Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume I, 123-129

An Integrated Simulation Model for Maritime Cybersecurity: A Comparative Research Analysis Approach

Ekaterina Dyankova
Department of Information Technologies
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
edyankova@naval-acad.bg

Dilyana Dimitrova
Department of Information Technologies
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
di.dimitrova@naval-acad.bg

***Abstract*—This paper presents the development of an integrated simulation model for maritime cybersecurity training, based on a comparative analysis of existing training platforms. For the purposes of the study, leading international and industrial solutions were evaluated, including Cyber-SHIP Lab, Naval Cyber Range, CDeX Maritime Cybersecurity Scenario, SeaSAFER, K-Sim, and NavSim. Through the applied comparative approach, the advantages and limitations of standalone physical and virtual training environments were identified. Based on these findings, a new, integrated hybrid model was designed that conceptually combines real ship bridge infrastructure with dynamic virtual cyberattack scenarios. It is concluded that the proposed architecture improves trainee preparation by simultaneously developing technical competencies, analytical thinking, and crew coordination in managing cyber incidents at sea.**

Keywords— comparative analysis, hybrid simulators, integrated model, maritime cybersecurity, simulation training.

I. INTRODUCTION

Simulation technologies play a central role in the training of maritime professionals due to the increasing digitization and automation of the maritime industry. They provide a realistic learning environment in which trainees can practice various skills without risk to life and crew. The evolution of these technologies - from classical bridge simulators to modern platforms with augmented reality (Augmented Reality/Virtual Reality) elements - reflects the dynamic changes in maritime education and the need to update teaching approaches.

In recent years, maritime simulations have evolved to include environments focused on cybersecurity. This development is due to the growing reliance of modern ships on interconnected digital systems, including navigation, communication, and control technologies. While these systems improve operational efficiency, they also create vulnerabilities that can be exploited through cyberattacks. As a result, simulation-based training is used increasingly to support the development of competencies related to navigation, engineering, cybersecurity awareness, decision-making, and coordinated response in critical situations.

Simulation-based training is aligned with the principles of experiential learning [1], enabling the acquisition of practical skills through active engagement, analysis of outcomes, and application of knowledge in realistic contexts. Maritime simulators are widely used for developing competencies such as vessel navigation, compliance with international regulations, engine room management, and emergency response [2]. The importance of such training is emphasized by the International Maritime Organization (IMO), which highlights the role of human factors and the need to learn from past incidents in order to improve safety practices.

Traditional full-mission simulators have been established as effective tools for procedural training and standards compliance, particularly within the framework of the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) [3]. At the same time, emerging technologies based on virtual, augmented, and mixed reality are integrated into training environments, offering enhanced realism and user engagement [2]. A master's program in "Simulation Engineering" with a specialization in "Maritime Simulators" has been developed at the Nikola Vaptsarov Naval Academy in Varna, Bulgaria [4], reflecting the growing recognition of the importance of these technologies in the training of maritime specialists. These developments indicate a shift toward more immersive and adaptive maritime training environments.

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol1.114

Maritime cybersecurity has become a critical component of overall maritime safety. Effective training in this domain requires simulation platforms capable of integrating realistic operational conditions with dynamic cyber threat scenarios. Existing research demonstrates a variety of approaches to simulation-based training and system evaluation.

The main aim of the paper is to analyze and evaluate existing maritime simulation platforms from both technological and educational perspectives, and to propose an integrated hybrid model for maritime cybersecurity training.

II. MATERIALS AND METHODS

In order to evaluate current approaches to maritime cybersecurity training, a structured methodological framework is applied. The study is based on a comparative analysis of selected simulation platforms, using defined criteria that address both technological capabilities and educational effectiveness. The findings serve as the basis for the development of an integrated hybrid simulation model.

