Cybersecurity Awareness Among Deck Nautical Cadets in the Era of Digital Navigation Systems: A Descriptive Study

Boedojo Wiwoho Soetmoko Jogo [1*]

[1] *Maritime Institute, Sekolah Tinggi Ilmu Pelayaran Jakarta, North Jakarta, Indonesia*

Keywords
cybersecurity awareness; digital navigation systems; ECDIS; maritime cyber risk; deck officer education

Correspondence Email:
Boedojo_Wiwoho@stipmail.ac.id

Abstract
The progressive digitalization of shipboard navigation systems — encompassing Electronic Chart Display and Information Systems, Automatic Identification Systems, GPS-dependent positioning infrastructure, and Vessel Traffic Service communication networks — has created a cybersecurity threat landscape directly relevant to deck officer professional competency that IMO's Maritime Cyber Risk Management guidelines have formally recognized but that maritime vocational education has not yet systematically addressed. This study examines cybersecurity awareness among 10 Deck Nautical cadets at Sekolah Tinggi Ilmu Pelayaran (STIP) Jakarta across three domains: Navigation System Vulnerability Awareness, Cyber Hygiene Behavior, and Incident Response Knowledge. A mixed quantitative design employing Likert-scale self-assessment combined with an objective cybersecurity knowledge test was administered from August 2025 to March 2026. Overall Cyber Awareness Index mean was 2.87/5.00 (Moderate-Low), with Navigation System Vulnerability Awareness (M = 2.84) and Incident Response Knowledge (M = 2.31) falling below functional competency thresholds, and Cyber Hygiene Behavior recording a moderate score (M = 3.47). Objective knowledge test performance averaged 48.3% correct, confirming that self-assessed awareness substantially overestimates actual knowledge. Only 1 of 10 cadets correctly identified IMO Resolution MSC.428(98) as the governance instrument requiring maritime cyber risk integration into the ISM Code. The study establishes the first cybersecurity awareness baseline for DN cadets at STIP Jakarta and provides evidence for the urgency of cybersecurity integration within the Nautika program curriculum.

1. Introduction

The electronic bridge of a modern commercial vessel is a cyber-physical system whose operational integrity depends on the security of the digital networks, software platforms, and data communication channels through which its navigational systems function. The Electronic Chart Display and Information System receives chart updates and correction notices through internet-connected data links. The Automatic Identification System broadcasts and receives vessel identity, position, and voyage data through VHF digital communications channels whose message contents can be manipulated through software-defined radio

equipment available at modest cost. The Global Navigation Satellite System positioning infrastructure on which ECDIS, AIS, and Vessel Traffic Service communication rely is vulnerable to signal spoofing — the broadcast of false positioning signals capable of causing a vessel to display an incorrect position on the ECDIS and transmit that false position to traffic management authorities — a threat whose technical feasibility has been documented in multiple maritime cybersecurity research studies and whose occurrence in real maritime operational contexts has been reported by affected vessel operators [1]. The deck officer who navigates a vessel through congested coastal waters trusting digital navigation system outputs without awareness of these system vulnerabilities is not merely a less-than-ideal professional but a potential safety risk whose graduation from maritime education represents an institutional failure to address a documented and growing operational threat category.

The International Maritime Organization formalized the maritime cyber risk management requirement through Resolution MSC.428(98) in 2017, requiring ship operators to address cyber risks within their Safety Management Systems under the ISM Code by no later than the annual ISM verification due after 1 January 2021, and issued detailed operational guidance through the Maritime Cyber Risk Management in Safety Management Systems circular (MSC-FAL.1/Circ.3) [2]. These instruments establish a regulatory framework for shipboard cyber risk management that has direct implications for deck officers' professional competency requirements: deck officers who are parties to the ISM-required cyber risk assessment and mitigation process aboard their vessels must possess sufficient understanding of shipboard cybersecurity threat categories, vulnerability profiles, and incident response procedures to participate meaningfully in that process. Yet the STCW Convention's Table A-II/1 competency framework, which specifies watchkeeping officer training requirements, does not explicitly include cybersecurity competency among its specified learning outcomes, leaving a regulatory gap between IMO's cyber risk management mandate and the maritime education framework through which that mandate's human capital requirements are supposed to be developed.

