TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 19
Number 3
September 2025
DOI: 10.12716/1001.19.03.01

Development of Maritime Cybersecurity Protocols – Enhancing Awareness on Cyberthreats in Maritime Transport

G. de Melo Rodriguez[1], A. Chronopoulos[2], T. Gregorič[3], I. Bodus-Olkowska[4], L. Singh[5], M. Dramski[6], K. Karampidis[7], A. Bautu[8], N. Wawrzyniak[4] & I. Garczyńska-Cyprysiak[4]
[1] *Technical University of Catalonia, Catalonia, Barcelona, Spain*
[2] *IDEC SA, Pireas, Greece*
[3] *Spinaker d.o.o., Portoroz, Slovenia*
[4] *Maritime University of Szczecin, Szczecin, Poland*
[5] *Centre for Factories of the Future Sweden AB, Alingsas, Sweden*
[6] *Sealearn Technologies Sp. z o.o., Szczecin, Poland*
[7] *Hellenic Mediterranean University, Heraklion, Greece*
[8] *Romanian Naval Academy, Constanca, Romania*

ABSTRACT: The paper presents collaborative research conducted by European researchers, mariners, and cybersecurity experts on identifying and developing preventive procedures for maritime cybersecurity within the CyberSEA project. The project's objective is to equip seafarers with the necessary knowledge to detect and respond effectively to cyber threats, minimizing the risk of disruptions to maritime operations. The research included several key tasks aimed at developing the proposed cybersecurity protocols. The initial phase involved identifying cyber vulnerabilities in the maritime sector and defining the main risk areas. Subsequently, 34 real-life scenarios were constructed to illustrate these threats. Comprehensive desk research was conducted on best cybersecurity practices in other industries that were transferable to the maritime sector to establish a set of preventive measures. The final phase resulted in the development of 10 detailed protocols for seafarers, specifying the procedural steps to be taken in response to distinct cyber threats. The study highlights the essential role of human factors and education in maritime cyber resilience, offering a transferable framework for integration into Safety Management Systems and vocational training curricula.

1 INTRODUCTION

The maritime industry's increasing dependence on digital technologies for navigation, communication, propulsion, and cargo operations has significantly expanded its vulnerability to cyber threats. The convergence of Information Technology (IT) and Operational Technology (OT) onboard vessels has created complex, interconnected systems that are often inadequately protected against cyber risks. As a response to this emerging threat landscape, the International Maritime Organization (IMO) mandated the integration of cyber risk management into Safety Management Systems (SMS) through Resolution MSC.428(98) [6], supplemented by detailed technical guidance in MSC-FAL.1/Circ.3/Rev.2 [7] and MSC.1/Circ.1639 [8].

Despite the existence of such regulatory instruments, effective implementation at the operational level remains limited. Studies show that the human element is frequently the weakest link in maritime cybersecurity, underscoring the urgent need for systematic training and awareness programs [3]. A Delphi study by Chowdhury et al. [4] demonstrated that cybersecurity training in critical infrastructure sectors must be both modular and scenario-based to be effective—especially in complex, high-risk environments like shipping. However, current training frameworks do not yet include standardized cybersecurity learning outcomes, leaving a gap in the formal and informal education of seafarers.

The CyberSEA project (2023-1-ES01-KA220-VET-000159793), co-funded by the European Union under Erasmus+, aims to address this gap through the

development of evidence-based training resources and system-specific cybersecurity protocols. One of the foundational pillars of the project is the recognition that maritime cyber resilience must be approached as a multidisciplinary educational challenge, integrating technical knowledge with procedural competence and human-centered risk awareness [1], [2]. Drawing on cross-sectoral practices and lessons learned from cybersecurity education in other high-stakes domains [11], CyberSEA adopts a modular and holistic framework for enhancing cyber readiness in maritime vocational education and training.

A central element of this effort was the development of structured cybersecurity protocols tailored to critical maritime subsystems. The design of these protocols is rooted in a system-level vulnerability assessment, supplemented by cross-industry best practices [10], [5], and validated through the analysis of real and hypothetical cyber incidents affecting maritime operations [9]. The goal was to ensure that the protocols not only align with international regulatory standards but also support practical implementation onboard, bridging the gap between policy and practice.