Comparative analyses have been applied in different maritime contexts. Time-domain simulations have been evaluated against experimental models in studies related to ship stability [5]. In the field of autonomous systems, hardware-in-the-loop simulations have been used to assess detection methods, demonstrating improved performance in integrated sensor approaches [6]. Augmented reality applications have been shown to enhance training effectiveness and user engagement, although limitations remain in representing complex technical interactions [7]. Similarly, virtual and immersive simulation environments contribute to the safe development of practical skills while maintaining a high level of interactivity [8].

Further studies have confirmed the reliability of simulation platforms through comparisons with real-world measurements [9]. In educational settings, the use of advanced simulators has been associated with improved decision-making, faster response times, and enhanced overall performance of trainees [10].

Despite these contributions, limited research has been identified that provides a comprehensive comparative analysis of simulation platforms specifically focused on maritime cybersecurity training. In particular, the integration of physical and virtual simulation environments within a unified training framework remains limited. This gap highlights the need for approaches that combine technological realism with structured pedagogical models for cybersecurity competence development.

A variety of maritime simulation solutions are offered by both industry and academia. Some focus on traditional tasks (navigation, engine room), while others are specifically focused on cybersecurity. In the field of maritime cybersecurity, significant progress has been made in the development of specialized simulators and training platforms. Shipping relies more and more on digitalized systems such as Electronic Chart Display and Information System (ECDIS), AIS/GPS receivers, automated engine rooms, and communication networks. These systems are becoming more connected to the Internet via satellite and 4G/5G networks, making them vulnerable to cyberattacks. Breaches of electronic navigation systems or malware infections can lead to course deviation, loss of connectivity, accidents, and other consequences. To address these issues, a requirement was introduced in 2021 by the International Maritime Organization (IMO) (MSC.428(98)), mandating that cyber risks be included in safety management (ISM Code) [11].

An example of a modern maritime cybersecurity training facility is the Cyber-SHIP Lab at the University of Plymouth, United Kingdom, where the bridge and related ship systems of a modern vessel have been physically replicated. In this controlled laboratory environment, cyber vulnerabilities, exploits, and the operational consequences of attacks are studied by researchers and students [11]. The equipment includes ECDIS, AIS (Automatic Identification System), VDR (Virtual Data Recorder), radars, and communication devices, through which a realistic environment is provided for simulating and analyzing cyberattacks, as well as for developing practical tools and training programs for seafarers [11].

Similarly, a modular cyber range - the Naval Cyber Range - has been developed by the French Naval Academy (École Navale), replicating the IT/OT infrastructure of a medium-sized passenger ship (PLC (Programmable Logic Controller) controllers, AIS, GPS, radar, VDR, etc.) [12]. Training scenarios include phishing and malware attacks, as well as direct manipulation of navigation data. The platform is used as a realistic training tool for both naval personnel training and research [13].

Another such platform is the CDeX Maritime Cybersecurity Scenario, a joint project between CDeX, Shipadvisors, and the Maritime Academy Antwerp [14]. Participants are placed in a simulation of a 150-meter tanker (MV Vigilant Sailor), where leadership roles are assumed and a variety of cyberattacks are encountered, including fake emails, infected updates, and ECDIS sabotage through GPS jamming, AIS spoofing, and data modification (speed, depth, etc.) [15]. Through this type of training, skills for recognizing cyber threats, rapid response, and recovery under realistic conditions are developed.

The K-Sim system is offered by Kongsberg Maritime and includes full-scale bridge, engine, and environmental simulators. These products are used in universities, maritime academies, navies, coast guards, and shipping companies worldwide [16]. Similarly, NavSim products by Wärtsilä are widely used; their navigation simulators support training in both educational environments and VR/AR settings, as well as distributed (online) platforms compliant with international standards [17].

SeaSAFER, developed under the leadership of the Lithuanian Maritime Academy, is an online training platform in which real reports of maritime incidents and accidents are transformed into simulated scenarios. The main advantages of the platform include ease of access, lower costs compared to traditional simulators, and the possibility of certification recognized in partner countries and across Europe [18].

