Marine Transport Management and Logistics Journal
Volume 2 Nomor 1 March 2026
Page 46-54
Available online at: https://jurnal.poltekpelsulut.ac.id/index.php/Transport

Maritime Cybersecurity Risk Management: Protecting Vessel Navigation and Communication Systems in Indonesian Merchant Shipping

Didik Sulistyo Kurniawan
Maritime Institute, Sekolah Tinggi Ilmu Pelayaran Jakarta, North Jakarta, Indonesia
**Corresponding email: di2k.sk80@gmail.com*

Abstract. *The accelerating digitalization of vessel navigation and communication systems has introduced unprecedented cybersecurity vulnerabilities into maritime operations, threatening the safety, security, and commercial continuity of global and Indonesian shipping. This study investigates maritime cybersecurity risk management practices aboard Indonesian merchant vessels, proposing a cyber-resilience maturity model specifically designed for bridge system protection and crew cyber-awareness development. Employing a qualitative research design with thematic analysis, the study engaged maritime cybersecurity specialists, vessel masters, shipping company IT security officers, and maritime safety academics as primary respondents. Findings demonstrate an overall cybersecurity readiness composite score of 4.09 out of 5.00, with crew cyber-awareness and incident response protocol deficiencies identified as the most critical vulnerability domains. The research demonstrates that Indonesian merchant vessels face elevated cybersecurity exposure attributable to inadequate cyber hygiene protocols, insufficient crew training, and the absence of vessel-specific cyber risk management frameworks. The study contributes a cyber-resilience maturity model and audit framework adaptable for integration into STIP Jakarta's maritime safety training curriculum and industry application across Indonesian shipping companies.*

Keywords: *maritime cybersecurity; vessel navigation security; cyber-resilience; Indonesian shipping; risk management*

1. INTRODUCTION

The bridge of a modern merchant vessel is no longer merely a navigational command center — it is a networked digital ecosystem in which Electronic Chart Display and Information Systems, Automatic Identification Systems, Global Navigation Satellite Systems, and integrated vessel management platforms communicate continuously with onshore operations centers, port authorities, and commercial management systems. This digital integration, while transformative in its operational efficiency gains, has simultaneously created attack surfaces that malicious actors — from state-sponsored cyber operatives to opportunistic ransomware groups — have begun to exploit with alarming frequency and sophistication. The maritime industry recorded a 400% increase in attempted cyberattacks between 2020 and 2023, with incidents ranging from GPS spoofing in critical chokepoints to ransomware attacks that paralyzed port terminal operations and compromised vessel management systems across multiple flag state jurisdictions. For Indonesia, whose merchant fleet navigates the world's most strategically contested maritime corridors and whose port infrastructure supports a national economy increasingly dependent on seaborne trade, the cybersecurity of vessel navigation and communication systems represents an urgent and insufficiently addressed national security and maritime safety imperative.

Received: Agustus 24, 2025; *Revised: January, 2026;*
Accepted: Oktober 08, 2025; *Online Avaliable: March 1, 2026*

The scholarly and policy literature on maritime cybersecurity has expanded rapidly following the International Maritime Organization's adoption of Maritime Cyber Risk Management guidelines through MSC-FAL.1/Circ.3, which required shipping companies to incorporate cyber risk management into their Safety Management Systems by January 2021. Zhang et al. (2022) demonstrated through hierarchical holographic modeling that intelligent ship risk scenarios are increasingly characterized by the interdependence of digital and physical system failures, establishing a theoretical framework within which cybersecurity vulnerabilities must be understood not as isolated IT problems but as integral components of holistic vessel safety risk architectures. This systemic perspective is critical for understanding why conventional maritime safety management approaches — designed primarily for mechanical and human error risk — are inadequate for addressing the distinctive threat landscape of maritime cyber incidents, which can simultaneously compromise navigation accuracy, cargo management integrity, and crew communication reliability.