The structure and methodology adopted in this research reflect contemporary thinking on educational design for cyber resilience, emphasizing applied learning, modularity, and contextualization [1], [2], [4]. Ultimately, the protocols produced in CyberSEA are intended to inform the evolution of training frameworks thereby contributing to a more resilient and operationally prepared maritime workforce.

2 IDENTIFICATION OF CYBER VULNERABILITIES AT SEA

First task of the research was dedicated to a comprehensive identification of cyber vulnerabilities affecting maritime operations. The goal was to systematically assess risk-prone systems and establish a knowledge base that would inform the development of targeted cybersecurity protocols and training resources for seafarers. Structured risk assessment framework across ten critical maritime systems, encompassing both onboard and port infrastructure was applied. These main areas of risks were specified as:

- Navigation Systems
- Communication Networks
- Propulsion and Engine Control Systems
- Cargo Management Systems
- Satellite Communication Systems
- Power Management Systems
- Integrated Bridge Systems
- Passenger and Crew Management Systems
- Weather Monitoring Systems
- Onboard Entertainment Systems

For each system, a detailed analysis was performed based on expert consultation, technical documentation, real-world case reports, and cyber incident records. Identified threats were evaluated using a quantitative risk matrix adapted from the Health and Safety Executive (HSE) ALARP model, combining the dimensions of severity, likelihood, and impact. The risk scores ranged from 1 (low) to 25 (critical), allowing prioritisation of cybersecurity measures. The analysis resulted in a risk-weighted inventory of threats, which served as the foundation for the later development of mitigation strategies and training protocols.

Table 1.

System	Cyber Threat / Vulnerability	Potential Consequences	Estimated Risk Score
Navigation Systems	GPS Spoofing / Jamming	Vessel misrouting, grounding, or collision	20
Navigation Systems (ECDIS, AIS)	Malware Infiltration	Corrupted navigation data, route manipulation	18
Communication Networks	Unauthorized Access / Data Breach	Disruption of internal communications, data theft	16
Propulsion and Engine Control	System Compromise via OT interface	Loss of control over propulsion, potential mechanical damage	20
Cargo Management Systems	Data Manipulation / Ransomware	Incorrect cargo tracking, port delays, revenue loss	16
Power Management Systems	Centralised control failure / malware	Total loss of shipboard electrical systems	25 (Critical)
Satellite Communication Systems	Signal Interference / Spoofing	Loss of connectivity, misinformation	14
Integrated Bridge Systems	Aggregated system dependency	Cascading failure of navigation, communication, and monitoring systems	17
Passenger & Crew Systems	SQL Injection / Phishing	Exposure of personal data, platform hijack	12
Weather Monitoring Systems	Data tampering / sensor spoofing	Inaccurate forecasts, unsafe routing decisions	13

The highest-scoring risk was associated with power management systems, rated at a maximum risk score of 25, given their central role in maintaining shipboard functionality and safety. Navigation-related disruptions and propulsion system compromise followed closely with risk scores around 20. AIS spoofing, SQL injection, and unauthorized system access were rated as medium risks, generally scoring around 12. The overall average risk score across all systems was 16.8, highlighting a generally high level of cyber exposure in the maritime sector. Notably, vulnerabilities in integrated bridge systems, which combine multiple control interfaces, were found to amplify risk due to the potential for cascading failures.

3 DESK RESEARCH ON BEST CYBERSECURITY PRACTISES

Having determined the biggest vulnerabilities, the research focused on identifying, analysing, and transferring effective cybersecurity practices from other sectors into the maritime domain. Recognizing that the maritime industry often lags behind other critical sectors in cyber preparedness, the goal of this task was to establish a foundation of transferable cybersecurity measures that could be adapted to the operational realities of shipping, ports, and also maritime education institutions.