The development of maritime simulation technologies demonstrates a clear trend toward the integration of cybersecurity as an essential element of maritime safety and professional training. With the increasing digitalization of ship systems, the likelihood of cyberattacks is also increasing. A variety of approaches to achieving the common goal of improving awareness and preparedness of maritime personnel for responding to cyber incidents are demonstrated by platforms such as Cyber-SHIP Lab, Naval Cyber Range, and the CDeX Maritime Cybersecurity Scenario, as well as by industrial solutions such as K-Sim, NavSim, and SeaSAFER. Each platform offers a different level of technical complexity and applicability within a training context.

Based on these considerations, a comparative analysis of existing simulation platforms is necessary to assess their technical characteristics and educational value in maritime cybersecurity training. This analysis supports the identification of effective approaches and provides the basis for the proposed integrated hybrid simulation model, which combines physical and virtual environments to enhance training effectiveness.

III. RESULTS AND DISCUSSION

A. *Comparison of maritime cybersecurity training platforms and simulators*

TABLE 1. COMPARATIVE ANALYSIS OF MARITIME CYBERSECURITY TRAINING PLATFORMS AND SIMULATORS

Platform / Criteria	Cyber-SHIP Lab	Naval Cyber Range	CDeX Maritime Cybersecurity Scenario	SeaSAFER	NavSim / K-Sim (industry)
Type	Physical hardware laboratory/navigation simulator “ship bridge”	Modular cyber range	Software service in a cyber range based on scenarios	Online training platform	Commercial simulators (hardware and cloud-based)
Realism of the simulation environment	Physical systems, real devices	Real IT/OT infrastructure, PLC	Realistic scenarios	Cases in a virtual environment	Navigation simulators, “ship bridge” and others, cloud-based options and augmented reality
Types of attacks / scope	GPS/AIS spoofing, ECDIS compromise, malware, PLC tests	Wide range of IT/OT: PLC, networks, navigation	Phishing, infected updates, GPS jamming, AIS spoofing	Case study scenarios based on real incidents	Navigation and operational scenarios; possibilities for integrating cybersecurity-related scenarios
Pedagogical approach	Practical exercises, research in a controlled environment	Practical exercises, research in a controlled environment	Role-playing training, operational team exercises	Case-based learning	Combined learning platforms - courses, practical exercises, access to a cloud environment
Target audience	Researchers, students, maritime specialists	Military and civilian personnel, cyber specialists	Maritime crews, ship operators, researchers	Maritime personnel, trainees	Universities, maritime academies, shipping companies, maritime crews, maritime personnel, researchers
Positive aspects	Realistic simulation of a “ship bridge”, modern equipment	Modular and flexible cyber range suitable for testing multiple attacks	Realistic scenarios with a variety of attacks, suitable for practical training	Low cost, easy access, certification opportunity	Large-scale solutions, global distribution, support for virtual and learning environments

The following criteria are selected for the comparative analysis of the selected platforms:

- Type - allows technology to be classified according to the degree of physical implementation and infrastructure resources, which is important for assessing its applicability in an educational environment.
- Realism of the simulation environment - in cybersecurity training, the realism of the simulation environment helps students acquire skills that are as close as possible to the real working environment.
- Types of attacks/scope - show how up to date the system is, whether it covers current threats, and what competencies it can develop in learners.
- Pedagogical approach - to be applied in educational programs, the system must include specific learning formats (scenarios, role-playing games, practical exercises) that develop both technical skills and place learners in realistic decision-making situations.
- Target audience - determines who the platform is intended for - students, crews, engineers, officers, etc.
- Positive aspects - highlight the main strengths that make a system effective for training.

The selected criteria combine technical, pedagogical, and applied aspects, which allows for an assessment of the role of simulation technologies in maritime cybersecurity training.

