Maritime Cybersecurity: The Human Factor as a Key Element in Defense Against Cyberattacks

DOI: 10.25043/19098642.294

Ferney Martínez Ossa [1]
Yury Natalia Rojas Lara [2]
Luis Enrique Sánchez Crespo [3]
Antonio Santos-Olmo [4]

Abstract

The increasing integration of advanced technological solutions within maritime environments, such as ships and ports, combined with the adoption of emerging technologies and the establishment of new standards and guidelines, has elevated cybersecurity to a critical concern. This study focuses on the development of specific strategies and technical measures to strengthen cybersecurity in these environments, emphasizing key challenges such as the human factor, identified as the weakest link in the defense chain. This research explores how attentional biases influence individuals' responses to cyber threats. Using a technological tool with integrated biofeedback, a training program was developed to improve cybersecurity awareness. The findings revealed that fostering a cybersecurity culture had a more significant impact than prior knowledge on the subject, as it facilitated the identification of errors during tasks. Moreover, repeated use of the tool led to a reduction in errors, which correlated with increased awareness and emotional self-regulation. This pioneering study in the field of cybersecurity underscores the importance of interdisciplinary approaches that integrate engineering, psychology, and cybersecurity training to mitigate human vulnerabilities and enhance the resilience of maritime systems.

Key words: Culture of Cybersecurity, Human factor, Security psychology, defense, cyberattacks.

How to cite this article
To cite this article, use the following format:

IEEE Format
[1] F. Martínez Ossa, Y. N. Rojas Lara, L. E. Sánchez Crespo and A. Santos-Olmo "Maritime Cybersecurity: The Human Factor as a Key Element in Defense Against Cyberattacks" Ship Science and Technology (Cartagena), vol. 19, no. 38, pp. 73-85, 2026. DOI: 10.25043/19098642.294

Date Received: October 23rd, 2024
Date Accepted: November 15th, 2024
Publication Date: March 5th, 2026

University of Castilla-La Mancha, GSyA Security and Audit Group, Ciudad Real, España. ROR: https://ror.org/05r78ng12
[1] Email: fmartinez@cotecmar.com ORCID: https://orcid.org/0000-0002-6622-4387
[3] Email: luise.Sanchez@uclm.es ORCID: https://orcid.org/0000-0003-0086-1065
[4] Email: antonio.santosolmo@uclm.es ORCID: https://orcid.org/0000-0002-2349-3894

Armada de colombia, Ministerio de defensa Nacional. Bogotá, Colombia. ROR: https://ror.org/01xjag017
[2] Email: yury.rojas@armada.mil.co ORCID: https://orcid.org/0009-0005-3023-5585

DOI: 10.25043/19098642.294

Introduction

The evolution of technology across various fields, particularly in the maritime sector, has increased exposure to cyber threats. Therefore, implementing technological solutions alone is not sufficient. It is essential to develop an organizational culture of cybersecurity to minimize risks. This article analyzes two fundamental perspectives that contribute to this objective: on the one hand, the sociocultural aspect, focused on psychological and organizational factors; and, on the other hand, the technical aspect, oriented toward the implementation of robust technological measures from a high-level perspective. The expansion of cyberspace offers remarkable solutions to many human needs; however, it also increases vulnerabilities, creating a high-risk environment. Society will need to confront this challenge to build the trust required to ensure security and freedom within this environment [1].

In the maritime domain, cybersecurity has become a critical factor due to the exponential use of technological resources such as connectivity and the digitalization of systems within the naval industry. Modern vessels and port infrastructures conduct their operations using increasingly sophisticated systems, which open opportunities for cyberattacks by exploiting vulnerabilities that arise from the pursuit of efficiency and productivity in operational processes [2]. Many of these vulnerabilities highlight the central role of the human component, which, as in any technology, without aware and properly trained personnel, can become the weakness that prevents the establishment of a robust defense against cyber threats.

Therefore, the psychological and sociocultural aspects of cybersecurity are essential to ensure effective detection of and response to cyberattacks. Establishing mechanisms that promote awareness, improve personnel skills, and foster commitment to shared responsibility are key factors for anticipating and reducing the impact of attacks, as well as strengthening system resilience. This study aims to evaluate the impact of cybersecurity training in the maritime sector, with a focus on improving awareness and response capabilities to cyber threats. The role of the human factor will be analyzed through training in simulated environments and psychological assessments.

