MBNA Publishing House Constanta 2025


# Proceedings of the International Scientific Conference SEA-CONF

SEA-CONF PAPER • OPEN ACCESS

## Increasing cybersecurity at sea – an update on the CyberSEA Project

To cite this article: A. BAUTU, N. WAWRZYNIAK, GERMAN DE MELO RODRIGUEZ, A. CHRONOPOULOS, L. SINGH, K. KARAMPIDIS, M. VASILAKIS, M. DRAMSKI, M. KLEIN, T. GREGORIČ, Proceedings of the International Scientific Conference SEA-CONF 2025, pg. 90-94.

Available online at www.anmb.ro

**ISSN: 2457-144X; ISSN-L: 2457-144X**

doi: 10.21279/2457-144X-25-011

# Increasing cybersecurity at sea – an update on the CyberSEA project

**Andrei Bautu[1,*], Natalia Wawrzyniak[2], German de Melo Rodriguez[3], Aris Chronopoulos[4], Lakhvir Singh[5], Konstantinos Karampidis[6], Manos Vasilakis[7], Mariusz Dramski[8], Monika Klein[9], Tomaz Gregorič[10]**

[1*] Romanian Naval Academy, Romania, andrei.bautu@anmb.ro
[2] Maritime University of Szczecin, Poland, n.wawrzyniak@pm.szczecin.pl
[3] Universitat Politècnica de Catalunya, Spain, german.de.melo@upc.edu
[4] IDEC SA, Greece, aris@idec.gr
[5] Centre for Factories of the Future, Sweden, lakhvir.singh@c4ff.se
[6] Hellenic Mediterranean University, Greece, karampidis@hmu.gr
[7] Hellenic Mediterranean University, Greece, mvasilakis@hmu.gr
[8] Sealearn Technologies, Poland, m.dramski@sealearn.pl
[9] Berlin School of Business and Innovation, monika.klein@berlinsbi.com
[10] Spinaker d.o.o., Slovenia, tomaz.gregoric@spinaker.si

**Abstract**. In the context of the accelerated digitalization of the maritime industry, cybersecurity is becoming an essential pillar for the safety of ships, crews and port infrastructures. The CyberSEA project - Increasing Cyber Security at SEA through digital training responds to this need through a complex and structured approach, focused on identifying cyber vulnerabilities specific to the maritime sector, developing dedicated protocols, as well as training future and current seafarers through modern digital learning methods. This article provides an updated overview of the progress made within the project, presenting the main activities carried out so far, the results obtained and the prospects for their application in the maritime professional environment. Contributions in the field of applied research, professional training and educational innovation in the context of maritime cybersecurity are highlighted.
**Keywords:** maritime cybersecurity, digital training, maritime protocols, virtual labs

## 1. Introduction

Cybersecurity has become a major concern in the maritime industry, as commercial ships, port systems and maritime logistics infrastructure become increasingly dependent on digital and interconnected solutions. Cyber vulnerabilities can have serious consequences: from the disruption of naval operations to compromising the physical safety of crew and the environment. In this context, a concerted effort is needed to assess cyber risks specific to the maritime sector and to train seafarers to prevent and manage them.

The CyberSEA project - Increasing Cyber Security at SEA through digital training, funded by the Erasmus+ programme, aims to actively contribute to increasing cyber resilience in the maritime domain through a combination of applied research, development of specific protocols and advanced

digital training. The project activities aim not only to identify cyber threats, but also to create a modern, comprehensive and accessible educational framework, adapted to the real needs of teachers, cadets and seafarers in action.

This article provides an update on the progress made within the CyberSEA project, highlighting key milestones, resources developed, and potential impact on maritime cybersecurity training.

## 2. Methodology

The activities of the *CyberSEA – Increasing Cyber Security at SEA through digital training* project are organized around an applied research methodology, which combines technical assessment of cyber vulnerabilities with modern educational practices, aiming to create concrete tools for increasing cyber resilience in the maritime domain.

The methodological approach was structured in three major work directions:

*1. Identification of cyber risks and vulnerabilities in maritime transport*

This stage consisted of a systematic analysis of critical maritime systems – including navigation, communications, propulsion, cargo management and satellite communications – in order to identify potential entry points for cyber attacks. Both documentary sources (incident reports, case studies) and consultations with experts in the field were used to build a validated database of risk scenarios and triggers (ANSSI, 2016).