Based on the selected criteria, a comparative analysis of the platforms is presented in Table 1. It shows that maritime cybersecurity training is developing in the direction of combining ship bridge simulators with simulated attacks in a virtual environment. Platforms such as Cyber-SHIP Lab and Naval Cyber Range offer a high level of simulation fidelity through real physical or hybrid infrastructure (IT/OT systems, PLC, navigation equipment), making them suitable for training specialists and conducting experimental research. At the same time, CDeX and SeaSAFER demonstrate a flexible pedagogical model focused on scenario- and role-based training, accessible online and with a lower cost for building the infrastructure itself.

Industrial simulators such as K-Sim offer a high degree of realism in the maritime operating environment, combining traditional bridge training with elements of cybersecurity. This makes them a valuable tool for maritime academies and shipping companies seeking compatibility between classic navigation skills and cyber defense on board.

The analysis shows that training effectiveness increases when simulation environments combine a high degree of realism, scenario-based training, and the ability to reflect real incidents. In terms of target groups, the platforms cover a wide spectrum - from cadets and crews to researchers and military specialists - highlighting the versatility and applicability of the simulation approach in maritime cybersecurity. It can be concluded that a combined model integrating physical and virtual simulations would be highly effective for training purposes, as it supports both technical competence and the development of analytical thinking, which are essential for responding to cyber incidents in the maritime industry.

B. Design of an integrated simulator for maritime cybersecurity training

The proposed integrated simulation model (Fig. 1) includes the main components and interrelationships in the maritime cybersecurity training system and enables work in a hybrid environment. It includes physical infrastructure, virtual environment, communication modules and modules for evaluation and feedback. The aim of the diagram is to present the integration of physical and virtual components, to show the flow of information and interactions between the system and trainees, and to demonstrate how simulation develops technical and operational skills for recognizing, responding to, and controlling cyber threats in a safe and controlled environment.

The physical environment contains bridge, engine room, IT/OT systems, navigation and communication systems. Based on this, students can develop competencies in technical skills, critical thinking, physical feedback, and muscle memory. The results of the student’s actions are assessed and analyzed by a module for the assessment and analysis of physical competencies.

The virtual environment contains cyber range, scenarios, simulated attacks, VR/AR. Based on this, students can acquire the skills to detect and analyze threats, classify incidents, and work with cybersecurity software. The results of the students’ actions are assessed and analyzed by a module designed to evaluate and analyze the skills acquired in a virtual environment.

Trainees from different environments can exchange information in a virtual environment. They can compare data from the compromised system with that from the physical system to identify the source of a malfunction on the ship, which may be mechanical or due to external interference.

Cross-validation in physical and virtual learning environments is a process of mutual verification and confirmation of the knowledge and skills gained in both environments. The knowledge gained through virtual simulations is applied and tested in the physical environment, and the results from practical tests are then compared with the virtual models. This two-way

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol1.114

assessment determines how effective the skills are, identifies discrepancies, and allows for adjustments, leading to a more secure, accurate, and lasting retention of knowledge.

The assessment of competencies in a hybrid environment includes team communication between participants, real-time risk assessment, prioritization of crew actions, and working under critical conditions. Competency assessment can be performed automatically or by the instructor. The calculated grade for automated competency assessment includes:

- Trainees response time upon detecting a vulnerability.
- Accuracy of the sequence of actions taken to prevent the incident.
- Condition of the ship's physical parameters during and after the cyberattack.