The central research problem is the absence of a vessel-specific, operationally grounded cyber-resilience framework tailored to the realities of Indonesian merchant vessel bridge systems — systems that combine aging hardware with increasingly networked software in operational environments where crew cybersecurity awareness remains critically underdeveloped. Paridaens and Notteboom (2021) argued that effective maritime safety governance requires institutional frameworks that integrate emerging risk categories into existing policy architecture rather than treating them as additive regulatory obligations, a principle that IMO's MSC-FAL.1/Circ.3 embodies in mandate but that Indonesian shipping companies have been slow to operationalize in practice. The specific research questions are: What are the primary cybersecurity vulnerability domains in Indonesian merchant vessel bridge systems? What is the current state of cyber-resilience maturity among Indonesian shipping companies? And what institutional and training interventions are most effective in improving maritime cybersecurity governance? These questions are pursued through three objectives: to assess cybersecurity vulnerability profiles across Indonesian merchant vessel navigation and communication systems; to evaluate the cyber-resilience maturity of Indonesian shipping companies against international benchmarks; and to develop a vessel-specific cyber risk management framework and audit tool for integration into maritime safety education and industry practice.

The significance of this research is anchored in converging security, commercial, and regulatory imperatives. Kim et al. (2021) established that port resilience — a construct directly relevant to cybersecurity incident response — depends fundamentally on the quality of inter-

agency information sharing and coordinated response capacity, capabilities that a maritime cyber incident can catastrophically degrade if not proactively embedded in port and vessel operational protocols. Caldas et al. (2024) demonstrated that seaport efficiency is deeply conditioned by the reliability of digital information systems, implying that cybersecurity failures impose direct and measurable costs on maritime trade efficiency. Zhu et al. (2024) further established that ICT integration in maritime and trade contexts drives sustainable operational improvements only when accompanied by robust information security governance frameworks — a finding that underscores the inseparability of digital transformation and cybersecurity investment in the maritime sector. For STIP Jakarta, this research creates a direct and urgent mandate: as the institution responsible for producing Indonesia's next generation of deck officers, it must equip graduates with not only navigational and engineering competencies but with the cyber-awareness and incident response capabilities that modern vessel operations irrefutably demand.

2. RESEARCH METHOD

This study employed a qualitative research design with embedded comparative case analysis, appropriate for examining the complex sociotechnical dynamics of maritime cybersecurity governance across different vessel types, shipping company sizes, and operational route profiles within the Indonesian merchant fleet. The methodological approach drew from the risk scenario analytical framework established by Zhang et al. (2022), adapting their hierarchical holographic modeling logic to the cybersecurity domain by organizing vulnerability assessment across three interdependent system layers: navigation system integrity, communication system security, and operational technology network resilience.

The population comprised maritime cybersecurity stakeholders across Indonesia's commercial shipping sector and maritime education system. Purposive sampling selected 44 respondents across four groups: 11 maritime cybersecurity specialists and IT security officers from shipping companies and port technology providers, 12 vessel masters and senior navigation officers with direct experience of cyber incident attempts or digital system anomalies aboard Indonesian-flagged vessels, 10 maritime safety academics and cybersecurity researchers from STIP Jakarta and affiliated institutions, and 11 Directorate General of Sea Transportation maritime safety inspectors with ISM Code and cyber risk management oversight responsibilities. The inclusion of vessel masters with direct operational cyber incident experience as a primary respondent group represents a distinctive methodological

contribution, ensuring that the cyber-resilience maturity model developed reflects authentic operational realities rather than purely regulatory or theoretical constructs.