The task employed a structured desk research methodology, involving the comparative review of cybersecurity governance frameworks, technical standards, and operational policies across seven

European countries: Germany, Sweden, Greece, Poland, Romania, Finland, and Spain. The analyzed organizations represented diverse sectors including education, information technology, telecommunications, construction, and logistics. Each case study examined a wide range of practices across several domains:

- Governance and Policy Frameworks (e.g., presence of cybersecurity policies, adherence to standards such as ISO/IEC 27001 and NIS2)
- Access Control and Authentication (e.g., RBAC, MFA, VPN usage)
- Data Protection (e.g., encryption, backup regimes, data retention policies)
- Network and Infrastructure Security (e.g., firewalls, intrusion detection/prevention systems)
- Incident Response and Monitoring (e.g., security logging, automated alerts, structured response plans)
- Employee Training and Awareness (e.g., phishing simulations, mandatory e-learning modules)
- Mobile Device and BYOD Policies (e.g., device control, encryption requirements)
- Third-Party Risk Management (e.g., vendor assessments, contractual clauses)

The analysis of these cross-sectoral cybersecurity practices reveals that while levels of cyber maturity differ significantly across industries and national contexts[fig.1], there are recurring, transferable best practices that offer strong potential for adaptation within the maritime domain.

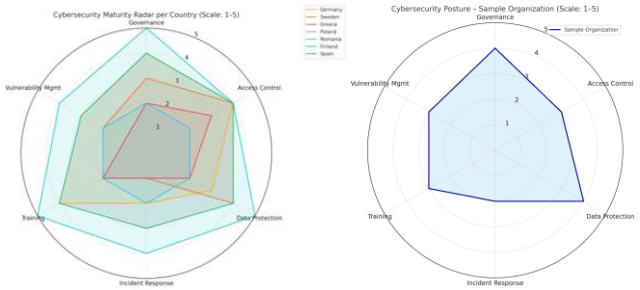

Figure 1. Radar charts comparing cybersecurity maturity across six key domains. Right: representative cybersecurity posture of a sample organization, based on synthesized patterns observed in the desk research. Right: comparative national-level profiles derived from best practices identified across seven countries (Germany, Sweden, Greece, Poland, Romania, Finland, Spain).

One of the most prevalent findings was the widespread adoption of cybersecurity policy frameworks in medium and large organizations. For example, institutions in Germany and Sweden consistently aligned their internal policies with ISO/IEC 27001, while entities in the UK and Finland also referenced NIS2 and GDPR-aligned practices. These policies were complemented by structured governance models wherein cybersecurity responsibilities were clearly delegated—either to Chief Information Security Officers (CISOs) or to interdisciplinary IT committees. While maritime stakeholders often lack such formal structures onboard, the implication was that vessels and shipping companies must adopt similar hierarchical and accountable frameworks, especially regarding bridge, propulsion, and communication systems.

Authentication and access control practices were particularly advanced in sectors dealing with sensitive data. 85% of the organizations surveyed enforced multi-factor authentication (MFA) for critical access points, often supplemented by role-based access control (RBAC) and user-specific VPN tunneling. Authentication methods ranged from token-based entry (e.g., YubiKeys in Sweden) to biometric and token-based identity validation. Moreover, access logs were monitored and archived for security audits, with high-risk access zones (e.g., server rooms or control systems) under physical surveillance. In contrast, maritime systems—especially onboard navigation consoles—frequently operate on default credentials or shared logins, exposing a serious gap. Implementing vessel-specific RBAC profiles with MFA for ECDIS, propulsion interfaces, and cargo systems is a minimum standard that should be enforced under IMO guidelines.

On the technical side, data protection protocols varied in robustness. While 90% of reviewed organizations used encryption-at-rest and in-transit, only 60% actively monitored or updated their encryption protocols. Daily or weekly backup routines were standard across all institutions, typically using cloud-based or geographically redundant storage. Several German and Swedish organizations utilized AES-256 encryption in conjunction with automated patch management tools, ensuring system resilience and quick recovery in case of breach. In maritime terms, this underscores the necessity for encrypted backup of navigation data, propulsion configurations, and crew records, ideally on both local (air-gapped) and satellite-synchronized backups. Furthermore, system updates and vulnerability scans, while routine in land-based sectors, were absent in many maritime scenarios, despite the proliferation of maritime-targeted malware such as NotPetya and Ryuk.

Another insight was the emphasis placed on user awareness and simulation-based training. Organizations in Greece, Poland, and Finland routinely conducted phishing simulations, reporting a 40–60% improvement in user response after repeated drills. In contrast, maritime crews often lack structured cybersecurity training. Implementing annual cyber awareness programs, tailored to officer ranks and operational roles, would directly address this deficit. Especially impactful were incident response frameworks that included predefined roles, escalation protocols, and communication templates. These were tested via tabletop exercises or red team simulations at least annually. Such approaches are notably absent from current STCW-aligned training syllabi, representing a key opportunity for the CyberSEA project to propose amendments at both institutional and regulatory levels.