*2. Adapting good practices from other critical industrial sectors*

Starting from the idea that the maritime industry can learn from the experience of more advanced fields in terms of cybersecurity, like IT, telecom, education, logistics, etc., the project team carried out a comparative research in seven European countries. This aimed to analyze governance policies, authentication and access control, encryption, incident response plans and personnel training. The results were adapted to maritime operational realities, taking into account the specifics of the vessels and the level of technological maturity of the operators.

*3. Developing maritime cyber scenarios and protocols*

Based on previous analyses, more than 30 cyber attack scenarios were developed, inspired by real incidents, industry reports or realistic projections on maritime systems. Each scenario was structured on essential components: attack vector, warning signals, operational consequences and response measures. On this foundation, 10 cyber protocols were developed, each dedicated to a maritime subsystem (e.g. navigation, propulsion, communication systems, etc.), in line with IMO standards and international norms (e.g. ISO/IEC 27001, NIS2). The protocols include both technical measures and procedures for crew training and incident management.

The project methodology emphasizes the integration of risk assessment, contextualized training and practical application tools. This approach allows the adaptation of the results into shipboard safety management systems (SMS), as well as into the curricula of maritime education institutions.

## 3. Rezultate

To date, the CyberSEA project has generated a series of concrete results, with direct applicability in increasing the level of cybersecurity in maritime transport. These fall into three complementary directions: applied research, development of educational content, and creation of digital infrastructure for practical training.

### *3.1. Maritime cyber protocols*

Based on the analysis of critical maritime systems and attack scenarios, the project team has developed 10 protocols dedicated to different subsystems on board ships: navigation, propulsion, communications, cargo, power supply, satellite connectivity, weather monitoring, entertainment equipment, crew management and integrated command systems. Each protocol includes preventive measures and operational reactions to cyber incidents, being aligned with IMO regulations (IMO,

2021), (IMO, 2022) and international standards such as ISO/IEC 27001 or NIS2. The protocols are designed to be easily integrated into Safety Management Systems (SMS) and can serve as a basis for internal audits or crew training.

### *3.2. Educational scenarios based on real incidents*

More than 30 educational scenarios have been developed, built on real incidents, industry reports or credible hypothetical situations. These scenarios cover a wide range of threats: GPS spoofing, malware infections in ECDIS systems, ransomware attacks on cargo systems, compromise of communication systems via infected USBs, SQL injection on personnel databases, etc. Each scenario is accompanied by recommendations for early recognition, indicators of abnormal behavior, and concrete prevention and remediation measures.

### *3.3. Curriculum and training materials*

A modern curriculum has been defined for a cybersecurity training course dedicated to merchant marine officers (Chowdhury, 2022) (Oruc, A, 2024). It includes modular content, adaptable for different levels of experience, covering both the technical component (threat identification, security controls, incident response) and the human component (human risk factors, social engineering, security culture). The course materials include graphic resources, explanatory videos, interactive presentations and exercises based on the described scenarios.

### *3.4. E-learning platform and CyberSEA Virtual Hub*

In order to ensure flexible and interactive access to training, the CyberSEA Virtual Hub was designed and implemented – a platform that hosts remote laboratories dedicated to maritime cybersecurity training. The platform integrates functionalities such as:

- secure authentication and distinct roles for learners and trainers;
- virtual laboratories with cyberattack simulations;
- intuitive interfaces for navigating scenarios and applying protocols;
- activity log and evaluation mechanisms.

Virtual labs are connected to containerized infrastructures that replicate real maritime systems and allow for the controlled deployment of cyber challenges. They provide valuable hands-on experience, especially in a context where access to real ships or simulators is often limited.

### *3.5. Validation, testing and improvements*

All project resources – from protocols and scenarios, to the curriculum and digital platform – have undergone rigorous validation processes: focus groups with expert and peer review sessions. The feedback collected has been integrated into the latest revisions, resulting in clearer, more applicable and operationally relevant resources. A pilot testing session with cadets and seafarers is also planned for further validation.