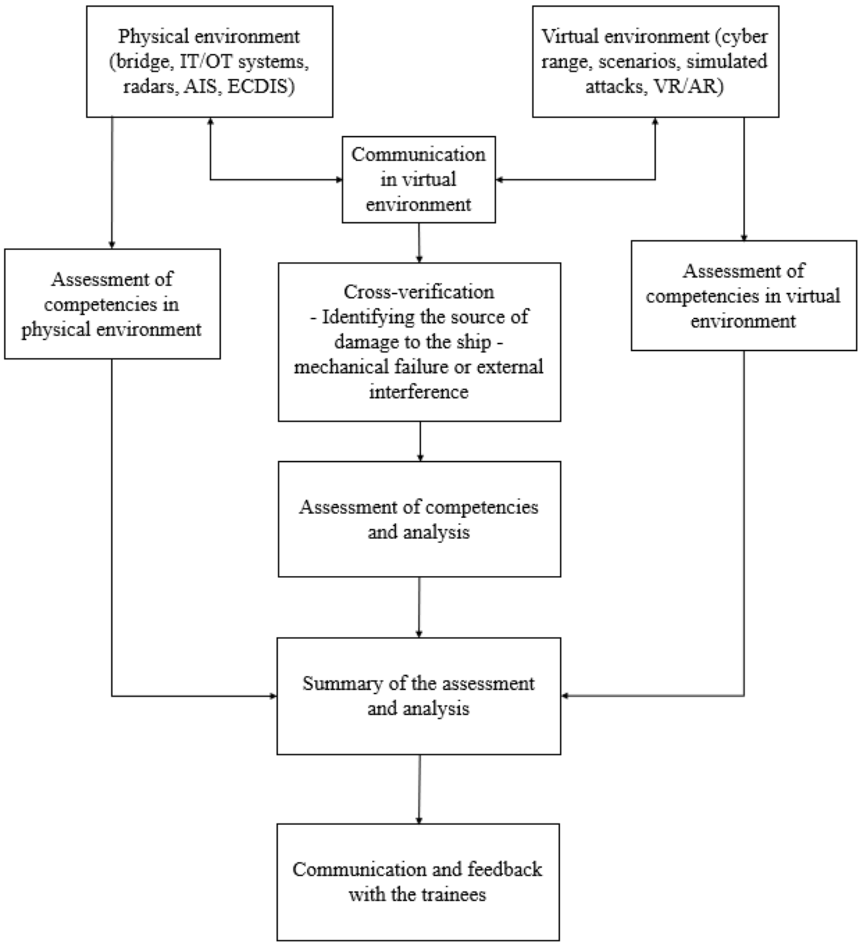

Fig. 1. Integrated model of a simulator for maritime cybersecurity training

The instructor observes the trainee's actions and conducts a post-session review of:

- Communication during the attack.
- The effectiveness of decision-making during the process of preventing the attack.
- Analysis of the mistakes made by the trainees.

The results of the assessment of competencies in the physical environment, the virtual environment, and communication in the virtual environment are summarized and analyzed. This allows for tracking of trainees progress, identification of their strengths and areas for improvement, and the implementation of appropriate measures to enhance the effectiveness of the training process. Timely and constructive feedback is also provided to students, which supports their development and improvement.

The proposed integrated hybrid simulation model provides a comprehensive and effective framework for the development, assessment, and continuous improvement of maritime cybersecurity competencies within a realistic and controlled training environment.

IV. CONCLUSIONS

As part of organizational risk management processes, staff training is essential. The goal is to ensure that all employees acquire the knowledge and skills needed to recognize and manage risks arising from the use of various technologies. Effective training and awareness are key elements in building comprehensive cyber resilience in the maritime industry.

Simulation technologies have become an important tool for maritime cybersecurity training, providing a safe and controlled environment for developing technical skills, analytical thinking, and coordinated responses to cyber incidents. Comparative analysis shows that platforms combining physical ship systems with virtual cyberattack scenarios are highly effective, as they offer both realism and opportunities to practice responses in conditions close to real operations. Platforms such as Cyber-SHIP Lab and Naval Cyber Range demonstrate strong technical reliability and support experimental research, while solutions like CDeX and SeaSAFER offer flexibility, lower cost, and accessibility. Industrial simulators such as K-Sim integrate traditional maritime training with cybersecurity components, enabling large-scale training aligned with international standards. Overall, a hybrid approach that integrates physical and virtual simulation appears to be the most effective for preparing maritime personnel to address modern cyber threats.