From a technical perspective, various strategies have been developed to protect critical maritime infrastructures. These include the implementation of threat detection systems based on artificial intelligence (AI), which enable the identification of anomalous behaviors in real time, as well as the integration of the Automatic Identification System (AIS) and the Electronic Chart Display and Information System (ECDIS) with advanced security technologies. In addition, encryption measures and robust protocols are employed to secure communications and operations of vessels and ports. Each of these technologies not only enhances resilience against cyberattacks but also complements the human component by reducing vulnerabilities associated with operational failures.

This article is structured as follows: Section 2 presents the problem statement and justification, highlighting the need to foster a cybersecurity culture. Section 3 addresses strategies for building an organizational security culture, emphasizing the human factor and emerging technologies. Section 4 details the proposed methodology for implementing these strategies, while Section 5 analyzes the expected results and the practical implications of the study. Finally, Section 6 lays out conclusions and recommendations for future research and applications in the maritime domain.

Problem Statement and Justification

Currently, organizations either operate within or are in the process of adopting environments

based on the use of technologies, where cyber threats are continuously evolving. A study by Cybersecurity Ventures [3] indicates that by 2025, the global cost of cybercrime is expected to reach USD 10.5 trillion annually, underscoring the urgency of implementing strategies and controls to protect digital assets. However, although technology is advancing at an increasingly rapid pace, a large proportion of cyber incidents result from human error or a lack of knowledge regarding cybersecurity best practices. This raises the following question: how can organizations foster a cybersecurity culture that accounts for both individuals' limited capabilities and the need for technological solutions?

In this context, identifying and establishing processes that promote the adoption of a cybersecurity mindset not only addresses the challenges associated with cyber threats and the efforts made by companies in technology and process development, but also provides a foundation for organizational resilience that supports a stable and progressive process over time [4].

According to recent studies by IBM [5], 95% of security breaches are related to the human factor, further reinforcing the proposal of human-centered strategies. These initiatives suggest a combination of educational, technological, and organizational strategies that address all dimensions of the cybersecurity framework under implementation.

In another study conducted by the Ponemon Institute [6], it was demonstrated that when organizations implement cybersecurity training and awareness strategies, the costs associated with security incidents can be reduced by up to 40%. This economic impact stresses not only the importance of training personnel but also the need to establish cybersecurity as a fundamental pillar of organizational culture.

From a technical perspective, the use of emerging technologies such as artificial intelligence (AI) and machine learning provides new opportunities to strengthen cybersecurity. The implementation of AI in threat identification has decreased response times, enabling more efficient incident management. These technologies not only enhance human efforts but also increase operational capabilities in critical situations [7].

Finally, the use of digital systems within global interconnectivity and critical environments such as the naval domain highlights the need for interdisciplinary approaches. Cybersecurity in these contexts is not only a technical issue but also a strategic one, as incidents may have economic and national security implications. In this context, strengthening Organizational Cybersecurity Awareness through the integration of engineering, psychology, and other disciplines that contribute to continuous training becomes an essential priority.

Sociocultural Aspect: Psychological Dimension

Human factors constitute one of the primary causes of cybersecurity incidents; therefore, addressing the psychological dimension is essential for mitigating risks. Emotional responses influence both the recognition of alerts and vulnerability to cyberattacks, which are aspects determined by the level of knowledge in information security, trust in technology, and the perceived severity of attacks. Understanding the interactions among emotional, cognitive, and behavioral variables is fundamental for improving the capacity to respond effectively to cyber threats.

Awareness and Continuous Training

Cybersecurity awareness requires more than occasional training sessions; it demands a continuous and dynamic approach. Regular training programs that educate employees about cyber threats and secure practices have proven to be effective. A study published in Cyberpsychology, Behavior, and Social

Networking concluded that recurrent training significantly improves awareness of digital risks and reduces unsafe behaviors [8]. These programs should include updated content based on the latest threat-related trends, such as advanced phishing, ransomware, and social engineering techniques.

Additionally, incorporating simulations of real-world attacks is recommended to enhance the understanding of risks and prepare personnel to respond appropriately to real incidents. Practical simulations not only reinforce skills but also contribute to the identification of malicious behavior patterns, a critical aspect for early cyberattack detection. Individual responsibility is fostered more effectively when supported by cybersecurity training that strengthens employees' awareness and skills, ensuring that they remain prepared to address emerging threats.

