Green Intelligent Systems and Applications

Research Article
Volume 5(2), 2025, 205−216
https://doi.org/10.53623/gisa.v5i2.930

Maritime Cybersecurity Readiness and Training Standards in Indonesia

Stevian G. A. Rakka*, Bagja Gumilar, Haryadi Wijaya, Azhar Ariansyah Ansar

Department of Nautical Studies, Politeknik Pelayaran Sulawesi Utara, Jl. Trans Sulawesi KM.80, Ds. Tawaang Timur, Kec. Tenga, Kabupaten Minahasa Selatan, Sulawesi Utara 95355, Indonesia

*Correspondence: stevian@poltekpelsulut.ac.id

SUBMITTED: 28 November 2025; REVISED: 22 December 2025; ACCEPTED: 24 December 2025

ABSTRACT: The rapid digitalization of maritime operations through IoT-enabled navigation systems and cyber-physical ship infrastructures increased Indonesia's exposure to cybersecurity risks. Strengthening cybersecurity competence within Maritime Education and Training (MET) institutions was therefore essential to ensure navigational safety, operational reliability, and national maritime resilience. This study assessed cybersecurity readiness, training standards, instructor competence, and facility availability in Indonesian MET institutions with reference to international frameworks, including IMO MSC-FAL.1/Circ.3, BIMCO guidelines, and ISO/IEC 27001. A descriptive quantitative approach was employed using structured questionnaires to evaluate organizational readiness, curriculum implementation, instructor qualifications, and supporting facilities. Data were analyzed using percentage distributions to identify institutional conditions and gaps relative to global requirements. The results indicated that cybersecurity training in most MET institutions remained largely theoretical, with limited practical exposure. Nearly 80% of respondents reported having no prior cybersecurity training, while hands-on facilities such as cyber laboratories and simulation environments were largely unavailable. Instructor expertise and standardized cybersecurity modules aligned with international guidelines were insufficient to adequately address threats to AIS, GPS, ECDIS, and integrated IT–OT systems. These findings revealed a significant gap between existing training practices and the competencies required for secure digital maritime operations. The study concluded that standardized, practice-oriented cybersecurity training was urgently needed, supported by instructor upskilling, curriculum alignment with international standards, and the development of shared training facilities. Strengthening these aspects was critical to improving national maritime cyber readiness and supporting resilient intelligent maritime systems.

KEYWORDS: Cybersecurity readiness; maritime training; iot-enabled systems; cyber-physical systems

1. Introduction

The rapid development of digital technologies in the maritime industry has significantly transformed ship and port operations worldwide, including in Indonesia. Modern navigation systems such as Radar, Automatic Identification System (AIS), and Electronic Chart Display

and Information System (ECDIS) have become essential components of voyage planning and operational safety, forming the backbone of contemporary maritime operations [1,2]. Additionally, digital technologies that support data collection, transmission, and analysis have increasingly enhanced navigation efficiency, port services, and environmental protection efforts [3–5]. However, this digital transformation has also introduced new cyber vulnerabilities, exposing maritime systems to threats that may compromise navigational safety and operational continuity [6–11].

Despite the increasing reliance on digital and interconnected maritime systems, cybersecurity preparedness within Indonesia's Maritime Education and Training Institutions (METIs) has remained insufficiently examined. Existing studies have largely focused on technological risks or regulatory frameworks, while empirical assessments of cybersecurity readiness and training capacity at the institutional education level have been limited, particularly in developing maritime nations. This gap is critical, as METIs are responsible for equipping future seafarers with competencies aligned with evolving cyber risks. Indonesia, as the world's largest archipelagic state with over 17,000 islands, depends heavily on maritime transportation for national connectivity and economic activity. Recent national data indicate a significant rise in cyber incidents targeting critical infrastructure, while surveys reveal that a substantial proportion of Indonesian seafarers lack adequate understanding of maritime cyber risks and mitigation measures [15]. These conditions suggest a mismatch between the rapid digitalization of maritime operations and the preparedness of human resources responsible for operating and managing these systems.

