, making them attractive targets for criminal groups and terrorism-oriented actors seeking high impact disruptions.
- Global Cascading Effects: A successful cyber-attack on a single terminal can rapidly propagate through electronic data-exchange networks and Port Community Systems (PCS) [11], causing delays and revenue losses across multiple ports and shippers worldwide.
- Vulnerable Cyber-Physical Systems: Modern terminals rely heavily on integrated IT, OT, and CPS/IIoT platforms ranging from automated cranes to wireless sensor networks, which broaden the attack surface and expose critical operational controls to remote exploitation.
- People and Device-Driven Entry Points: Thousands of mariners and Port workers connect personal laptops, tablets, and USB drives to both shipboard and shore networks, unwittingly providing malware vectors and credential-phishing gateways that can traverse into control rooms without robust segmentation or monitoring.
- Erosion of Cyber Resilience Attributes: Cyberattacks degrade the ability of ports to maintain data integrity, confidentiality, and availability, undermining billing systems, cargo manifests, safety alarms, and emergency response plans, compromising both operational continuity and personnel safety.
- Diverse Adversary Motivations: Beyond financial extortion, adversaries range from hacktivists and industrial spies to nation-state actors seeking espionage or strategic disruption, each employing evolving tactics that demand adaptive, multi-layered defense postures [12].

Collectively, these factors underscore why Port authorities and terminal operators must elevate cybersecurity from a technical afterthought to a board-level priority integrating threat intelligence, risk assessments, and cross-sector collaboration into every aspect of Port management.

III. Cyber-Threat Landscape in Port and Maritime Industry

As Port authorities embrace digital transformation and increasingly integrate IT, OT, and IIoT domains, they confront a multifaceted and rapidly evolving cyber-threat landscape. The convergence of these domains, while enabling efficiency and automation, also introduces systemic vulnerabilities that adversaries are keen to exploit. This section provides a structured analysis of key cyber-attack vectors across IT and OT layers, emerging threat trends, to Port ecosystems. Table I presents the summary of cyber threat attack vectors and mitigation in Port and Maritime Industry.

A. IT-Centric Attack Vectors

- Phishing and Social Engineering: Spear phishing campaigns frequently target administrative and operational personnel by leveraging contextual triggers, such as berth schedules or customs regulations, to extract credentials for corporate VPNs and cloud services. In parallel, Business Email Compromise (BEC) attacks are increasingly observed, wherein attackers impersonate Port executives or logistics vendors to initiate unauthorized financial transfers [17].

TABLE I
CYBERATTACK VECTORS AND MITIGATIONS IN PORT 4.0 AND MARITIME INDUSTRY

Attack Vector	Techniques / Examples	Consequences	High-Level Mitigations
IT-Centric	• Spear-phishing → credential theft • Exposed VPN/RDP endpoints • Injection flaws in PCS/TOS web apps	• Unauthorized network access • Data exfiltration • Fraudulent payments	• MFA & least-privilege [10] • Web-app WAFs & secure coding [9] • EDR & SIEM [13]
OT-Centric	• Legacy PLC exploits • Modbus/OPC-UA replay attacks • Wireless jamming of AGV controls	• Equipment malfunctions • Safety incidents • Environmental spills	• Zones-and-conduits segmentation [14] • OT-aware IDS/IPS [15] • Firmware patching
Supply-Chain / Third Party	• Vendor-access VPN compromise • Malicious code in TOS/PCS updates • Counterfeit IoT sensors	• Persistent backdoors • Lateral movement • Data integrity loss	• Vendor security SLAs & attestations [16] • Jump-servers for maintenance • Code-signing and device validation
Emerging Techniques	• Ransomware-as-a-Service (RaaS) • APT footholds in both IT/OT layers • AI-driven network mapping	• Prolonged downtime • High ransom demands • Stealthy reconnaissance	• Threat-intelligence sharing [13] • Anomaly detection & UEBA • Regular tabletop exercises

- Remote Access Vulnerabilities: Unsecured Remote Desktop Protocol (RDP) endpoints and VPN gateways, often deployed for vendor access or remote maintenance, remain frequent entry points due to poor segmentation and lack of multi-factor authentication. Misconfigured cloud assets such as exposed storage containers or overly permissive Identity and Access Management (IAM) roles have also led to data breaches and privilege escalations [18].
- Web and API Exploits: Web-facing services, including PCS and cargo-tracking platforms, are susceptible to injection attacks (e.g., SQLi, XSS), while broken authentication in mobile APIs can permit unauthorized access to sensitive shipment data and operational parameters.