Sekolah Tinggi Ilmu Pelayaran Jakarta's Deck Nautical program trains the watchkeeping officers who will navigate Indonesian-flagged and internationally-trading vessels through the increasingly cyber-contested maritime environment that ECDIS dependency and GPS infrastructure vulnerability define. Whether current STIP Jakarta DN cadets possess the cybersecurity awareness — specifically the navigation system vulnerability knowledge, cyber hygiene behavior, and incident response knowledge — that effective IMO cyber risk management requires has not been empirically assessed. This study addresses that empirical gap, pursuing three objectives: first, to measure DN cadet cybersecurity awareness across the three domains of Navigation System Vulnerability Awareness, Cyber Hygiene Behavior, and Incident Response Knowledge using validated self-assessment and objective knowledge instruments; second, to identify the specific knowledge areas and behavioral domains exhibiting the most pronounced deficits; and third, to examine the relationship between self-assessed awareness and objective cybersecurity knowledge as a metacognitive calibration indicator relevant to curriculum design priorities.

1.1 Theoretical Framework

This study frames maritime cybersecurity awareness through the Knowledge-Attitude-Practice (KAP) model — a theoretical framework extensively applied in health education and increasingly in information security awareness research — distinguishing the cognitive dimension of cybersecurity knowledge from the attitudinal dimension of perceived cyber risk relevance and the behavioral dimension of actual cyber hygiene practice [3]. The KAP framework generates a theoretically specific prediction for maritime cybersecurity education: that knowledge (what cadets know about navigation system vulnerabilities), attitude (how relevant they perceive cybersecurity to their professional roles), and practice (what cybersecurity behaviors they actually perform) may be misaligned in ways that aggregate self-reported awareness measures cannot detect, making the combination of Likert-scale self-assessment with objective knowledge testing essential for accurate cybersecurity awareness diagnosis.

Protection Motivation Theory [4], which proposes that individuals' motivation to protect themselves against a threat is a joint function of threat appraisal (perceived threat severity and vulnerability) and coping appraisal (perceived self-efficacy and response effectiveness), provides a complementary framework for understanding why low cybersecurity knowledge may not automatically translate into motivated protective behavior even when threat awareness exists in general terms. Applied to DN cadets' cybersecurity awareness, this framework predicts that the most critical education gap may not be in general threat awareness — cadets may broadly know that ships can be hacked — but in the specific threat appraisal accuracy (understanding of GPS spoofing mechanisms, ECDIS vulnerability pathways) and coping appraisal capacity (knowing how to recognize an anomalous ECDIS display, what to report, and how to respond) that functional maritime cybersecurity professional behavior requires.

2. Method

This study employed a quantitative cross-sectional design combining Likert-scale self-assessment with an objective knowledge test, administered to 10 Level 2 Deck Nautical cadets at STIP Jakarta from August 2025 to March 2026 as part of the institution's Digital Transformation assessment. The n=10 single-program sample is the design-specified data slice for this paper within the broader STIP Jakarta Digital Transformation dataset [5], appropriate for the descriptive baseline assessment that this first-generation institutional cybersecurity awareness study requires and consistent with methodological guidance for pilot-scale diagnostic assessment in specialized professional education contexts [6].

The assessment instrument comprised two components. Component 1 was a 15-item Likert-scale Cyber Awareness Self-Assessment covering three domains of five items each: Navigation System Vulnerability Awareness (NSVA), assessing self-reported understanding of ECDIS/AIS cyber vulnerabilities, GPS spoofing risks, and shipboard network security threats; Cyber Hygiene Behavior (CHB), assessing self-reported password management, software update practices, removable media handling, and network access security behavior; and Incident Response Knowledge (IRK), assessing self-reported understanding of IMO cyber risk management requirements, ISM Code cyber provisions, and on-board cyber incident reporting and response procedures. All items were scored on a five-point Likert scale (1 = No awareness / Never to 5 = Full awareness / Always). Component 2 was a 20-item objective knowledge test assessing factual cybersecurity knowledge across the same three domains, scored dichotomously (correct/incorrect) with percentage accuracy reported by domain and overall. The knowledge test was developed from IMO's Maritime Cyber Risk Management guidance documents [2] and reviewed by one maritime cybersecurity specialist and one STIP Jakarta Nautika lecturer.

Data were analyzed using descriptive statistics for domain-level Likert means and objective knowledge accuracy rates, and Pearson correlations examining the relationship between self-assessed domain awareness and objective knowledge accuracy to assess self-assessment calibration [7].

3. Results and Analysis

3.1 Cyber Awareness Self-Assessment: Likert Domain Profiles

Table 1 presents mean Likert scores across the three cybersecurity awareness domains, revealing a domain-specific awareness profile with significant variation between the moderate Cyber Hygiene Behavior domain and the consistently below-threshold Navigation System Vulnerability Awareness and Incident Response Knowledge domains.