Human factors play a dominant role in maritime cyber incidents, accounting for approximately 65.8% to 80% of reported cases [16,17]. This highlights the importance of structured cybersecurity education and training. Although the International Maritime Organization (IMO) has mandated the integration of cyber risk management into ship safety management systems since January 2021 [18], the adoption of IMO cybersecurity guidelines (MSC-FAL.1/Circ.3) within Indonesian maritime education has been inconsistent and uneven across institutions. Prior research also identified gaps between industry cybersecurity requirements and training practices in developing countries [19–22], reinforcing the need for localized empirical investigation. Maritime Education and Training Institutions play a central role in preparing seafarers to operate safely in digitalized and cyber-physical shipboard environments [23]. However, challenges persist, including limited institutional capacity, insufficient instructor competence, and the absence of standardized, practice-oriented cybersecurity curricula [24, 25]. These constraints raise concerns regarding the ability of Indonesian METIs to meet international maritime cybersecurity expectations.

In response to these gaps, this study provides an evidence-based assessment of cybersecurity readiness in Indonesian MET institutions. The novelty of this research lies in its integrated approach, which simultaneously evaluates cybersecurity awareness among cadets and instructors, examines existing training practices and institutional support, and identifies gaps relative to international standards, particularly in the context of IoT-enabled and cyber-physical maritime systems. The objectives of this study were to identify core maritime cybersecurity competencies defined by international frameworks, assess awareness and training implementation within METIs, and analyze institutional readiness to support effective cybersecurity education. Through this approach, the study contributes to the development of targeted educational strategies aimed at strengthening Indonesia's maritime cyber resilience.

2. Materials and Methods

This study adopted a mixed-methods approach, combining qualitative and quantitative techniques to comprehensively address the research objectives. Specifically, an Exploratory Sequential Design was employed, in which the research process began with qualitative data collection and analysis, followed by quantitative data gathering to validate and generalize the qualitative findings. This design enabled the integration of both datasets to determine how the quantitative outcomes reinforced or complemented the initial qualitative insights [26].

2.1. Research design.

The qualitative phase involved gathering expert perspectives from maritime instructors within MET institutions under the Ministry of Transportation, as well as insights from maritime practitioners and regulatory authorities. Literature related to maritime cybersecurity training was also analyzed to strengthen the conceptual foundation [5, 6, 15, 29]. The findings from this phase were used to construct the quantitative survey instruments, which were administered to measure awareness levels, technical competencies, and cybersecurity-related perceptions among instructors and cadets.

2.2. Data collection techniques.

Three data collection techniques were employed in this study: observation, literature review, and questionnaires.

2.2.1. Observation.

Direct classroom observations were conducted at Politeknik Pelayaran Sulawesi Utara over one academic semester, with multiple observation sessions during cybersecurity-related classes. Each session lasted approximately 90–120 minutes and focused on predefined criteria, including instructional methods, use of learning media, integration of cybersecurity content into courses, student engagement, and the availability of practical or simulation-based activities. These criteria ensured consistency and replicability of the observation process.

2.2.2. Literature review.

Relevant documents on maritime cybersecurity education and training, including international guidelines such as BIMCO Cyber Security Onboard Ships and IMO standards, were reviewed. Additional cybersecurity frameworks, including ISO/IEC 27002:2022, ISO/IEC 27032:2023, and the NICE Framework by NIST, also informed the development of research instruments [27,28].

2.2.3. Questionnaire.

A structured questionnaire using a Likert scale was developed based on the qualitative findings. The instrument measured cybersecurity awareness, technical competencies (incident detection, risk management), and perceptions of training effectiveness among instructors and cadets [17]. The final survey consisted of five variable domains, with multiple indicator items for each construct.

2.3. Sampling technique.

Primary data were gathered through observation and questionnaires using a stratified random sampling technique. This method was appropriate for a heterogeneous population divided into proportional strata [29]. Samples were drawn from four MET institutions in Eastern Indonesia, covering two respondent groups: instructors and cadets. A total of 430 respondents participated in the quantitative survey, including 22 instructors and 408 cadets. This sampling approach enabled a representative assessment of maritime cybersecurity readiness within the region.