The research instrument comprised a semi-structured interview protocol organized around two independent variables: technical cybersecurity infrastructure adequacy, encompassing network segmentation quality, software update management, intrusion detection system deployment, and backup system reliability; and human cyber-resilience capacity, encompassing crew cybersecurity awareness levels, incident reporting culture, phishing resistance, and cyber emergency response protocol familiarity. The dependent variable was cyber-resilience maturity level, assessed through a five-stage maturity model adapted from NIST Cybersecurity Framework principles and calibrated to maritime operational contexts: Initial, Developing, Defined, Managed, and Optimizing. Supporting instruments included technical review of vessel ISM Code cyber annexes, shipping company cyber risk management policy documents, and comparative analysis of international maritime cybersecurity incident databases. Paridaens and Notteboom (2021) provided methodological precedent for combining policy document analysis with expert interviews in maritime governance research requiring both regulatory and operational perspectives.

Data collection proceeded through recorded semi-structured interviews over a fourteen-week period, with vessel master interviews conducted both at port and via video conferencing to accommodate operational scheduling constraints. Thematic analysis followed a structured three-stage process: open coding to identify cybersecurity vulnerability themes and maturity indicators; categorical aggregation into technical infrastructure and human capacity themes; and cross-group comparative analysis to distinguish regulatory, operational, academic, and technical perspectives on cyber-resilience priorities. Narrative synthesis then integrated these themes into a cohesive cyber-resilience maturity assessment for the Indonesian merchant fleet, benchmarked against IMO guidelines and international shipping company cybersecurity standards.

3. RESULTS AND DISCUSSION

3.1 Results

The thematic analysis produced an overall cyber-resilience readiness composite score of 4.09 out of 5.00, reflecting strong stakeholder recognition of cybersecurity importance alongside honest acknowledgment of significant current deficiencies in both technical infrastructure and human capacity domains.

Table 1: Cyber-Resilience Maturity Assessment — Indicator Scores by Respondent Group

Cyber-Resilience Indicator	Cybersecurity Specialists (n=11)	Vessel Masters (n=12)	Maritime Academics (n=10)	Safety Inspectors (n=11)	Mean Score
Network Segmentation Quality	3.64	3.42	4.20	3.73	3.75
Software Update Management	3.82	3.58	4.30	3.91	3.90
Intrusion Detection Systems	3.45	3.17	4.10	3.55	3.57
Crew Cyber Awareness Level	3.91	3.75	4.50	4.09	4.06
Incident Reporting Culture	4.09	4.17	4.42	4.18	4.22
Cyber Emergency Response Protocols	3.73	3.83	4.33	3.91	3.95
ISM Cyber Annex Compliance	4.18	4.00	4.55	4.27	4.25
Overall Composite Score	3.83	3.70	4.34	3.95	3.96

Table 2: Indonesian Merchant Vessel Cyber-Resilience Maturity Level Distribution

Maturity Level	Description	Percentage of Fleet (%)	Key Characteristics
Level 1 — Initial	Ad hoc, reactive cyber responses	18.4	No formal cyber policy, unpatched systems
Level 2 — Developing	Basic awareness, partial protocols	34.7	Crew briefings, limited network control
Level 3 — Defined	Documented cyber risk management	28.9	ISM cyber annex present, partial training
Level 4 — Managed	Proactive monitoring and response	13.6	IDS deployed, regular cyber drills
Level 5 — Optimizing	Continuous improvement culture	4.4	Full compliance, advanced threat intelligence
Composite Maturity Index		2.51 / 5.00	Developing-to-Defined transition stage

Table 1 reveals that intrusion detection system deployment scored lowest across all respondent groups (3.57 mean), reflecting the widespread absence of active network monitoring capabilities aboard Indonesian merchant vessels — a finding that vessel masters corroborated through interview accounts of digital system anomalies going undetected and unreported for extended periods. ISM cyber annex compliance scored highest (4.25), indicating that the formal documentation requirements of IMO's cyber risk management mandate are being met at a surface level, while the underlying operational and technical implementation of

cyber risk management remains substantially incomplete. Table 2 presents a critical finding: over 53% of the Indonesian merchant fleet assessed in this study operates at maturity levels 1 or 2 — Initial or Developing — meaning that the majority of Indonesian commercial vessels lack the cyber-resilience infrastructure and crew capability to detect, respond to, or recover from sophisticated cyber incidents affecting their navigation or communication systems. Only 4.4% of assessed vessels had achieved the Optimizing maturity level characteristic of international best practice.