Table 1. Cyber Awareness Self-Assessment Domain Means — DN Cadets, STIP Jakarta (n = 10)

Domain	Mean (SD)	Range	Interpretation
Navigation System Vulnerability Awareness (NSVA)	2.84 (0.94)	1.80–3.60	Moderate-Low
Cyber Hygiene Behavior (CHB)	3.47 (0.82)	2.40–4.60	Moderate

Domain	Mean (SD)	Range	Interpretation
Incident Response Knowledge (IRK)	2.31 (1.02)	1.20–3.80	Low
Overall Cyber Awareness Index (CAI)	**2.87 (0.91)**	**1.80–3.87**	**Moderate-Low**

Scale: 5.00 = Full awareness/Always; 4.00–5.00 = High; 3.00–3.99 = Moderate; 2.00–2.99 = Low-Moderate; 1.00–1.99 = Low

The domain profile in Table 1 reveals that Cyber Hygiene Behavior (M=3.47, Moderate) substantially exceeds the other two domains, reflecting the partial overlap between general digital hygiene behaviors — password management, software update practices — and the everyday digital technology literacy that cadets have developed through personal device use independent of maritime education. Navigation System Vulnerability Awareness (M=2.84, Moderate-Low) and Incident Response Knowledge (M=2.31, Low) represent the maritime-specific cybersecurity knowledge domains requiring formal professional education to develop, and both fall below any reasonable functional competency threshold for deck officers who will be professional parties to ISM-required cyber risk management processes. Incident Response Knowledge's lowest score (M=2.31) is the study's most safety-consequential finding: a deck officer who cannot recognize and respond appropriately to a suspected GPS spoofing or AIS data manipulation incident is professionally unable to fulfill the IMO cyber risk management responsibilities that Resolution MSC.428(98) places on all ISM-covered vessel operators.

3.2 Objective Knowledge Test: Domain-Level Accuracy

Table 2 presents objective knowledge test accuracy by domain, revealing the systematic overestimation of actual cybersecurity knowledge that self-assessment produces.

Table 2. Objective Cybersecurity Knowledge Test Accuracy by Domain — DN Cadets (n = 10)

Domain	Self-Assessed Awareness (1–5)	Objective Knowledge Accuracy (%)	Overestimation Gap
Navigation System Vulnerability (NSVA)	2.84	44.0%	Moderate overestimation
Cyber Hygiene Behavior (CHB)	3.47	64.0%	Small overestimation
Incident Response Knowledge (IRK)	2.31	36.5%	Moderate overestimation
Overall (CAI / Test)	**2.87**	**48.3%**	**17.7 pts gap (self vs. test)**

The 48.3% overall knowledge test accuracy — less than half of items correctly answered — confirms that DN cadets' cybersecurity knowledge is substantially below functional professional competency even in domains where self-assessment suggests moderate awareness. The CHB domain shows the smallest self-assessment overestimation (3.47 self-assessment vs. 64.0% objective accuracy, consistent with the Moderate interpretation), confirming that the everyday digital hygiene knowledge cadets have acquired through personal device experience translates relatively well into objective performance. NSVA and IRK both show moderate overestimation, consistent with Protection Motivation Theory's [4] prediction that individuals in low-threat-exposure environments overestimate their coping capacity for threats they have not directly encountered.

Figure 1 presents five specific knowledge test findings that most directly illuminate the maritime-specific dimensions of the DN cadet cybersecurity knowledge deficit.