2.4. Data analysis.

Qualitative data were analyzed using Thematic Analysis to identify recurring patterns and generate themes capable of addressing the research questions, consistent with approaches described by Castleberry and Nolen [30]. These themes guided the construction of the quantitative instrument. Quantitative data underwent reliability and validity testing to ensure accuracy and consistency. Internal consistency reliability was evaluated using Cronbach's alpha, with all constructs exceeding the commonly accepted threshold of 0.70, indicating satisfactory reliability. Content validity was established through expert review during the qualitative phase, while construct validity was assessed through item–total correlation analysis. Subsequently, descriptive statistical analysis was performed to determine mean scores and percentage distributions of cybersecurity awareness and competency levels among respondents. These results were interpreted to reflect the overall readiness of MET institutions in Indonesia.

3. Results and Discussion

The results of this study combined qualitative insights from observations, document analysis, and literature review with quantitative findings obtained through a structured questionnaire. These two forms of data provided a comprehensive understanding of the current condition of maritime cybersecurity training in Indonesian MET institutions. The qualitative findings highlighted the fundamental competencies that maritime professionals must possess in accordance with international standards. Through thematic analysis of the literature, guidelines from IMO, BIMCO, and the ISO/IEC 27000 series, and institutional documents, a competency framework was constructed describing the essential elements of maritime cybersecurity capability. This framework included core competencies such as understanding maritime cyber threats, cyber risk management, incident detection and response, and cyber hygiene, as well as supporting competencies related to technical cybersecurity skills, OT/ICS security awareness, compliance and governance, digital forensics, and emergency support. These competencies aligned with the Protect–Detect–Respond cycle outlined in IMO MSC-FAL.1/Circ.3/Rev.2 and were consistent with global cybersecurity expectations for seafarers. This qualitative framework provided a reference baseline against which the quantitative findings were interpreted, enabling a clearer identification of gaps between expected and actual institutional readiness.

3.1. Respondent profile.

The quantitative analysis began with a description of the respondent profile, which is presented in Table 1. As shown, the majority of participants were cadets (94.9%), with instructors making up only 5.1%. Respondents were predominantly from Politeknik Ilmu Pelayaran Makassar (64.4%), followed by Politeknik Pelayaran Barombong (22.3%), Politeknik Pelayaran Sulawesi Utara (11.6%), and Politeknik Pelayaran Sorong (1.6%). Additionally, 79.5% of respondents reported having never received prior cybersecurity training. This respondent distribution indicated that the findings strongly reflected the perspective of future maritime professionals while still capturing instructor viewpoints, which are critical for evaluating institutional readiness and curriculum effectiveness. The high proportion of respondents without prior cybersecurity training underscored the urgency of strengthening cybersecurity education within MET institutions.

Table 1. Respondent characteristics.

Category	Description	Frequency (F)	Percentage (%)
Training Institution	Maritime Polytechnic of North Sulawesi	50	0.116
	Maritime Polytechnic of Sorong	7	0.016
	Maritime Polytechnic of Barombong	96	0.223
	Maritime Science Polytechnic of Makassar	277	0.644
Respondent Role	Instructor/Lecturer	22	0.051
	Cadet	408	0.949
Work Experience	No experience	409	0.951
	< 2 years	0	0
	2–5 years	3	0.007
	> 5 years	18	0.042
Previous Cybersecurity Training	Yes	88	0.205
	No	342	0.795

3.2. Overall descriptive statistics.

Descriptive statistical results for all variables were summarized in Table 2 and visualized in Figure 1. The mean scores for all five variables exceeded 3 on the Likert scale, suggesting a generally positive perception of maritime cybersecurity among respondents. The highest mean value was observed in “Perception and Development Needs” (mean = 4.03), indicating strong demand for further cybersecurity education.