To summarize, key recommendations include the adoption of ISO-based governance structures, systematic access segmentation, comprehensive encryption, regular backup audits, and perhaps most importantly crew-centric awareness training.

4 REAL LIFE SCENARIOS OF CYBERTHREATS AT SEA

The identification of cyber vulnerabilities in maritime systems together with a review on cybersecurity practices, provided the structural foundation for the development of scenario-based training materials. Recognizing that the theoretical mapping of vulnerabilities must be anchored in operational realities to be pedagogically effective, next task focused on compiling, structuring, and analysing a comprehensive set of cyber incident scenarios. These were drawn from three complementary sources: (1) well-documented real-world maritime cyberattacks, (2) lesser-known or confidential incidents partially disclosed in industry and academic channels, and (3) hypothetical, yet technically plausible, threat situations extrapolated from similar sectors or system architectures. Each scenario was developed with reference to one of the ten critical maritime subsystems mentioned in chapter 2: navigation, propulsion, power, communication, satellite connectivity, cargo, weather monitoring, entertainment, integrated bridge, and crew/passenger systems.

Each scenario developed in WP2.T4 follows a standardized analytical structure, intended to enable reproducibility, pedagogical clarity, and operational relevance. The framework includes the following elements:

- Description of Incident: A factual or constructed narrative detailing how the cyber event unfolded, including method of access, targeted system, and timeline.
- Identified Threat: A succinct technical formulation of the core cyber threat (e.g., ransomware, spoofing, malware injection).
- Result of Threat: Operational and/or safety-related outcomes of the attack (e.g., cargo rerouting, denial of propulsion, communication blackout).
- How to Identify / What to Monitor: Practical indicators for detection and awareness (e.g., abnormal sensor readings, system lag, unknown logins).
- Solutions / Mitigation Measures: Proposed countermeasures, often aligning with existing best practices (e.g., multi-factor authentication, endpoint hardening).
- Sources: Documentation or references supporting the scenario's construction (academic articles, incident reports, news sources, etc.).

A total of 34 scenarios were developed. While the scenarios span a wide spectrum of complexity and origin, several cross-cutting themes emerge that highlight the evolving threat landscape in maritime cyber risk. In navigation systems, scenarios focused on GPS spoofing, AIS manipulation, and ECDIS malware infections. One example involved the deliberate falsification of vessel position data via GNSS spoofing, leading to near-grounding events in congested traffic zones. Scenarios emphasize the need for redundant position sources (e.g., radar-based fixes) and crew training on anomaly recognition in bridge displays. Cargo management system scenarios were particularly rich, including high-profile cases such as the NotPetya attack on Maersk. Another detailed a criminal organization's compromise of an Australian customs database, enabling illicit cargo routing. These cases illustrated how supply chain integration and shore-side access vectors can cascade into onboard consequences, particularly when authentication and access logging are weak. In power and propulsion systems, threats ranged from remote command injection via insecure remote maintenance channels to malware disrupting engine control units. For instance, one scenario described the infiltration of an auxiliary power system during shore-side servicing, which led to propulsion failure mid-voyage. Satellite and communication systems were often targeted through jamming, signal interference, or unencrypted backchannel exploitation. One real-life case involved a transatlantic vessel approaching the Port of New York whose control systems were degraded by malware delivered via a crew USB stick. Scenarios involving crew and passenger systems typically illustrated threats of a social engineering nature—phishing, credential harvesting, and SQL injection into manifest or personnel databases. Suggested mitigations included phishing awareness drills, MFA, and audit logging with anomaly detection. Even systems such as onboard entertainment and weather monitoring—often considered peripheral—were shown to be exploitable. A DDoS attack on an infotainment server was found to spread laterally due to poor network segmentation, affecting navigation displays. These highlight the importance of treating all IT-connected systems as part of a unified security perimeter.

The analysis reveals that most incidents share a common vulnerability: the human-system interface. Whether through poor credential practices, unverified device use, or the misinterpretation of corrupted data, crew behaviour plays a central role in either amplifying or mitigating cyber impact. Therefore, scenario-based training should not only deliver technical know-how, but also cultivate situational awareness, discipline in procedural compliance, and the confidence to act decisively under uncertainty.