B. OT-Centric Attack Vectors

- ICS and PLC Weaknesses: Many Port infrastructures still rely on legacy Programmable Logic Controllers (PLCs) with unpatched firmware and outdated operating systems, exposing known vulnerabilities (e.g., CVEs). Moreover, insufficient network segmentation between enterprise IT and control systems enables lateral movement by adversaries once initial access is gained [19].
- Protocol Exploits and Fieldbus Manipulation: Ports employing Modbus/TCP or OPC-UA protocols are susceptible to replay and man-in-the-middle (MitM) attacks, allowing adversaries to inject false telemetry or malicious actuation commands. Denial-of-service (DoS) scenarios have also been observed on control buses, directly impacting crane operations or water-lock systems.
- Wireless and AGV Exploits: Emerging threats target Autonomous Guided Vehicles (AGVs) and Unmanned Aerial Systems (UAS) through GPS spoofing and RF jamming, causing operational disruptions. The planned adoption of 5G-enabled private networks, if not configured with robust network slicing, may further expose OT traffic to external interception [20].

C. Supply Chain and Third Party Risks

- Vendor Access Abuse: Third party vendors, particularly equipment Original Equipment Manufacturer (OEM), are granted persistent VPN tunnels for firmware updates. Without stringent monitoring, these channels can serve as direct conduits into critical networks when vendor credentials are compromised. In some incidents, attackers have embedded persistent backdoors within legitimate vendor software packages.
- Component Tampering and Transitive Trust: Software supply chain risks are heightened by the potential insertion of malicious code during the development or delivery of PCS modules [22]. Similarly, counterfeit IoT devices deployed in sensor networks may generate corrupted telemetry, undermining situational awareness. The shared authentication infrastructure, such as Singlw Sign Out (SSO) portals used across customs, logistics firms, and Port authorities, introduces a transitive risk,

TABLE II
COMPARISON OF STANDARDS AND GUIDELINES FOR CYBERSECURITY IN PORT 4.0 AND MARITIME INDUSTRY

Standard/Guideline	Governance & Policy	Risk Assessment	Network Segmentation	Incident Response	OT-Tailored Controls
IMO MSC.428(98) [8]	✓	×	×	✓	×
ISO/IEC 27001 [9]	✓	✓	×	✓	×
ISO/IEC 62443 [14]	✓	✓	✓	✓	✓
NIST CSF [10]	✓	✓	✓	✓	×
BIMCO/INTERTANKO [21]	✓	×	×	✓	×
MTS-ISAC [13]	×	✓	×	✓	×

whereby compromise of one partner can jeopardize the entire ecosystem [23].

D. Emerging Threat Techniques

Recent threat intelligence reveals a marked increase in the commoditization of ransomware (Ransomware-as-a-Service, RaaS), enabling financially motivated actors to mount disruptive attacks against Port systems. State-backed Advanced Persistent Threats (APTs) are also embedding long term footholds to surveil critical infrastructure or vessel movement patterns. Furthermore, adversaries are beginning to leverage AI-driven tools for reconnaissance, enabling dynamic mapping of network topologies and optimization of attack timing.

IV. REGULATORY AND STANDARD ANALYSIS FOR SECURING PORT 4.0 AND MARITIME INDUSTRY

This section presents a comprehensive regulatory and standard frameworks that have been established, encompassing international mandates, industry-specific guidelines, and best practices in Port and Maritime Industry. A comparison and summary of these standards is shown in Table II.

A. International Maritime Organization

IMO Resolution MSC.428(98) [8] requires that cyber risks be incorporated into Safety Management Systems (SMS) by January 1, 2021, emphasizing the integration of cybersecurity within existing safety frameworks in line with the International Safety Management (ISM) Code [24]. This mandate strengthens management accountability for cybersecurity and facilitates integration by aligning with established ISM processes. However, it lacks specific cybersecurity controls, detailed implementation guidelines, and prescribed audit mechanisms to verify compliance. Failure to adequately manage cyber risks may result in the denial of a Document of Compliance (DoC, potentially preventing vessels from operating commercially.

B. ISO/IEC 27001 and ISO/IEC 62443

ISO/IEC 27001 [9] and ISO/IEC 62443 [14] provide comprehensive frameworks for managing cybersecurity in IT and OT domains, respectively. ISO/IEC 27001 outlines the requirements for establishing an Information Security Management System (ISMS), focusing on protecting sensitive company data through confidentiality, integrity, and availability measures (CIA traid) ISO/IEC 62443, on the other hand, addresses the cybersecurity needs of Industrial Automation and Control Systems (IACS), making it particularly relevant for Operational Technology (OT) in ports. It covers the entire security lifecycle, from risk assessment to network segregation, and defines specific roles for asset owners, system integrators, and suppliers. While both standards promote defense-in-depth strategies, implementation can be complex, resource-intensive, and requires substantial coordination among diverse stakeholders.