Table 2. Descriptive statistics of likert-scale variables.

Variable	N (Valid)	Mean	Median	Mode	Std. Deviation	Range	Min	Max
Cybersecurity Awareness	430	3.9823	4	4	0.77253	4	1	5
Technical Cybersecurity Competence	430	3.8326	4	4	0.77626	4	1	5
Curriculum and Training Implementation	430	3.874	4	4	0.80141	4	1	5
Institutional Support and Infrastructure	430	3.9	4	4	0.80067	4	1	5
Perception and Development Needs	430	4.0358	4	4	0.79739	4	1	5

In contrast, “Technical Cybersecurity Competence” recorded the lowest mean score (3.83), highlighting a gap between awareness and practical capability. These results suggested that while respondents recognized the importance of cybersecurity, existing training had not yet

translated into sufficient technical proficiency. Similar patterns were reported in prior studies, which noted that maritime personnel often demonstrated high awareness but limited hands-on competence in cyber incident detection and response [6, 10, 21].

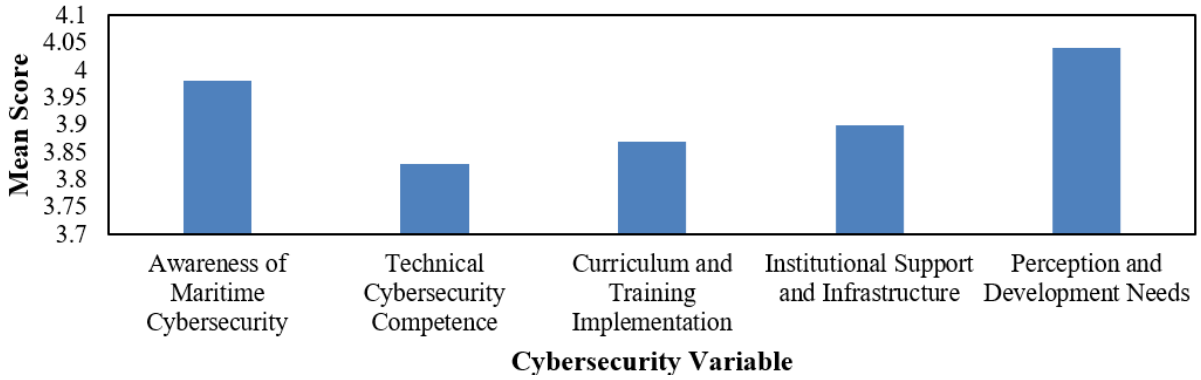

Figure 1. Descriptive statistics of likert-scale variables across five cybersecurity dimensions.

3.3. Comparison between instructors and cadets.

The independent t-test results (Table 3) revealed no statistically significant differences for most variables, except for curriculum implementation and institutional support. Instructors consistently reported lower mean scores than cadets, particularly regarding curriculum adequacy and infrastructure readiness. This difference indicated that instructors, drawing on professional experience and familiarity with international standards, tended to assess institutional readiness more critically. From a practical perspective, this finding suggested the need for greater instructor involvement in curriculum design, institutional planning, and the evaluation of cybersecurity training facilities. Incorporating instructor feedback could help MET institutions align training programs more closely with operational and regulatory realities.

Table 3. Independent t-Test based on respondent role.

Variable	Role	N	Mean	Std. Deviation	Std. Error Mean
Cybersecurity Awareness	Instructor/Lecturer	22	3.9636	0.74485	0.1588
	Cadet	408	3.9833	0.77486	0.03836
Technical Cybersecurity Competence	Instructor/Lecturer	22	3.6818	0.56454	0.12036
	Cadet	408	3.8407	0.78575	0.0389
Curriculum and Training Implementation	Instructor/Lecturer	22	3.5091	0.8041	0.17144
	Cadet	408	3.8936	0.79751	0.03948
Institutional Support and Infrastructure	Instructor/Lecturer	22	3.6182	0.61384	0.13087
	Cadet	408	3.9152	0.80732	0.03997
Perception and Development Needs	Instructor/Lecturer	22	4.1455	0.47882	0.10208
	Cadet	408	4.0299	0.81097	0.04015