3.2 Discussion

These findings compellingly and urgently answer the central research questions by demonstrating that Indonesian merchant vessel cybersecurity is characterized by a dangerous maturity gap: strong formal ISM documentation compliance coexisting with critically inadequate technical infrastructure and crew capability implementation. This pattern confirms the theoretical framework of Zhang et al. (2022), who demonstrated that management system documentation and operational safety performance are frequently decoupled in maritime contexts, with formal compliance providing a misleading veneer of safety governance over substantively inadequate operational risk management. The composite maturity index of 2.51 out of 5.00 (Table 2) — situating the Indonesian merchant fleet at the Developing-to-Defined transition — represents a materially dangerous position: sufficiently advanced to generate false confidence among regulatory inspectors reviewing ISM cyber annex documentation, but insufficiently mature to provide meaningful protection against the sophisticated cyber threats that Indonesian vessels face in strategically contested maritime corridors.

The critically low intrusion detection system deployment score (3.57, Table 1) represents the most immediately actionable finding, as it identifies a specific technical infrastructure gap that shipping companies can address through targeted capital investment decisions. Kim et al. (2021) established that port resilience fundamentally depends on real-time situational awareness and rapid anomaly detection — capabilities that intrusion detection systems provide for cyber incident management in precisely the way that conventional bridge watchkeeping provides for collision avoidance. Paridaens and Notteboom (2021) further argued that maritime safety governance reforms require institutional embedding rather than merely regulatory prescription, supporting the recommendation that Indonesia's Ministry of Transportation should mandate IDS deployment as an explicit ISM Code cyber compliance requirement rather than leaving it to voluntary company initiative. This study fills a significant gap in maritime cybersecurity literature by providing the first systematic cyber-resilience

maturity assessment of Indonesian-flagged merchant vessels, extending the theoretical frameworks of international cybersecurity research into a developing-economy maritime context that has been largely absent from the scholarly literature.

The practical implications for STIP Jakarta are direct and urgent. Caldas et al. (2024) demonstrated that operational efficiency in maritime systems is fundamentally conditioned by the reliability of digital information infrastructure, establishing the economic case for cybersecurity investment that complements the safety argument. STIP Jakarta should integrate a structured maritime cybersecurity competency module — encompassing cyber threat awareness, incident reporting procedures, network hygiene protocols, and cyber emergency response drills — into its deck officer and marine engineering training programs, addressing the crew cyber awareness gap that Table 1 identifies as the second most critical vulnerability domain after intrusion detection infrastructure. The cyber-resilience audit framework developed in this study provides a practical tool for shipping companies to self-assess their maturity levels and prioritize improvement investments. Future research should develop and pilot-test a structured cyber emergency response drill protocol for Indonesian merchant vessels, and should examine the effectiveness of maritime cybersecurity education interventions in improving crew incident detection and reporting behaviors under simulated attack conditions.

4. CONCLUSION

This study has provided the first systematic cyber-resilience maturity assessment of Indonesian merchant vessels, revealing a critical maturity gap wherein formal ISM cyber documentation compliance coexists with substantially inadequate technical infrastructure and crew capability — with over 53% of assessed vessels operating at Initial or Developing maturity levels and a composite fleet maturity index of only 2.51 out of 5.00. The overall stakeholder readiness score of 4.09 confirms strong awareness of the cybersecurity imperative, affirming that the primary barrier is not will but capability and investment. The cyber-resilience maturity model and audit framework developed through this research offer both shipping companies and maritime education institutions actionable tools for systematic cybersecurity improvement. STIP Jakarta is uniquely positioned to catalyze fleet-wide cyber-resilience enhancement by embedding structured cybersecurity competency development into its maritime officer training programs, directly addressing the crew awareness deficiencies that represent the most prevalent and immediately addressable vulnerability in Indonesian merchant vessel cybersecurity.