The proposed integrated simulation model demonstrates that combining physical ship infrastructure with a virtual cyber environment can significantly enhance training effectiveness. By linking real ship systems with cyber range scenarios, simulated attacks, and VR/AR technologies, the model supports the development of both technical and operational competencies. It facilitates individual skill acquisition, critical thinking, decision-making, and teamwork under realistic conditions. A key contribution of the model is cross-validation between physical and virtual environments, where knowledge gained in one setting is tested and reinforced in the other. This approach improves assessment accuracy, identifies competency gaps, and strengthens long-term knowledge retention. The integrated evaluation framework combines automated performance metrics with instructor-led assessment, ensuring a comprehensive evaluation of trainee performance.

The results of the comparative analysis and the proposed framework confirm that hybrid simulation-based training systems offer high realism, flexibility, and analytical capability. They support effective progress tracking, targeted feedback, and continuous competency development. Therefore, an integrated hybrid simulation approach represents a scalable and resilient solution for preparing maritime personnel to respond effectively to evolving cyber threats in complex operational environments.

ACKNOWLEDGMENTS

This report was financed by the Ministry of Education and Science under the National Science Program "Security and Defense", carried out in implementation of the National Strategy for the Development of Scientific Research 2017-2030 and adopted by Decision of the Council of Ministers No. 731 of October 21, 2021. The material reflects only the author's opinion and the Ministry of Education and Science is not responsible for the content.

REFERENCES

[1] Y. Kong, “The Role of Experiential Learning on Students’ Motivation and Classroom Engagement,” *Front. Psychol.*, vol. 12, p. 771272, Oct. 2021, https://doi.org/10.3389/FPSYG.2021.771272.

[2] M. H. Dewan, R. Godina, M. R. K. Chowdhury, C. W. M. Noor, W. M. N. Wan Nik, and M. Man, “Immersive and Non-Immersive Simulators for the Education and Training in Maritime Domain—A Review,” *Journal of Marine Science and Engineering 2023, Vol. 11, Page 147*, vol. 11, no. 1, p. 147, Jan. 2023, https://doi.org/10.3390/JMSE11010147.

[3] STCW online, “STCW Safety Officer on Board Online Course,” stcw.online. Accessed: Apr. 24, 2026. [Online]. Available: https://stcw.online/course/safety-officer-on-board/?utm_source=google&utm_medium=cpc&utm_campaign=Search_Low_Priority_Courses_High_Conversion&&utm_id=21488347567&utm_term=186364137043_ship%20safety%20training&utm_content=778296802923&gad_source=1&gad_campaignid=21488347567&gbraid=0AAAAADhSnhiAlJoXsQURbFdN8yuud782O&gclid=CjwKCAjwqazPBhALEiwAOuXqdJJKQ6JcPdMVOwHvJ1LFlT_mRKEyXDPlOn_hWPSlIw62B4YQq3_sxxoC10wQAvD_BwE

[4] [Nikola Vaptsarov Naval Academy, “Simulation engineering,” www.naval-acad.bg. Accessed: Apr. 24, 2026. [Online]. Available: https://www.naval-acad.bg/application/majors/master/simulation-engineering

[5] P. Ruponen, E. Altintas, J. Matusiak, and T. Mikkola, “A practical approach for simplified operational guidance to avoid parametric roll resonance,” *Ocean Engineering*, vol. 330, Jun. 2025, https://doi.org/10.1016/j.oceaneng.2025.121215.

[6] [Y. Eustache, C. Seguin, A. Pecout, A. Foucher, J. Laurent, and D. Heller, “Marine Object Detection Using LiDAR on an Unmanned Surface Vehicle,” *IEEE Access*, vol. 13, pp. 121658–121669, 2025, https://doi.org/10.1109/ACCESS.2025.3587315.