3.4. Cybersecurity awareness.

As summarized in Table 4, respondents demonstrated strong awareness of maritime cyber threats, particularly regarding the vulnerability of navigation systems (AIS, ECDIS, GPS) and the impact of cyberattacks on navigational safety. Awareness of personal responsibility in safeguarding data also scored highly. However, awareness of institutional cybersecurity

policies was relatively lower. This pattern suggested that individual awareness had developed more rapidly than institutional policy communication. Similar observations were reported in previous maritime cybersecurity studies, which emphasized that policy awareness often lagged behind general threat awareness [2,7]. Improving internal policy dissemination and embedding cybersecurity governance into daily training activities were therefore essential steps toward strengthening institutional readiness.

Table 4. Cybersecurity awareness indicators.

Item Statement	N	Mean	Median	Mode	Std. Deviation	Range	Min	Max
I understand what cyber threats mean in the maritime context.	430	3.85	4	4	0.863	4	1	5
I am aware that navigation systems (AIS, ECDIS, GPS) can be targets of cyberattacks.	430	4	4	4	0.873	4	1	5
I understand the serious impact of cyberattacks on navigational safety.	430	4.05	4	4	0.882	4	1	5
I know the cybersecurity policies applied in my institution.	430	3.92	4	4	0.869	4	1	5
I understand my personal responsibility in safeguarding data and digital devices.	430	4.1	4	4	0.86	4	1	5

3.5. Technical cybersecurity competence.

Technical cybersecurity competence, presented in Table 5, recorded the lowest overall mean score among all variables. Respondents reported limited ability to recognize early indicators of cyberattacks and to respond effectively to incidents. This finding confirmed a critical gap between awareness and operational capability, particularly in relation to IT–OT integrated ship systems. International standards such as IMO MSC-FAL.1/Circ.3/Rev.2 and ISO/IEC 27002 emphasize the importance of incident detection, response, and recovery competencies, which were not yet adequately reflected in current MET training practices. Similar deficiencies were identified in other developing maritime contexts [19–22]. These results highlighted the need for simulation-based and scenario-driven cybersecurity training.

Table 5. Technical cybersecurity competence indicators.

Item Statement	N	Mean	Median	Mode	Std. Deviation	Range	Min	Max
I can recognize early signs of a cyberattack.	430	3.77	4	4	0.879	4	1	5
I know basic steps for responding to a cyber incident.	430	3.81	4	4	0.87	4	1	5
I can correctly use security tools such as antivirus, VPN, or firewalls.	430	3.86	4	4	0.837	4	1	5
I understand best practices in password management and authentication.	430	3.89	4	4	0.858	4	1	5
I know procedures for backup and recovery in case of system disruption.	430	3.84	4	4	0.869	4	1	5

3.6. Curriculum and training implementation.

As shown in Table 6, respondents generally perceived the cybersecurity curriculum as relevant and the teaching methods as helpful. However, the adequacy of hands-on practice received the lowest mean score within this variable. This indicated that existing curricula emphasized theoretical understanding over practical application. From an international perspective, this fell short of BIMCO and IMO recommendations, which stress experiential learning through drills, simulations, and case-based exercises. Strengthening practical components would significantly enhance the effectiveness of cybersecurity education in MET institutions.

Table 6. Cybersecurity curriculum and training implementation.