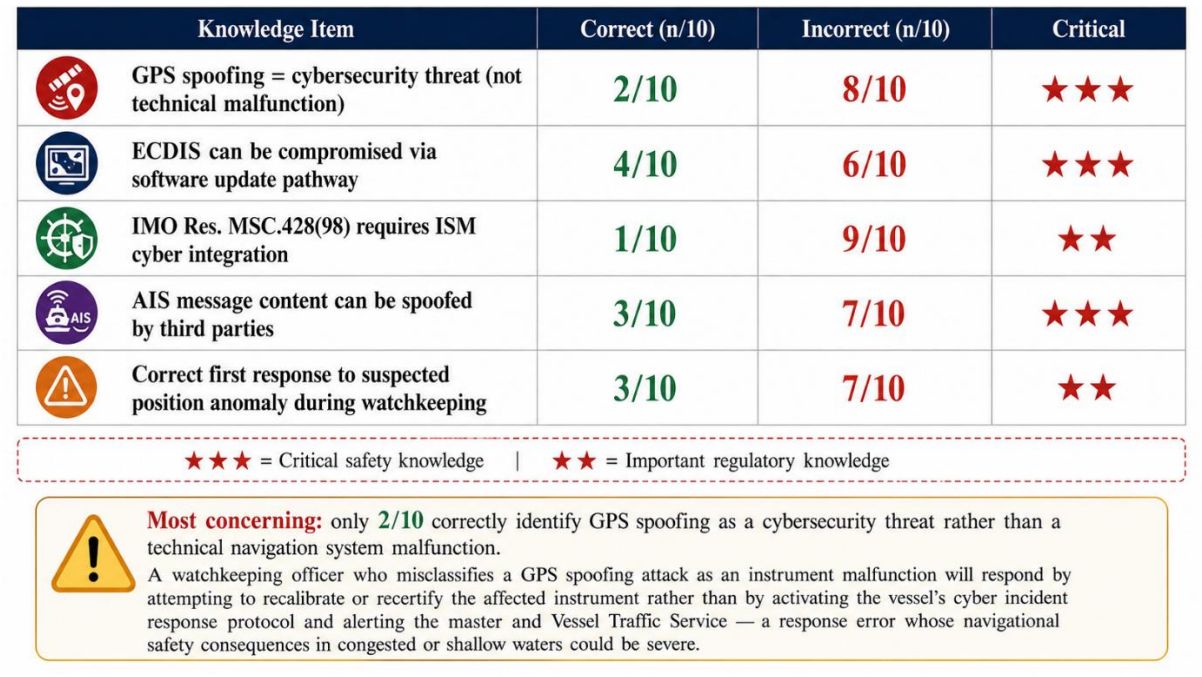

Figure 1. Selected Knowledge Test Item Findings — DN Cadets, STIP Jakarta (n = 10)

The finding that only 2 of 10 cadets correctly identified GPS spoofing as a cybersecurity threat — with the majority attributing hypothetical GPS position anomalies to technical instrument malfunction rather than deliberate external signal manipulation — is the study's most operationally critical knowledge gap finding. A watchkeeping officer who misclassifies a GPS spoofing attack as an instrument malfunction will respond by attempting to recalibrate or recertify the affected instrument rather than by activating the vessel's cyber incident response protocol and alerting the master and Vessel Traffic Service — a response error whose navigational safety consequences in congested or shallow waters could be severe.

3.3 Self-Assessment Calibration Analysis

Pearson correlation between domain-level self-assessment scores and objective knowledge accuracy rates revealed a moderate positive relationship across items ($r = 0.48$, $p = .043$), indicating that self-assessment has modest but statistically significant predictive validity for objective knowledge performance. However, the consistent positive direction of the overestimation gap — self-assessment exceeds objective performance across all three domains — confirms that self-assessment alone is insufficient for cybersecurity awareness diagnostic purposes and that objective knowledge testing is necessary for accurate curriculum gap identification in this domain.

3.4. Discussion

The study's convergent findings — overall Cyber Awareness Index of 2.87 (Moderate-Low), objective knowledge accuracy of 48.3%, and the critical finding that 8 of 10 cadets cannot correctly identify GPS spoofing as a cybersecurity rather than technical threat — establish a cybersecurity awareness deficit among STIP Jakarta DN cadets that has direct and measurable implications for the professional safety competency of the deck officers they are being formed as. The IMO Resolution MSC.428(98) regulatory framework, requiring cyber risk integration into ISM Safety Management Systems by 2021, creates a professional competency expectation for deck officers that the current STCW Table A-II/1 competency framework does not explicitly specify, generating a regulatory-educational gap that this study's knowledge test findings confirm is producing measurable professional knowledge deficits [2].

The GPS spoofing misclassification finding — only 2/10 cadets correctly identifying this attack vector as a cybersecurity rather than technical threat — is theoretically interpretable through the KAP model's distinction between knowledge and practice: cadets may have heard the term "cybersecurity" and may perform basic digital hygiene behaviors with moderate competency, but they have not developed the domain-specific threat conceptual framework necessary to correctly classify novel navigational anomalies as cybersecurity incidents. This is not a digital literacy deficit but a maritime-specific threat modeling deficit: knowing that ships can be attacked through digital channels while being unable to recognize specific attack manifestations in operational navigation contexts reflects the absence of professional-context threat scenario instruction rather than general technological unfamiliarity [8].