C. NIST Cybersecurity Framework (CSF)

The NIST Cybersecurity Framework (CSF) [10] provides a structured policy framework to help private sector organizations assess and improve their capabilities to prevent, detect, and respond to cyber threats. Organized into five core functions: Identify, Protect, Detect, Respond, and Recover. CSF is adaptable across industries, including maritime. The updated CSF 2.0, includes enhanced guidance on supply chain security and identity management. While it promotes continuous improvement and flexible risk management, it requires customization to address the specific needs of Port OT environments and lacks prescriptive controls, leaving organizations to define specific measures.

D. Industry-Specific Guidelines

Baltic and International Maritime Council (BIMCO) and INTERTANKO [25] have developed best practices aimed at enhancing cybersecurity in ship-to-shore interfaces and vendor management, addressing the maritime sector's specific challenges. The Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC) [13] further supports cybersecurity by serving

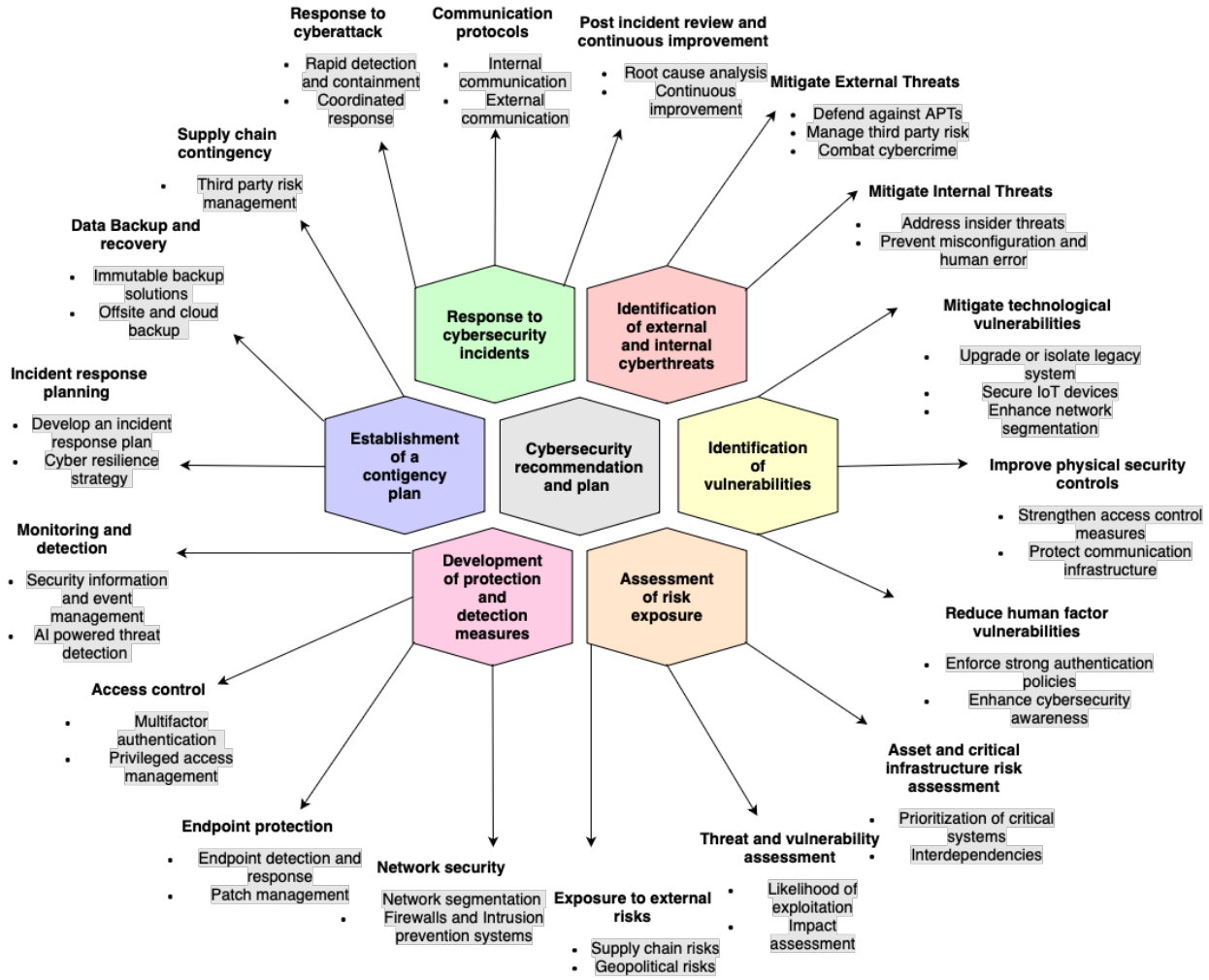

Fig. 1. Cybersecurity recommendation and plan for Port 4.0 and Maritime industry

as a centralized platform for sharing real-time cyber threat intelligence among maritime stakeholders, fostering public-private collaboration to strengthen cyber risk management. While these initiatives promote situational awareness and sector-wide coordination, participation in MTS-ISAC is voluntary, potentially resulting in inconsistent adoption, and its effectiveness relies heavily on the timely and accurate sharing of threat information by participants.