Promoting Individual Responsibility

Compliance with security policies largely depends on the responsibility assumed by each individual. Recent studies published in the Journal of Cybersecurity have identified the fact that employees with a strong sense of personal responsibility are more likely to adopt proactive cybersecurity measures [9]. To foster this perception, organizations should implement feedback systems that link individual behavior to overall security outcomes. Additionally, it is important that tangible incentives and public recognition be provided for adherence to best practices.

Clear communication of expectations and responsibilities is essential for fostering a sense of ownership in terms of organizational security. Clearly defining what is expected from each employee regarding cybersecurity guarantees that all personnel remain aligned with the organization's objectives. This includes explaining security policies in a comprehensible manner and emphasizing how individual actions impact overall security. Moreover, accountability programs may include analyses of previous incidents within the organization, highlighting how specific actions contributed either to preventing or exacerbating the consequences of an attack. This practice creates valuable organizational learning that reinforces the connection between individual actions and their impact on collective security.

Organizational Security Culture

Security culture should not only be a mandate but also a shared value that permeates all levels of the organization. According to Information Security Journal: A Global Perspective, organizations with a well-established cybersecurity environment demonstrate a significantly greater capacity to recover from incidents [10]. Achieving this requires:

- Clear and transparent policies: Policies must be accessible to all employees, understandable, and applicable in everyday contexts.
- Continuous communication: Regular meetings, cybersecurity newsletters, and updates on emerging risks reinforce the importance of security.
- Leadership involvement: Security must be a visible priority supported by senior leaders, who act as role models in complying with security policies. In addition, the establishment of interdepartmental cybersecurity committees can facilitate knowledge exchange and promote a shared vision regarding security objectives.

In this context, psychological aspects such as awareness, individual responsibility, and an organizational security culture play a fundamental role in preventing cyberattacks. The effectiveness of crew members in detecting and responding to threats depends not only on their training but also on their attitude toward security. Without a strong security culture, even the most advanced technological solutions become vulnerable to human error.

Continuous training and collective commitment are essential to reducing the likelihood of incidents, particularly in the maritime sector, where critical infrastructure depends both on technology and the human factor. The following section will analyze the main cyberattacks launched in the maritime domain, highlighting how human and technical vulnerabilities have been exploited to compromise security.

Major Cyberattacks in the Maritime Domain

Cyber threats are present across all industrial sectors, and the maritime domain is no exception to this issue. The main types of attacks occurring in this sector are outlined below:

- GPS Spoofing / GNSS Jamming: Navigation systems rely heavily on GPS- based technologies. Attacks such as spoofing and jamming can compromise critical systems that support the precise navigation of vessels, causing data confusion and route alterations.
- Ransomware: This has been one of the most notable threats, affecting both port facilities and onboard vessel systems by blocking operations and demanding ransom payments in exchange for restoring access to data.
- Phishing and Social Engineering Attacks: Phishing attempts and other forms of psychological manipulation remain persistent threats. These attacks exploit human vulnerabilities to gain unauthorized access to critical systems.
- Attacks on AIS Systems: The Automatic Identification System (AIS) is susceptible to manipulation that can alter information regarding vessel location and identification, thereby affecting navigational safety.

Table 1 summarizes several significant cyberattacks unleashed on the maritime domain over the past seven years, highlighting the critical role of the human factor in these incidents. The lack of strong cybersecurity awareness appears as a common denominator, underscoring the importance of implementing effective preventive measures, ongoing training programs, and the active promotion of organizational best practices. These elements are essential for mitigating cyber risks and strengthening resilience within the maritime environment.

Current Status and Defense Strategies

The previously identified issues, such as lack of awareness and low perception of risks in the maritime sector, establish the foundation upon which current defense strategies are developed. These strategies aim not only to address technical vulnerabilities but also to strengthen the mindset of digital protection and the human capacity to respond to attacks. Currently, and as part of innovation strategies, the maritime industry is evolving toward greater cybersecurity awareness, not only through training processes but also by incorporating awareness initiatives that evaluate human behavior and adaptability to new processes by turning individuals into active participants both in the problem and the solution.

Current strategies seek to tackle these challenges through a comprehensive approach that combines advanced technical measures with the reinforcement of an organizational security culture. Although significant challenges remain, the strategies being proposed rely on advanced systems and threat detection technologies that are insufficient if they are not supported by adequate preparation of the human component. The main methods, standards, and frameworks used to promote a cybersecurity culture and strengthen the human factor are listed below:

- International Standards: Regulations such

Table 1. Major Cyberattacks on the Maritime Domain and the Influence of the Human Factor.