The Cyber Hygiene Behavior domain's relatively higher performance (self-assessed M=3.47; objective 64.0%) provides an important pedagogical anchor: cadets already possess foundational digital hygiene knowledge from everyday device use. Cybersecurity curriculum integration in the DN program can build on this existing foundation rather than starting from zero, focusing instructional investment specifically on the maritime-context translation of general cybersecurity principles — how GPS spoofing manifests in ECDIS display anomalies, what AIS data manipulation looks like from the watchkeeping officer's instrument display, and what the ISM cyber incident response procedure requires the watchkeeper to do — that the 2.84 NSVA and 2.31 IRK scores confirm is most urgently absent [9].

4. Conclusion

This study has documented a cybersecurity awareness deficit among Deck Nautical cadets at STIP Jakarta that is most critically expressed in GPS spoofing misclassification, AIS vulnerability awareness, and IMO cyber risk management regulatory knowledge — the maritime-specific threat categories and professional responsibilities that everyday digital literacy does not develop and that the current Nautika curriculum does not address. An overall Cyber Awareness Index of 2.87 (Moderate-Low) and objective knowledge accuracy of 48.3% establish that cybersecurity is a documented professional competency gap in the current DN cadet population. These findings provide STIP Jakarta's Nautika curriculum with the first empirical baseline for a cybersecurity integration initiative specifically targeting navigation system vulnerability awareness and IMO-aligned incident response knowledge development.

5. References

[1] B. Svilicic, J. Kamber, S. Kasum, and D. Mohovic, "Improving maritime cybersecurity using advanced vulnerability assessment of ECDIS hardware," *J. Mar. Sci. Eng.*, vol. 9, no. 1, 2021. DOI: 10.3390/jmse9010067

[2] International Maritime Organization, "Maritime Cyber Risk Management in Safety Management Systems," MSC-FAL.1/Circ.3, IMO Publishing, London, 2017.

[3] B. K. Rimal, S. M. Paudel, and R. S. Bam, "Knowledge-attitude-practice study in health-related fields: a methodological review," *J. Inst. Med.*, vol. 43, no. 1, pp. 3–11, 2021.

[4] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," *J. Psychol.*, vol. 91, no. 1, pp. 93–114, 1975. DOI: 10.1080/00223980.1975.9915803

[5] J. W. Creswell and V. L. Plano Clark, *Designing and Conducting Mixed Methods Research*, 3rd ed. Thousand Oaks, CA: Sage Publications, 2017.

[6] A. Field, *Discovering Statistics Using IBM SPSS Statistics*, 5th ed. London: Sage Publications, 2018.

[7] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qual. Res. Psychol.*, vol. 3, no. 2, pp. 77–101, 2006. DOI: 10.1191/1478088706qp063oa

[8] K. Bogusławski, M. Gil, J. Nasur, and K. Wróbel, "Implications of autonomous shipping for maritime education and training: the cadet's perspective," *Marit. Econ. Logist.*, vol. 24, no. 2, pp. 327–343, 2022. DOI: 10.1057/s41278-022-00217-x

[9] A. Wahid, M. Y. Jinca, T. Rachman, and J. Malisan, "Determination of Indicators of Implementation of Sea Transportation Safety Management System for Traditional Shipping Based on Delphi Approach," *Sustainability*, vol. 15, no. 13, 2023. DOI: 10.3390/su151310080

[10] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Q.*, vol. 13, no. 3, pp. 319–340, 1989. DOI: 10.2307/249008

[11] F. Mutohhari, P. Sudira, F. D. Isnantyo, and N. W. A. Majid, "Generic green skills: maturity level of vocational education teachers and students in Indonesia," *Int. J. Eval. Res. Educ.*, vol. 14, no. 1, pp. 179–187, 2025. DOI: 10.11591/ijere.v14i1.29191

[12] L. Widaningsih, S. Rahayu, V. Dwiyanti, and W. Widanengsih, "Analysis and Mapping of Technical Competency Needs for TVET Teachers in the Era of Industry 4.0," *J. Tech. Educ. Train.*, vol. 17, no. 2, pp. 151–164, 2025. DOI: 10.30880/jtet.2025.17.02.011

[13] H. Li, S. I. Khattak, X. Lu, and A. Khan, "Greening the Way Forward: A Qualitative Assessment of Green Technology Integration and Prospects in a Chinese Technical and Vocational Institute," *Sustainability*, vol. 15, no. 6, 2023. DOI: 10.3390/su15065187

[14] International Maritime Organization, "Resolution MSC.428(98) — Maritime Cyber Risk Management in Safety Management Systems," IMO Publishing, London, 2017.

[15] R. S. Wulandari and T. Cahyadi, "Engineering Technology and Education in Maritime Studies: A Qualitative Examination," *J. Eng. Sci. Technol.*, vol. 20, no. 2, pp. 28–35, 2025.