5 DEVELOPMENT OF PROTOCOLS

The last step of the research was to develop procedural guides designed to support timely, informed, and consistent responses to cyber threats within critical shipboard and port-related systems. These protocols goal was enabling both reactive and preventive capabilities among maritime personnel. Each protocol was intended to address a particular category of system risk, in alignment with the defined previously risk domains and enriched through scenario-based analysis.

Each protocol follows a unified structure comprising:

- Purpose and Scope
- Applicable Regulations and Standards (e.g., IMO MSC-FAL.1/Circ.3, ISO/IEC 27001, NIS2)
- Roles and Responsibilities
- Risk Assessment and Threat Identification
- Technical and Procedural Cybersecurity Controls
- Incident Response and Recovery Procedures
- Training and Awareness Requirements
- Communication and Coordination Measures
- Audit, Compliance, and Review Cycles

It ensures interoperability with both the ISM Code and vessel-specific Safety Management Systems (SMS), while remaining adaptable to regulatory updates and emerging threats. It also includes the incident response plan, which outlines the roles, actions, and handovers required to effectively detect, contain, and recover from cyber incidents. The plan is structured across stakeholder roles [Fig.2] ensuring clarity of responsibility and coordinated decision-making throughout the response lifecycle.

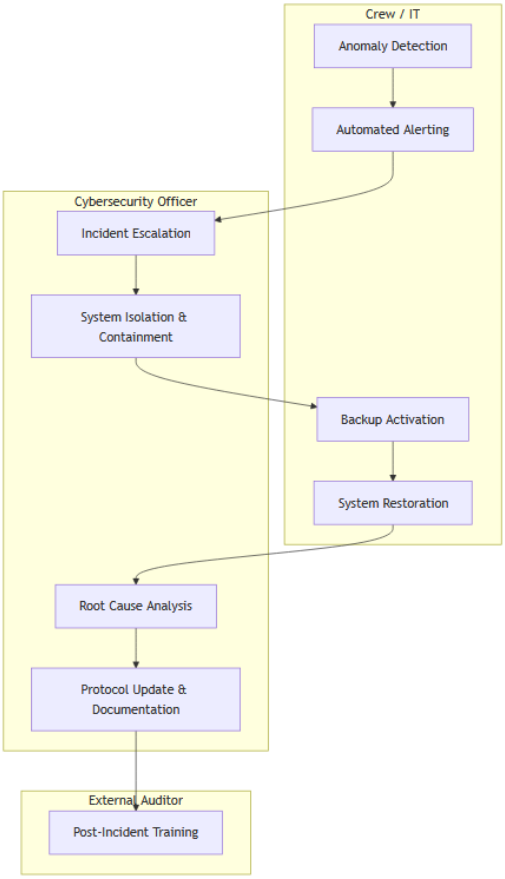

Figure 2. Workflow of the cybersecurity incident response plan, structured by role

A distinctive feature of the protocols is their tailored system specificity. For example, the protocol for navigation systems emphasizes redundancy through cross-verification of positional data (e.g., GPS vs. radar), strong authentication for ECDIS access, and USB device control. In contrast, the protocol for satellite communications focuses on encryption standards (AES-256, TLS 1.3), jamming resistance, and coordination with satellite service providers. Likewise, for cargo systems, the emphasis is placed on securing IoT-enabled monitoring devices, database integrity, and mitigation of ransomware attacks—a direct response to vulnerabilities documented in the Maersk NotPetya case and other real-world disruptions.

Importantly, the protocols extend beyond technology. Human factors are addressed through detailed training guidelines, which call for simulation-based exercises, annual refresher courses, phishing awareness modules, and specialized drills based on the WP2.T4 scenario set. For instance, the protocol for crew and passenger management systems includes guidelines for detecting phishing attempts and responding to social engineering attacks, which were shown to be prevalent vectors in prior incidents.

To ensure adaptability over time, each protocol includes a review and update cycle, typically conducted biannually, and includes triggers for immediate revision in response to significant cyber events, regulatory changes, or newly identified vulnerabilities. This dynamic framework is essential in the face of evolving threats such as AI-driven malware or quantum-resilient encryption requirements.