Item Statement	N	Mean	Median	Mode	Std. Deviation	Range	Min	Max
The cybersecurity training materials I receive are relevant to maritime industry needs.	430	3.88	4	4	0.866	4	1	5
The cybersecurity training provided is easy to understand and applicable.	430	3.88	4	4	0.85	4	1	5
The teaching methods (theory, simulation, case studies) help me understand cyber threats.	430	3.93	4	4	0.851	4	1	5
I receive sufficient hands-on practice in cybersecurity training.	430	3.8	4	4	0.877	4	1	5
The cybersecurity training offered aligns with international standards (IMO, BIMCO).	430	3.87	4	4	0.864	4	1	5

3.7. Institutional support and infrastructure.

Institutional support and infrastructure (Table 7) achieved a moderate mean score (3.90). While respondents acknowledged management support and instructor competence, concerns remained regarding the availability of cyber laboratories and secure training networks. When benchmarked against ISO/IEC 27002:2022 and ISO/IEC 27032:2023, these findings suggested that Indonesian MET institutions had not yet achieved the minimum infrastructure maturity required to support comprehensive cybersecurity training. The absence of dedicated cyber-lab facilities limited opportunities for hands-on learning and incident response simulation, thereby constraining skill development.

Table 7. Institutional support and infrastructure.

Item Statement	N	Mean	Median	Mode	Std. Deviation	Range	Min	Max
My institution provides secure facilities and networks for cybersecurity practice.	430	3.91	4	4	0.845	4	1	5
Management support for cybersecurity programs is adequate.	430	3.87	4	4	0.868	4	1	5
Instructors have sufficient competence to teach cybersecurity.	430	3.9	4	4	0.849	4	1	5
Cybersecurity training receives adequate institutional priority.	430	3.9	4	4	0.873	4	1	5
I feel my institution is prepared to face future cyber threats.	430	3.92	4	4	0.857	4	1	5

3.8. Perception and development needs.

Finally, Table 8 highlighted strong demand for enhanced cybersecurity training, particularly the development of simulators, digital learning modules, and collaboration with national agencies such as BSSN. This variable recorded the highest mean values across all dimensions. This strong demand reflected growing awareness among both cadets and instructors that current training was insufficient to address evolving maritime cyber threats. Similar calls for inter-agency collaboration and shared training infrastructure were emphasized in previous studies on maritime cybersecurity capacity building [21, 22].

Table 8. Perception and development needs.

Item Statement	N	Mean	Median	Mode	Std. Deviation	Range	Min	Max
Cybersecurity is an essential component of maritime training curricula.	430	4.01	4	4	0.828	4	1	5
I need more advanced cybersecurity training.	430	4.02	4	4	0.859	4	1	5
I expect simulators or digital modules for cybersecurity practice.	430	4.06	4	4	0.834	4	1	5
Cybersecurity training should be adapted to Indonesia's technological context.	430	4.02	4	4	0.84	4	1	5
Collaboration with national agencies such as BSSN is necessary to strengthen cybersecurity training.	430	4.07	4	4	0.843	4	1	5

4. Conclusions

This study provided an integrated assessment of maritime cybersecurity readiness across METIs, combining qualitative insights with quantitative measurements to evaluate awareness, technical competencies, curriculum implementation, institutional support, and development needs. The findings demonstrated that cybersecurity awareness among instructors and cadets was relatively high; however, technical competencies remained limited, particularly in incident detection, response procedures, and handling of cyber-physical systems that integrate IT and OT technologies. Although current training materials and teaching methods were generally aligned with industry expectations, practical training opportunities and simulation-based exercises remained insufficient to meet international standards such as IMO MSC-FAL.1/Circ.3/Rev.2, BIMCO Cybersecurity Guidelines, and ISO/IEC 27002. Institutional support was present but required strengthening, especially in the development of cyber-laboratory facilities, secure network infrastructures, and continuous professional development for instructors. The strong demand from respondents for advanced training, collaboration with national agencies such as BSSN, and the establishment of cybersecurity simulators underscored the growing urgency to modernize maritime training in response to escalating cyber threats. Overall, this research highlighted a significant gap between the current capabilities of METIs and the competencies required for secure digital maritime operations. Addressing these gaps requires standardized, practice-oriented cybersecurity training, improved institutional infrastructure, enhanced instructor qualifications, and multi-stakeholder collaboration. Strengthening these aspects will contribute to national maritime cyber resilience and support Indonesia's transition toward safe and intelligent maritime systems.