V. Cybersecurity Recommendation and Plan for Port 4.0 and Maritime Industry

In 2016, the BIMCO, the International Chamber of Shipping (ICS), INTERCARGO, INTERTANKO, and the Cruise Lines International Association (CLIA) published the "Guidelines on Cybersecurity Onboard Ships" [21]. As shown in Fig. 1 cybersecurity recommendation framework follows a six-step process designed to be iterative and adaptive. It begins with the identification of threats and vulnerabilities, both external (e.g., APTs, supply chain abuse) and internal (e.g., insider threats, human error). These feed into a structured risk assessment, where critical assets and interdependencies are prioritized. Based on the risk profile, ports then develop protection and detection measures, including segmentation, endpoint security, and continuous monitoring. To ensure resilience, a contingency plan is established, covering backups, redundancy, and supply chain continuity. When incidents occur, the framework provides guidance for response and coordinated communication, minimizing disruption and reputational damage. The process concludes with post-incident review and continuous improvement, feeding insights back into threat identification and keeping defenses dynamic. In practice, each block connects to the next, creating a closed-loop system of continuous security enhancement for port operations.

These guidelines provide a structured framework that can be adopted to ensure robust cybersecurity practices, not only on ships but across maritime infrastructure, including ports. In the context of Port 4.0, where advanced technologies such as IoT, AI, and automation are integrated, applying this six-step approach is critical to maintaining a secure, resilient Port environment.

The below cybersecurity recommendations are major based on the points published in the guidelines given in [21]. This will help strengthen the cybersecurity posture of the Port, mitigate risks, and ensure business continuity in the face of evolving cyber threats.

A. Identification of External and Internal Cyber Threats

1) Mitigate External Threats
   - Defend Against APTs: Implement network segmentation, Intrusion Detection Systems (IDS), and continuous monitoring to identify and respond to sophisticated threats such as phishing, DDoS, and MITM attacks targeting communication and operational networks.
   - Manage Third-Party Risk: Enforce rigorous security assessments, contract-based cybersecurity requirements, and continuous monitoring of vendors, contractors, and service providers to minimize vulnerabilities introduced via the supply chain.
   - Combat Cybercrime: Establish robust backup and recovery protocols, apply regular security patches, and deploy endpoint protection to prevent ransomware, data breaches, and financial fraud perpetrated by organized cybercriminal groups.
2) Mitigate Internal Threats
   - Address Insider Threats: Implement strict access controls, role-based permissions, and user activity monitoring to detect and prevent unauthorized or suspicious behavior by employees or contractors. Establish clear policies and provide regular cybersecurity awareness training to reduce the risk of intentional misuse or inadvertent compromise. Insider threat programs should include both technical controls and behavioral indicators.
   - Prevent Misconfiguration and Human Error: Enforce secure configuration baselines and regularly audit systems for compliance. Use automated configuration management tools to reduce manual errors, and establish change control procedures for all system updates. Promote a security-conscious culture through continuous training on best practices, including secure password management, phishing recognition, and safe data handling.

B. Identification of Vulnerabilities

1) Mitigate Technological Vulnerabilities
   - Upgrade or Isolate Legacy Systems: Conduct regular asset inventories to identify outdated systems and prioritize upgrades or isolation strategies. Apply virtual patching and network segmentation to limit exposure when full system replacement is not feasible.
   - Secure IoT Devices: Implement strong authentication mechanisms and encryption for all IoT devices, including sensors and automated equipment. Ensure regular firmware updates, disable unnecessary services, and isolate IoT networks from core operational systems.
   - Enhance Network Segmentation: Design and enforce robust network segmentation between IT and OT environments. Use firewalls, VLANs, and demilitarized zones to limit lateral movement in case of a breach and ensure continuous monitoring of cross-network traffic.
   - Practical Integration with Minimal Disruption: Full replacement of legacy OT systems is often infeasible due to cost and downtime. A layered defense strategy combining virtual patching, zones-and-conduits segmentation, OT-aware intrusion detection, and controlled isolation, offers an incremental, minimally disruptive, and effective transitional solution. This approach aligns with ISO/IEC 62443 and has been validated in early port security initiatives, demonstrating improved resilience without interrupting operations.
2) Improve Physical Security Controls
   - Strengthen Access Control Measures: Deploy multi-layered physical security controls such as biometric access, RFID badge systems, and surveillance for critical infrastructure zones. Regularly audit access logs and enforce strict visitor and contractor access policies.
   - Protect Communication Infrastructure: Ensure that all operational communication lines use encrypted protocols (e.g., TLS, VPN) and secure routing. Replace outdated or unencrypted systems to prevent data interception or tampering.
3) Reduce Human Factor Vulnerabilities
   - Enforce Strong Authentication Policies: Mandate complex passwords, implement Multi-Factor Authentication (MFA), and restrict access based on roles and responsibilities. Use centralized IAM systems to monitor credentials.
   - Enhance Cybersecurity Awareness: Launch continuous training programs for all personnel on cybersecurity threats, phishing, social engineering, and incident reporting. Integrate simulated

attack exercises to test and reinforce employee preparedness.