Date and Location of the Attack	Type of Attack and Impact	Duration and Reported Damage	Cybersecurity Culture Issues Attributed to the Attack
June 2017 - Maersk (Global)	Ransomware (NotPetya) – Disruption of global operations	10 days – Estimated losses of USD 300 million	Lack of awareness regarding system updates and security patching, which allowed for the ransomware to spread.
July 2018 - Cosco (USA)	Ransomware – Disruption of communications in the U.S.	5 days – Impact on regional operations	Lack of adequate training to prevent ransomware attacks and absence of a proactive cybersecurity strategy.
September 2018 - Port of San Diego, United States	Ransomware – Disruption of administrative services	8 days – Financial losses not disclosed	Lack of training in ransomware prevention and incident response practices.
September 2020 - CMA CGM (Global)	Ransomware – Unauthorized access to internal systems	2 weeks – Financial losses not disclosed	Possible lack of staff awareness regarding basic security measures and inadequate system updates.
October 2021 – Port of Houston, United States.	Brute-force attack – Unauthorized access to port systems	1 day – No significant damage reported	Use of weak passwords indicated a lack of awareness regarding the importance of strong password practices.
February 2022 – Port of Lisbon, Portugal	Ransomware – Disruption of digital services	1 week – Financial losses not disclosed	Lack of a cybersecurity culture to prevent attacks through staff training and proactive measures.
June 2023 – Port of Nagoya, Japan	Ransomware – Disruption of port operations	2 days – Delays in logistics and operations	Lack of preventive training for personnel regarding the identification of suspicious emails or links.
October 2024 – Port systems and public administrations, Belgium	Denial-of-Service attack – Server overload and operational disruption	8 days – Supply chain delays and loss of access to critical services	Lack of preparedness for DDoS attacks, insufficient staff awareness, and absence of interinstitutional cooperation.

as the International Maritime Organization guideline MSC-FAL.1/Circ. 3 and ISO/IEC 27001 provide specific guidance for maritime cybersecurity, including components related to personnel training and the management of human-related risks.

- Frameworks Incorporating Psychological and Sociocultural Contributions: Frameworks such as the NIST Cybersecurity Framework [11], the SANS Institute Security Awareness model, and the ISO 27000 family [12] emphasize the importance of incorporating awareness and training programs within cybersecurity strategies, as well as frameworks that address the psychological and behavioral aspects of personnel.
- Periodic Training and Simulations: Regular training, awareness campaigns, and cyberattack simulation activities enable personnel to recognize threats more effectively and respond appropriately, thus reducing vulnerability to attacks, particularly those based on social engineering.
- Sociocultural Risk Assessment: It is essential to understand that cultural and social factors influence the adoption of cybersecurity practices. Creating an environment in which cybersecurity is valued as a collective responsibility is fundamental for establishing a culture of protection.
- Anomalous Behavior Detection Technologies: The use of AI-based anomaly detection systems makes it possible to identify unusual behavior among personnel, which can help prevent security incidents caused by human error or manipulation.

The development of a strong organizational cybersecurity culture depends on structured training programs that strengthen individuals' capacity to identify, recognize, and respond to attacks, thereby fostering changes in risk perception and promoting the adoption of secure practices.

Proposed Methodology for a Comprehensive Cybersecurity Strategy

To develop a comprehensive cybersecurity strategy in the maritime domain that considers both technical and psychological aspects, the methodology presented in Fig. 1 is proposed. This figure provides a detailed scheme of the implementation phases of the intended methodological approach. Each phase focuses on strengthening digital security through initial risk assessment, constant personnel training, and the application of improvement strategies based on data analysis.

Table 2 details each of the five phases of the proposed methodological structure for managing cybersecurity culture in the maritime environment. These phases range from the initial assessment to continuous improvement. In each phase, the objective is to carry out a risk analysis in a comprehensive manner by combining human and technical aspects, which, when integrated, strengthen processes aimed at minimizing cybersecurity vulnerabilities originating from the human factor.

The foundations of a comprehensive cybersecurity strategy are based on four key pillars designed to provide coordinated and holistic protection against cyber threats while promoting the development of a cybersecurity culture within the maritime environment. The proposed approach includes these four pillars, as illustrated in Fig. 1.