Author Contribution

Stevian G. A. Rakka conceptualized the study, designed the research framework, conducted the literature analysis, and prepared the initial manuscript draft. Bagja Gumilar contributed to the methodological design, supervised data collection, and validated both qualitative and quantitative analyses. Haryadi Wijaya assisted in the development of research instruments, carried out statistical processing, and supported the interpretation of the results. Azhar Ariansyah Ansar coordinated field data collection, conducted document analysis, and contributed to the refinement and finalization of the manuscript.

Data Availability

Data availabe upon request from corresponding author.

Competing Interest

The authors declare that there are no competing interests or potential conflicts of interest related to the research, authorship, or publication of this article.

References

[1] Sanchez-Gonzalez, P.L.; Díaz-Gutiérrez, D.; Leo, T.J.; Núñez-Rivas, L.R. (2019). Toward digitalization of maritime transport. *Sensors*, *19*(4), 926. https://doi.org/10.3390/s19040926.

[2] Svilicic, B.; Brčić, D.; Žuškin, S.; Kalebić, D. (2019). Raising awareness on cyber security of ECDIS. *TransNav*, *13*(1), 231–236. https://doi.org/10.12716/1001.13.01.24.

[3] Kyaw, A.Y. (2024). Application of advanced technology on transport ships. *Maritime Park Journal of Maritime Technology and Society*, *3*(2), 1–7. https://doi.org/10.62012/mp.v3i2.35384.

[4] Wahyudi, M.N.A.; Budiyanto, C.W.; Widiastuti, I. (2025). Internet of Things applications for advancing sustainable development goals in Indonesia. *Discover Internet of Things*, *5*, 113. https://doi.org/10.1007/s43926-025-00229-y.

[5] Tan, A.Y.N.; Loh, H.S.; Hsieh, C.H.; Lopez, M.C.R. (2025). Adoption of digital technologies in the maritime industry: Insights from Singapore. *Maritime Technology and Research*, *7*(3). https://doi.org/10.33175/mtr.2025.275821.

[6] Afenyo, M.; Caesar, L.D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. *Ocean and Coastal Management*, *236*, 106493. https://doi.org/10.1016/j.ocecoaman.2023.106493.

[7] Akpan, F.; Bendiab, G.; Shiaeles, S.; Karamperidis, S.; Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. *Network*, *2*(1), 123–138. https://doi.org/10.3390/network2010009.

[8] Ben Farah, M.A.; Ukwandu, E.; Hindy, H.; Brosset, D.; Bures, M.; Andonovic, I.; Bellekens, X. (2022). Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information*, *13*(1), 22. https://doi.org/10.3390/info13010022.

[9] Karas, A. (2023). Maritime industry cybersecurity: A review of contemporary threats. *European Research Studies Journal*, *26*(4), 921–930. https://doi.org/10.35808/ersj/3336.

[10] Yu, H.; Meng, Q.; Fang, Z.; Liu, J. (2023). Literature review on maritime cybersecurity: State-of-the-art. *Journal of Navigation*, *76*(4–5), 453–466. https://doi.org/10.1017/S0373463323000164.

[11] Li, M.; Zhou, J.; Chattopadhyay, S.; Goh, M. (2024). Maritime cybersecurity: A comprehensive review. *arXiv*. https://doi.org/10.48550/arXiv.2409.11417.

[12] Harish, A.V.; Tam, K.; Jones, K. (2025). Literature review of maritime cyber security: The first decade. *Maritime Technology and Research*, *7*(2), 273805. https://doi.org/10.33175/mtr.2025.273805.

[13] Ungureanu, C.; Gasparotti, C. (2024). Assessing cyber risks onboard ships: A literature review. *Annals of "Dunărea de Jos" of Galati*, *47*, 33–40. https://doi.org/10.35219/AnnUgalShipBuilding/2024.47.04.

[14] Tam, K.; Jones, K.D. (2018). Maritime cybersecurity policy: Scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, *3*(2), 147–164. https://doi.org/10.1080/23738871.2018.1513053.