C. Assessment of Risk Exposure

1) Asset and Critical Infrastructure Risk Assessment
   - Prioritization of Critical Systems: Assess the importance of various assets (e.g., cargo management systems, SCADA systems) and evaluate the consequences of their potential failure or compromise.
   - Interdependencies: Identify how systems within the Port are interdependent, considering both IT and OT systems, to understand the cascading effects of vulnerabilities in one system impacting another.
2) Threat and Vulnerability Assessment
   - Likelihood of Exploitation: Evaluate the likelihood of identified cyber threats exploiting vulnerabilities based on current security controls. This includes penetration testing and vulnerability scanning.
   - Impact Assessment: Assess the potential impact on Port operations, reputation, and financial losses if a threat exploits vulnerabilities. This should consider disruption to cargo operations, data loss, and potential safety hazards.
3) Exposure to External Risks
   - Supply Chain Risks: Assess third-party risk and vulnerabilities arising from supply chain integrations. Ensure that cybersecurity measures extend to external vendors and service providers.
   - Geopolitical Risks: Evaluate the risk of cyberattacks from geopolitical tensions, particularly threats to Port infrastructure related to national security concerns.

D. Development of Protection and Detection Measures

1) Network Security
   - Network Segmentation: Implement Zero Trust Architecture (ZTA) with strict access control measures. Use network segmentation to isolate critical OT systems (e.g., cargo handling systems) from general IT infrastructure.
   - Firewalls and Intrusion Prevention Systems (IPS): Deploy next-generation firewalls (NGFW) and IPS solutions across all network layers to block unauthorized traffic and detect potential breaches.
2) Endpoint Protection
   - Endpoint Detection and Response (EDR): Deploy advanced EDR solutions across critical endpoints, including IoT devices, sensors, and industrial control systems (ICS), to detect anomalous behavior and potential cyber threats.
   - Patch Management: Regularly apply security patches and updates to all devices, particularly legacy systems that may be vulnerable to exploitation.
3) Access Control
   - Multi-Factor Authentication (MFA): Enforce MFA for all employees accessing critical systems, especially in control rooms, cargo handling, and security management systems.
   - Privileged Access Management (PAM): Use PAM tools to control and audit access to high-level systems, limiting the ability of unauthorized users to gain access to sensitive areas of the Port infrastructure.
4) Monitoring and Detection
   - Security Information and Event Management (SIEM): Implement a SIEM system for continuous monitoring of all network traffic, alerting security teams to unusual patterns or potential breaches.
   - AI-Powered Threat Detection: Integrate AI-based threat detection to identify potential attacks in real time and enhance detection capabilities for complex and evolving threats.

E. Establishment of Contingency Plan

1) Incident Response Planning
   - Develop an Incident Response Plan: Establish a comprehensive plan that includes roles, responsibilities, and communication procedures for responding to different types of cyber incidents (e.g., DDoS, ransomware, data breach).
   - Cyber Resilience Strategy: Build redundancy into critical systems (e.g., backup power systems, redundant network paths) to ensure business continuity in case of a cyberattack.
2) Data Backup and Recovery
   - Immutable Backup Solutions: Implement immutable backups for critical data, ensuring that data cannot be deleted or modified by cyber actors during a ransomware attack.
   - Offsite and Cloud Backup: Maintain offsite and cloud-based backups to protect data from local or regional threats.
3) Supply Chain Contingency
   - Third-Party Risk Management: Ensure that external vendors and third-party providers have contingency plans for cybersecurity incidents, including incident notification protocols, response time, and mitigation procedures.

F. Response to Cybersecurity Incidents

1) Response to Cyberattacks
   - Rapid Detection and Containment: Implement automated detection and containment protocols for immediate response to cybersecurity threats. This includes isolating affected systems, cutting off attack vectors, and preventing the spread of malware.
   - Coordinated Response: Establish a well-coordinated response team involving internal and external stakeholders (e.g., legal, law enforcement, IT support) to respond effectively and mitigate damage.
2) Communication Protocols
   - Internal Communication: Ensure clear and timely communication with all internal stakeholders, such as Port operators, security personnel, and executive management, during an incident.
   - External Communication: Have predefined templates for communicating with external stakeholders, including customers, regulators, and third-party vendors, to manage public relations and maintain transparency.
3) Post-Incident Review and Continuous Improvement
   - Root Cause Analysis: After an incident, conduct a detailed post-incident analysis to determine the root cause, understand gaps in the current security posture, and identify areas for improvement.
   - Continuous Improvement: Regularly update the incident response plan and security protocols based on lessons learned and new threat intelligence.