6 SUMMARY

The study presented a structured approach to the identification, analysis, and mitigation of cyber threats in the maritime sector, conducted within the framework of the CyberSEA project. The methodology was grounded in a system-level perspective, beginning with the classification of key maritime subsystems and their associated vulnerabilities, through a cross-sectoral review of cybersecurity best practices, development of realistic threat scenarios and formulation of dedicated cybersecurity protocols.

The vulnerability assessment revealed a wide spectrum of cyber risks across ten core operational domains, ranging from GPS spoofing in navigation systems to malware infiltration in cargo and communication networks. These findings informed the compilation of 34 cyberthreat scenarios, which served as empirical or semi-empirical models for understanding system-specific threats, response gaps, and potential mitigation strategies. These scenarios also provided the foundation for the design of targeted, practical training content for seafarers.

Based on these analytical components 10 structured cybersecurity protocols were developed, each corresponding to a specific shipboard or port-related subsystem. The protocols integrate technical controls, procedural safeguards, incident response guidelines, and training requirements, all aligned with applicable standards such as IMO MSC-FAL.1/Circ.3 and ISO/IEC 27001. Their development reflects both the operational needs of the maritime sector and the requirement for systematic integration of cybersecurity into broader safety and risk management frameworks.

The outcomes of this work contribute to the ongoing discourse on maritime cyber resilience by offering a coherent, evidence-based methodology for transitioning from risk identification to protocol implementation. Future work, including the validation of these protocols through training pilots and simulation exercises, will further inform their practical applicability and scalability across maritime training institutions and operational contexts.

ACKNOWLEDGEMENT

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union (Proj. no: 2023-1-ES01-KA220-VET-000159793). The opinions and points of view expressed in this publication commit only the authors and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of

Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them. For more information on the project please visit: www.cybersea-project.eu

REFERENCES

[1] Aris S., Isa W., Yahaya W. and Mohamad S., Multidisciplinary curriculum design approaches towards balanced and holistic graduates, 2017 IEEE 9th International Conference on Engineering Education (ICEED), Kanazawa, Japan, 2017, pp. 17-22, doi: 10.1109/ICEED.2017.8251157.

[2] Oruc, A., Chowdhury, N. & Gkioulos, V. A modular cyber security training programme for the maritime domain. Int. J. Inf. Secur. 23, 1477–1512 (2024). https://doi.org/10.1007/s10207-023-00799-4

[3] Goh P., Humans as the weakest link in maintaining cybersecurity: building cyber resilience in humans Introduction To Cyber Forensic Psychology: Understanding The Mind Of The Cyber Deviant Perpetrators (2021), pp. 287-305, https://doi.org/10.1142/9789811232411_0014

[4] Chowdhury N., Katsikas S., Gkioulos V., Modeling effective cybersecurity training frameworks: A delphi method-based study, Computers & Security, Vol. 113, p. 102551 2022, https://doi.org/10.1016/j.cose.2021.102551

[5] Class, N.K.: Guidelines for designing cyber security onboard ships. Tokyo, Japan, 2020. https://www.nextdeal.gr/sites/default/files/sitefiles_2020-07/ guidelines_for_designing_cyber_security_onboard_ships.pdf (visited: 11.04.2025)

[6] IMO. MSC 98/5/2 Measures to enhance maritime security. The incorporation of cyber risk management in Safety Management Systems. London, UK, 2017

[7] IMO. MSC-FAL.1-Circ.3-Rev.2 Guidelines on maritime cyber risk management. London, UK, 2022

[8] IMO. MSC.1/Circ.1639 The guidelines on cyber security onboard ships. London, UK, 2021

[9] Akpan, F.; Bendiab, G.; Shiaeles, S.; Karamperidis, S.; Michaloliakos, M. Cybersecurity Challenges in the Maritime Sector. Network 2022, 2, 123-138. https://doi.org/10.3390/network2010009

[10] ANSSI. Best practices for cyber security on board ships. 2016 https://cyber.gouv.fr/sites/default/files/2017/06/best-practices-for-cyber-security-on-board-ships_anssi.pdf (visited 11.04.2025)

[11] Bacasdoon et al.: A multiple case study of METI cybersecurity education and training: A basis for the development of a guiding framework for educational approaches. In: TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation 16.2 (2022), pp. 319–334. https://doi.org/10.12716/1001.16.02.15