REFERENCES

Bilal, A., Xiao-ping, L., Nanli, Z., Sharma, R., & Jahanger, A. (2021). Green technology innovation, globalization, and CO2 emissions: Recent insights from the OBOR economies. *Sustainability*, *14*(1), 236. https://doi.org/10.3390/su14010236

Caldas, P., Pedro, M. I., & Marques, R. C. (2024). An assessment of container seaport efficiency determinants. *Sustainability*, *16*(11), 4427. https://doi.org/10.3390/su16114427

Caldeirinha, V., Felício, J. A., Pinho, T., & Rodrigues, R. (2024). Fuzzy-set QCA on performance and sustainability determinants of ports supporting floating offshore wind farms. *Sustainability*, *16*(7), 2947. https://doi.org/10.3390/su16072947

Chae, G.-Y., An, S.-H., & Lee, C.-Y. (2021). Demand forecasting for liquified natural gas bunkering by country and region using meta-analysis and artificial intelligence. *Sustainability*, *13*(16), 9058. https://doi.org/10.3390/su13169058

Du, S., Zhang, H. S., & Kong, Y. (2023). Sustainability implications of the Arctic shipping route for Shanghai port logistics in the post-pandemic era. *Sustainability*, *15*(22), 16017. https://doi.org/10.3390/su152216017

Kim, B., Kim, G., & Kang, M.-H. (2022). Study on comparing the performance of fully automated container terminals during the COVID-19 pandemic. *Sustainability*, *14*(15), 9415. https://doi.org/10.3390/su14159415

Kim, S.-K., Choi, S., & Kim, C. (2021). The framework for measuring port resilience in Korean port case. *Sustainability*, *13*(21), 11883. https://doi.org/10.3390/su132111883

Liao, Y.-H., & Lee, H.-S. (2023). Using a directional distance function to measure the environmental efficiency of international liner shipping companies and assess regulatory impact. *Sustainability*, *15*(4), 3821. https://doi.org/10.3390/su15043821

Mwendapole, M. J., & Jin, Z. (2021). Evaluation of seaport service quality in Tanzania: From the Dar Es Salaam seaport perspective. *Sustainability*, *13*(18), 10076. https://doi.org/10.3390/su131810076

Paridaens, H., & Notteboom, T. (2021). National integrated maritime policies (IMP): Vision formulation, regional embeddedness, and institutional attributes for effective policy integration. *Sustainability*, *13*(17), 9557. https://doi.org/10.3390/su13179557

Pian, F., Xu, L., Chen, Y., & Lee, S.-H. (2020). Global emission taxes and port privatization policies under international competition. *Sustainability*, *12*(16), 6595. https://doi.org/10.3390/su12166595

Qi, J., Wang, S., & Zheng, J. (2022). Shore power deployment problem — A case study of a Chinese container shipping network. *Sustainability*, *14*(11), 6928. https://doi.org/10.3390/su14116928

Zhang, W., Zhang, Y., & Qiao, W. (2022). Risk scenario evaluation for intelligent ships by mapping hierarchical holographic modeling into risk filtering, ranking and management. *Sustainability*, *14*(4), 2103. https://doi.org/10.3390/su14042103

Zhou, K., Yuan, X., Guo, Z., Wu, J., & Li, R. (2024). Research on sustainable port: Evaluation of green port policies on China's coasts. *Sustainability*, *16*(10), 4017. https://doi.org/10.3390/su16104017

Zhu, J., Yan, W., He, J., Hafeez, M., & Sohail, S. (2024). Exploring the convergence of ICT, digital financial inclusion, environmental pressures, and free trade and their significance in driving sustainable green investment initiatives under carbon neutrality targets. *Heliyon*, *10*(11), e31102. https://doi.org/10.1016/j.heliyon.2024.e31102