The proposed recommendations are scalable and adaptable, enabling both advanced and resource-constrained ports to strengthen their cybersecurity posture. Larger ports can adopt AI-driven monitoring and Zero Trust frameworks, while smaller ports may begin with essential measures such as segmentation, access control, and awareness training. This layered, modular approach ensures improvements remain achievable and cost-effective across diverse operational contexts. Grounded in both Industry 4.0 principles and the practical realities of port management, the framework offers a pragmatic roadmap to enhance resilience, close digital divides, and safeguard global trade.

VI. AI-assisted cybersecurity solution for the Port 4.0 and Maritime Industry

By integrating AI solutions for incident response strategies, and monitoring techniques, Port authorities can significantly strengthen the security of Port 4.0 environments and reduce the risk posed by cyberattacks. Some of the possible ways to integrate AI for defence against cyberattacks are discussed below:

The emergence of Port 4.0 leverages advanced digital systems, IoT devices, and AI technologies to optimize Port operations. While these advancements significantly enhance operational efficiency, they also introduce increased cybersecurity risks. Robust AI-assisted cybersecurity solutions are essential to safeguard critical infrastructure, prevent data breaches, and mitigate potential threats in Port 4.0 environments [26].

To further enhance incident response capabilities, automated tools such as CTIMiner [27] can be integrated to gather real-time threat intelligence, facilitating rapid detection and response to emerging threats. CTIMiner leverages AI algorithms to identify indicators of compromise (IoCs) and generate actionable insights, thus accelerating incident response efforts and minimizing potential damage.

Continuous monitoring is equally critical in detecting evolving threats within Port 4.0 systems. Data mining techniques, as explored by Tsai et al. [28], can be utilized to analyze network traffic and device logs, identifying abnormal patterns that may signal security breaches. By implementing such data analysis methods, ports can detect potential threats early and initiate appropriate countermeasures.

Furthermore, predictive models proposed by Soldo et al. [29] can be integrated to anticipate potential threats by analyzing historical attack patterns and clustering data. These models can forecast likely attack vectors, allowing security teams to proactively adjust defenses and allocate resources effectively.

Recommendation systems like MENTOR [30] provide another layer of security enhancement. By assessing factors such as region, deployment time, and cost, MENTOR guides the selection of appropriate protection services, ensuring that security investments align with the specific needs and risk profile of each Port. This targeted approach enables ports to deploy optimal security controls while maintaining cost-effectiveness and operational efficiency.

A. Validation and Practical Considerations

While AI-assisted cybersecurity solutions hold great promise for Port 4.0, their effectiveness must be validated in real-world contexts before large-scale adoption. Current research and industry practice suggest multiple approaches for ensuring practical reliability:

- Pilot Deployments in Ports: Several smart port initiatives, such as those in Rotterdam and Singapore, have begun integrating AI-driven monitoring and anomaly detection tools. These trials demonstrated measurable improvements in incident detection and

response times, indicating the feasibility of deploying AI-assisted defense in operational maritime environments [4], [22].

- Cyber Range and Testbed Validation: Because replicating live cyberattacks in operational ports is impractical and risky, many researchers validate solutions using maritime-specific cyber ranges and digital twin environments, such as the MARSec-COE testbeds and EU Horizon-funded maritime cyber ranges [7], [19]. These platforms safely simulate attack vectors—including phishing, ransomware, and OT-protocol exploits—providing evidence of detection accuracy and system resilience.
- Benchmark Datasets and Simulation: AI models for intrusion detection and predictive threat modeling are often evaluated using publicly available datasets such as UNSW-NB15, CICIDS2017, and maritime/ICS traffic traces [27], [31], [32]. Although not always maritime-specific, these datasets support benchmarking of detection rates, false positives, and predictive accuracy, helping to refine models prior to port-specific adaptation.
- Hybrid Validation Approach: An effective validation strategy combines cyber-range testing with limited pilot deployments in selected port subsystems. This enables gradual scaling of AI-assisted solutions while monitoring performance against key indicators such as detection accuracy, false alarm rates, and response latency [26], [29].
- By grounding validation in both controlled environments and operational pilots, Port authorities can ensure that AI-assisted cybersecurity solutions are not only theoretically effective but also resilient under the complex and dynamic conditions of real-world maritime operations.