## 4. Discussions and perspectives

The results obtained so far in the CyberSEA project indicate not only the urgent need to improve cybersecurity in the maritime domain, but also the real potential of an integrated approach, combining technical expertise with practical training and human awareness. By integrating vulnerability analysis with cross-sectoral best practices and adapted educational scenarios, the project has demonstrated that a coherent, applicable and scalable framework for maritime cybersecurity training can be created.

One of the important lessons learned from the research activity is that, despite technological advances, the human factor remains a critical point in managing cyber threats (Goh, 2021). Many of the attack vectors included in the developed scenarios are based on human error or lack of vigilance: the use of insecure USB devices, default or shared passwords, lack of recognition of indicators of

compromise. Thus, the training of shipboard personnel must go beyond simple familiarization with technologies and include behavioral and decision-making dimensions, through simulations, red team exercises, drills and reaction tests.

Another essential element is the translation of knowledge into operational practice. The protocols developed in the project can be integrated into the current procedures of shipping companies or into the Safety Management Systems (SMS), but this requires institutional will and managerial support. Moreover, the recommendations formulated within the project can contribute to updating the STCW framework (Convention on Standards of Training, Certification and Service) in order to introduce minimum cyber training requirements.

In terms of educational infrastructure, the development of the CyberSEA Hub marks an important step in democratizing access to practical training, reducing dependence on physical locations and providing a safe environment for testing, controlled failure and active learning. This model can be extended to other related areas – ports, logistics, industrial fishing – or integrated into the national curricula of maritime and military educational institutions.

In the medium and long term, the sustainability of these results depends on:

- official recognition of certifications based on CyberSEA training;
- periodic updating of scenarios and protocols according to emerging threats (e.g. AI-driven malware, Starlink network exploits, etc.);
- strengthening cooperation between education, industry and regulatory authorities.

## 5. Conclusions

The *CyberSEA – Increasing Cyber Security at SEA through digital training* project proposes an innovative and coherent approach to increasing cyber resilience in the maritime domain, responding to a pressing need for training, awareness and intervention in the face of increasingly complex digital risks. Through applied research activities, development of specific protocols and modern educational tools, the project manages to translate abstract security concepts into a practical, useful and adaptable framework for seafarers, instructors and managers in the shipping industry.

The major contributions of the project include:

- a clear mapping of vulnerable maritime systems and the associated risks;
- adaptation of good practices from other industries to the naval specifics;
- development of realistic scenarios and operational cyber protocols;
- development of a curriculum dedicated to the training of shipboard personnel;
- creation of a virtual hub of laboratories for practical distance training.

All these results are based on a rigorous methodology and validated through end-user testing, which gives them a genuine applied value. They can serve as a model for other initiatives in the field of digital cybersecurity training, both in the maritime sector and in related industries.

In a world where the digitalization of maritime transport brings both efficiency and vulnerability, CyberSEA shows that technological progress must be accompanied by a strong security culture. By integrating practical training, clear protocols and international collaboration, the project contributes to building a generation of seafarers prepared not only for the physical sea, but also for the "digital sea" that surrounds their ship.

**Funding:** 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. ANSSI. (2016). Best Practices for Cybersecurity Onboard Ships. https://cyber.gouv.fr
2. IMO. (2021). *MSC.1/Circ.1639 - Guidelines on Cyber Security Onboard Ships*. International Maritime Organization, London.
3. IMO. (2022). MSC-FAL.1/Circ.3/Rev.2 - Guidelines on Maritime Cyber Risk Management. International Maritime Organization, London.
4. Chowdhury, N., Katsikas, S., Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A Delphi method-based study. Computers & Security, 113, 102551. https://doi.org/10.1016/j.cose.2021.102551
5. Oruc, A., Chowdhury, N., Gkioulos, V. (2024). A modular cyber security training programme for the maritime domain. International Journal of Information Security, 23, 1477–1512. https://doi.org/10.1007/s10207-023-00799-4
6. Goh, P. (2021). Humans as the Weakest Link in Maintaining Cybersecurity: Building Cyber Resilience in Humans. In: Introduction to Cyber Forensic Psychology, pp. 287-305. https://doi.org/10.1142/9789811232411_0014