[15] Kanwal, K.; Shi, W.; Kontovas, C.; Yang, Z.; Chang, C.H. (2024). Maritime cybersecurity: Are onboard systems ready? *Maritime Policy & Management*, *51*(3), 484–502. https://doi.org/10.1080/03088839.2022.2124464.

[16] Ashraf, I.; Park, Y.; Hur, S.; Kim, S.W.; Alroobaea, R.; Zikria, Y. B.; Nosheen, S. (2023). Cyber security threats in IoT-enabled maritime industry. *IEEE Transactions on Intelligent Transportation Systems*, *24*(2), 2677–2690. https://doi.org/10.1109/TITS.2022.3164678.

[17] Miller, T.; Durlik, I.; Kostecka, E.; Sokołowska, S.; Kozlovska, P.; Zwolak, R. (2025). Artificial intelligence in maritime cybersecurity: A systematic review. *Electronics*, *14*, 1844. https://doi.org/10.3390/electronics14091844.

[18] Dimakopoulou, A.; Rantos, K. (2024). Comprehensive analysis of maritime cybersecurity landscape based on the NIST CSF v2.0. *Journal of Marine Science and Engineering*, *12*(6), 919. https://doi.org/10.3390/jmse12060919.

[19] Kavallieratos, G.; Diamantopoulou, V.; Katsikas, S. K. (2020). Shipping 4.0: Security requirements for cyber-enabled ships. *IEEE Transactions on Industrial Informatics*, *16*(10), 6617–6625. https://doi.org/10.1109/TII.2020.2976840.

[20] Chupkemi, D.C.; Mersinas, K. (2024). Challenges in maritime cybersecurity training and compliance. *Journal of Marine Science and Engineering*, *12*(10), 1844. https://doi.org/10.3390/jmse12101844.

[21] Bacasdoon, J.; Bolmsten, J. (2022). METI cybersecurity education and training: A multiple case study. *TransNav*, *16*(2), 319–334. https://doi.org/10.12716/1001.16.02.15.

[22] Kayisoglu, G.; Bolat, P.; Duzenli, E. (2023). Modelling maritime cyber security education and training. *Pedagogy*, *95*(6s), 64–78. https://doi.org/10.53656/ped2023-6s.07.

[23] Cabaj, K.; Domingos, D.; Kotulski, Z.; Respício, A. (2018). Cybersecurity education: Evolution of the discipline and master programs. *Computers & Security*, *75*, 24–35. https://doi.org/10.1016/j.cose.2018.01.015.

[24] Peslak, A.; Hunsinger, D. S. (2019). What is cybersecurity and what cybersecurity skills are employers seeking? *Issues in Information Systems*, *20*(2), 62–72. https://doi.org/10.48009/2_iis_2019_62-72.

[25] Pambudi, D.; Hwang, J. (2025). Cybersecurity challenges and adaptive strategies in smart mobility. *Iran Journal of Computer Science*. 1573–1595. https://doi.org/10.1007/s42044-025-00278-0.

[26] Sell, K.; Amella, E.; Mueller, M.; Andrews, J.; Wachs, J. (2015). Individualism and partnership: A descriptive qualitative analysis of the chronic disease phenomenon as perceived by older adults. *Open Journal of Nursing*, *5*(10), Article 99. https://doi.org/10.4236/ojn.2015.510099.

[27] ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection—Information security controls. (accessed on 1 November 2025) Available online: https://www.iso.org/standard/75652.html.

[28] ISO/IEC. (2023). ISO/IEC 27032:2023 — Cybersecurity Guidelines for Internet Security. (accessed on 1 November 2025) Available online: https://www.iso.org/standard/76070.html.

[29] Sugiyono. (2017). Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Alfabeta: Bandung, Indonesia

[30] Castleberry, A.; Nolen, A. (2018). Thematic analysis of qualitative research data. *Currents in Pharmacy Teaching and Learning*, *10*(6), 807–815. https://doi.org/10.1016/j.cptl.2018.03.019.