While AI-assisted cybersecurity offers powerful capabilities for detection and response, there are also risks of overreliance that must be acknowledged. Adversarial attacks, such as data poisoning or evasion techniques, can exploit vulnerabilities in AI models, while algorithmic bias may lead to false positives or missed threats. Therefore, AI should serve as a complement to human expertise and traditional defense-in-depth strategies, not a standalone solution. Continuous validation, adversarial robustness testing, and hybrid human-in-the-loop approaches are essential to ensure that AI systems remain reliable, explainable, and resilient against evolving cyber risks.

VII. Conclusion

This paper underscores the urgent need for robust cybersecurity measures in the maritime sector as it embraces digital transformation. It emphasizes the integration of cyber risk management into existing safety frameworks, as mandated by the IMO, while also highlighting the necessity for tailored cybersecurity recommendations that address the unique challenges of Port and Maritime Industry. The paper further analyzes existing standards and guidelines while also providing structured cybersecurity recommendations, inclusive of the "Guidelines on Cybersecurity Onboard Ships." Additionally, this paper discusses the role of AI in Port 4.0 by highlighting AI-assisted solutions for anomaly detection, predictive threat modeling, and automated incident response. Importantly, the effectiveness of these AI-assisted solutions must be validated through pilot deployments, cyber-range testbeds, and benchmark datasets, ensuring their reliability in operational contexts. While large-scale real-world deployments remain limited due to safety and resource constraints, early trials in leading smart ports and maritime testbeds demonstrate promising outcomes. Future work will focus on collaborative efforts with port authorities and industry stakeholders to implement controlled pilot studies, refine validation methods, and ultimately scale AI-assisted cybersecurity solutions across diverse port ecosystems.

By combining practical validation with continuous adaptation, Port 4.0 environments can achieve a resilient, adaptive cybersecurity posture that safeguards global maritime trade against emerging threats.

Acknowledgment

This work was supported in part by Interreg Atlantic Area co-funded by the European Union under grant EAPA_0016/2022 (ENEPORTS) and Taighde Éireann - Research Ireland under grants 12/RC/2289_P2 (Insight). For the purpose of Open Access, the author has applied a CC BY public copyright licence to any Author Accepted Manuscript version arising from this submission.

References

[1] M. Shahbakhsh, G. R. Emad, and S. Cahoon, "Industrial revolutions and transition of the maritime industry: The case of seafarer's role in autonomous shipping," *The asian journal of shipping and logistics*, vol. 38, no. 1, pp. 10–18, 2022.

[2] B. Behdani, "Port 4.0: A conceptual model for smart port digitalization," *Transportation Research Procedia*, vol. 74, pp. 346–353, 2023.

[3] P. Verma, T. Newe, G. D. O'Mahony, D. Brennan, and D. O'Shea, "Towards a unified understanding of cyber resilience: A comprehensive review of concepts, strategies, and future directions," *IEEE Access*, 2025.

[4] I. Progoulakis, N. Nikitakos, D. Dalaklis, A. Christodoulou, A. Dalaklis, and R. Yaacob, "Digitalization and cyber physical security aspects in maritime transportation and port infrastructure," in *Smart ports and robotic systems: Navigating the waves of techno-regulation and governance*, pp. 227–248, Springer, 2023.

[5] Safety4Sea, "Cyber attacks on maritime ot systems increased 900% in last three years," 2020. Accessed: 2025-05-12.

[6] M. Ammar and I. A. Khan, "Cyber attacks on maritime assets and their impacts on health and safety aboard: A holistic view," *arXiv preprint arXiv:2407.08406*, 2024.

[7] M. A. Ben Farah, E. Ukwandu, H. Hindy, D. Brosset, M. Bures, I. Andonovic, and X. Bellekens, "Cyber security in the maritime industry: A systematic survey of recent advances and future trends," *Information*, vol. 13, no. 1, p. 22, 2022.

[8] International Maritime Organization, "Resolution msc.428(98): Maritime cyber risk management in safety management systems." https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution Adopted on 16 June 2017.

[9] International Organization for Standardization, "ISO/IEC 27001:2018 — Information technology — Security techniques — Information security management systems — Requirements." https://www.iso.org/standard/54534.html, 2018. Available at: https://www.iso.org/standard/54534.html.

[10] C. I. Cybersecurity, "Framework for improving critical infrastructure cybersecurity," *URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP*, vol. 4162018, no. 7, 2018.

[11] V. Caldeirinha, J. A. Felício, A. S. Salvador, J. Nabais, and T. Pinho, "The impact of port community systems (pcs) characteristics on performance," *Research in Transportation Economics*, vol. 80, p. 100818, 2020.