[7] A. M. A. Reverón, C. E. M. Luis, and J. M. Gutiérrez, “NavAR, an App for Training in Cartography and Maritime Navigation Through Augmented Reality,” in *Lecture Notes in Mechanical Engineering*, San Cristóbal de La Laguna: Springer Science and Business Media Deutschland GmbH, 2024, pp. 319–329. https://doi.org/10.1007/978-3-031-51623-8_31.

[8] Y. Bohdan, I. Bohomolova, A. Satulov, S. Voloshynov, and V. Savchuk, “COMPARATIVE ANALYSIS FOR STATE-OF-THE-ART SIMULATION TRAINING SYSTEMS THOSE INFLUENCE ONTO THE FUTURE ENGINEERS’ KNOWLEDGE AND SKILLS,” in *21st Annual General Assembly, IAMU AGA 2021 - Proceedings of the International Association of Maritime Universities ,IAMU Conference*, Kherson, 2021. Accessed: Nov. 11, 2025. [Online]. Available: https://www.scopus.com/pages/publications/85124620290?origin=resultslist

[9] J. Orović, M. Valčić, V. Knežević, and Z. Pavin, “Comparison of the on Board Measured and Simulated Exhaust Gas Emissions on the Ro-Pax Vessels,” *Atmosphere (Basel).*, vol. 13, no. 5, May 2022, https://doi.org/10.3390/atmos13050794.

[10] M. Nikolova, E. Andreev, and Y. Kolarov, “Creation of Scenarios with VSTEP Simulator and Evaluation of Simulators Use in Maritime Education and Training,” *Scientific Bulletin of Naval Academy*, vol. XXVI, pp. 64–72, 2023, https://doi.org/10.21279/1454-864X-23-I2-007.

[11] University of Plymouth, “Maritime cyber threat mitigation training - University of Plymouth,” Maritime cyber threat

mitigation training. Accessed: Oct. 03, 2025. [Online]. Available: https://web.archive.org/web/20250615142908/https://www.plymouth.ac.uk/research/cyber-ship-lab/maritime-cyber-threat-mitigation-training

[12] Naval Systems Cyber Defense Chair, "Cyberrange | Chaire de Cyberdéfense des Systèmes Navals," cyberrange. Accessed: Oct. 03, 2025. [Online]. Available: https://web.archive.org/web/20250719120754/https://chaire-cyber-navale.fr/en/cyberrange/

[13] Naval Systems Cyber Defense Chair, "Advanced simulation platform for cyber security of maritime systems." Accessed: Nov. 07, 2025. [Online]. Available: https://web.archive.org/web/20251107135426/https://chaire-cyber-navale.fr/en/cyberrange/

[14] CDEX, "Defending the Seas — CDeX's Maritime Cybersecurity Scenario," Defending the Seas — CDeX's Maritime Cybersecurity Scenario. Accessed: Oct. 03, 2025. [Online]. Available: https://cdex.cloud/blog/technology-updates/defending-the-seas-cdexs-maritime-cybersecurity-scenario/

[15] CDEX, "Discover the Power of CDeX Training Catalogue." Accessed: Nov. 07, 2025. [Online]. Available: https://cdex.cloud/blog/technology-updates/discover-the-power-of-cdex-training-catalogue/

[16] Kongsberg Maritime, "Simulation - Kongsberg Maritime," Simulation. Accessed: Oct. 06, 2025. [Online]. Available: https://web.archive.org/web/20250518200707/; https://www.kongsberg.com/maritime/products/simulation/

[17] Wärtsilä, "Wärtsilä Navigational simulators," www.wartsila.com. Accessed: Oct. 03, 2025. [Online]. Available: https://web.archive.org/web/20250905015437/https://www.wartsila.com/marine/products/simulation-and-training/navigational-simulators

[18] SeaSAFER, "SeaSAFER Background," SeaSAFER.com. Accessed: Oct. 03, 2025. [Online]. Available: https://web.archive.org/web/20251003123235/https://seasafer.com/bg/