[12] P. M. Beaumont and S. Wothusen, "Cyber-risks in maritime container terminals: Analysis of threats and simulation of impacts," tech. rep., The Royal Holloway University of London, 2017. Accessed: 2019-05-07.

[13] Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC), "2021 annual report." https://www.mtsisac.org/resources/annual-reports, 2021. Available at: https://www.mtsisac.org/resources/annual-reports.

[14] International Electrotechnical Commission and International Organization for Standardization, "Iso/iec 62443-3-3:2018 — security for industrial automation and control systems — system security requirements and security levels." https://webstore.iec.ch/publication/60225, 2018. Available at: https://webstore.iec.ch/publication/60225.

[15] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "Industrial cyber-physical systems: A review of Industry 4.0 technologies," *Computers in Industry*, vol. 89, pp. 1–18, 2016.

[16] N. Polemi, "Cybersecurity for maritime industrial control systems," in *Advances in Transport*, vol. 12, pp. 67–82, Elsevier, 2017.

[17] M. Loupasakis, G. Potamos, and E. Stavrou, "Revolutionizing social engineering awareness raising, education and training: generative ai-powered investigations in the maritime domain," in *International Conference on Human-Computer Interaction*, pp. 70–83, Springer, 2024.

[18] C. Kapalidis, S. Karamperidis, T. Watson, and G. Koligiannis, "A vulnerability centric system of systems analysis on the maritime transportation sector most valuable assets: Recommendations for port facilities and ships," *Journal of Marine Science and Engineering*, vol. 10, no. 10, p. 1486, 2022.

[19] B. Croteau, "Lessons learned from teaching a maritime industrial control systems cybersecurity course," in *2023 IEEE 48th Conference on Local Computer Networks (LCN)*, pp. 1–6, IEEE, 2023.

[20] R. K. Nichols, H. C. Mumm, W. Lonstein, S. Sincavage, C. M. Carter, J.-P. Hood, R. Mai, M. Jackson, and B. Shields, "Disruptive technologies with applications in airline & marine and defense industries," 2021.

[21] Baltic and International Maritime Council (BIMCO), International Chamber of Shipping (ICS), INTERCARGO, INTERTANKO, and Cruise Lines International Association (CLIA), "The guidelines on cyber security onboard ships." https://www.econstor.eu/bitstream/10419/209316/1/hicl-2017-23-343.pdf, 2016. First published version of industry guidelines on maritime cyber security.

[22] C. Senarak, "Port cyberattacks from 2011 to 2023: a literature review and discussion of selected cases," *Maritime Economics & Logistics*, vol. 26, no. 1, pp. 105–130, 2024.

[23] Y. Wang, P. Chen, B. Wu, C. Wan, and Z. Yang, "A trustable architecture over blockchain to facilitate maritime administration for mass systems," *Reliability Engineering & System Safety*, vol. 219, p. 108246, 2022.

[24] A. J. Rodriguez and M. C. Hubbard, "International safety management (ism) code: a new level of uniformity," *Tul. L. Rev.*, vol. 73, p. 1585, 1998.

[25] BIMCO and Industry Partners, "The guidelines on cyber security onboard ships, version 5." https://www.bimco.org/products/publications/titles/the-guidelines-on-cyber-security-onboard-ships/, November 2024. Published on 14 November 2024.

[26] N. Nomikos, G. Xylouris, G. Patsourakis, V. Nikolakakis, A. Giannopoulos, C. Mandilaris, P. Gkonis, C. Skianis, and P. Trakadas, "A distributed trustable framework for ai-aided anomaly detection," *Electronics*, vol. 14, no. 3, p. 410, 2025.

[27] D. Kim and H. K. Kim, "Automated dataset generation system for collaborative research of cyber threat analysis," *Security and communication networks*, vol. 2019, no. 1, p. 6268476, 2019.

[28] C.-W. Tsai, C.-F. Lai, M.-C. Chiang, and L. T. Yang, "Data mining for internet of things: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 1, pp. 77–97, 2013.

[29] F. Soldo, A. Le, and A. Markopoulou, "Predictive blacklisting as an implicit recommendation system," in *2010 Proceedings IEEE INFOCOM*, pp. 1–9, IEEE, 2010.

[30] M. F. Franco, B. Rodrigues, and B. Stiller, "Mentor: the design and evaluation of a protection services recommender system," in *2019 15th international conference on network and service management (CNSM)*, pp. 1–7, IEEE, 2019.

[31] N. Moustafa and J. Slay, "Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set)," in *2015 military communications and information systems conference (MilCIS)*, pp. 1–6, IEEE, 2015.

[32] I. Sharafaldin, A. H. Lashkari, A. A. Ghorbani, *et al.*, "Toward generating a new intrusion detection dataset and intrusion traffic characterization.," *ICISSp*, vol. 1, no. 2018, pp. 108–116, 2018.