First, the Threat and Control Taxonomy categorizes and prioritizes cyber threats,

Fig. 1. Methodological proposal for promoting a cybersecurity culture.

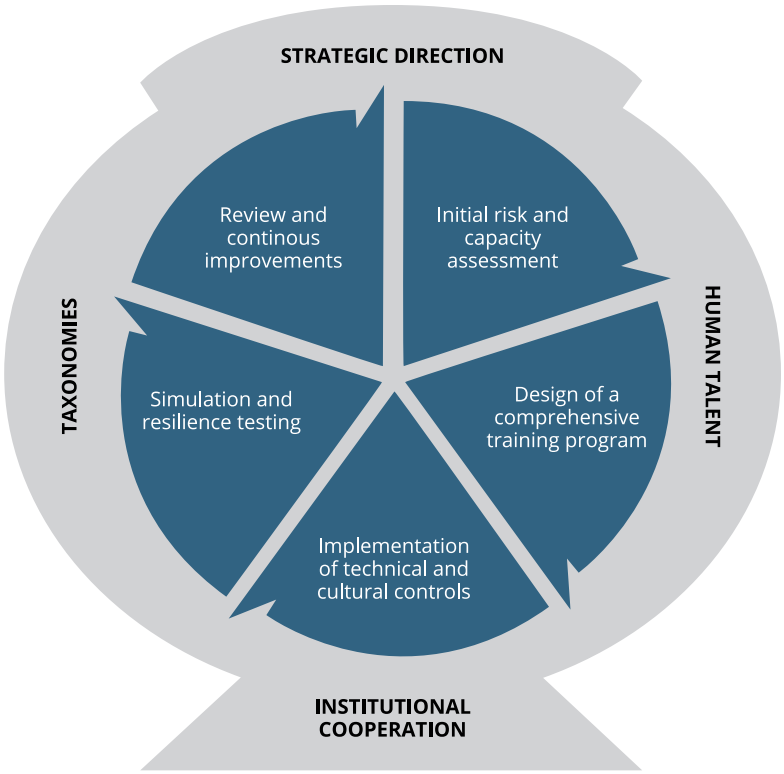


Table 2. Methodological Phases for Comprehensive Cybersecurity Management in Maritime Environments.

Phase	Description	Activities
Initial Risk and Capability Assessment	Identification of critical systems and technical vulnerabilities, and evaluation of risk perception.	Technical Analysis: Security audits, evaluation of technological infrastructure, vulnerability analysis using scanning tools.
		Psychological and Sociocultural Assessment: Identification of risk profiles using risk perception questionnaires, group interviews, and participatory workshops.
Design of a Comprehensive Training Program	Cybersecurity training for personnel addressing both technical and psychological dimensions.	Technical Training: Online learning modules, in-person workshops with cybersecurity experts, and attack scenario simulations.
		Psychological Training: Phishing attack simulations, training in emotional response techniques, and training in executive cognitive functions through role-based dynamics to strengthen critical thinking.
Implementation of Technical and Cultural Controls	Implementation of technical protection measures and promotion of a security culture.	Technical Controls: Installation and configuration of security systems (firewalls, multi-factor authentication), periodic penetration testing, and patch management and software updates.
		Promotion of a Security Culture: Internal communication campaigns and recognition programs highlighting employees who adhere to best practices, as well as monthly meetings to discuss incidents and lessons learned.
Simulations and Resilience Testing	Evaluation of the effectiveness of protocols and team response through simulations.	Cyberattack Simulations: Red-teaming exercises including both technical attacks and human manipulation.
		Regular Behavioral Assessments: Implementation of behavior monitoring tools, analysis of anomalous usage patterns, and generation of automated alerts to review suspicious activities.
Review and Continuous Improvement	Post-incident analysis and continuous feedback collection.	Post-Incident Analysis: Meetings to document the stages of the attack and development of corrective action plans.
		Continuous Feedback: Satisfaction surveys regarding cybersecurity policies, suggestion boxes, and quarterly feedback sessions.

facilitating the identification of specific risks and the design of strategies for effective mitigation. Second, the Human Talent and Organizational Culture represent the foundation of robust cybersecurity; continuous training and personnel awareness are essential for recognizing and responding appropriately to threats. Additionally, the Alignment with Strategic Objectives ensures that cybersecurity policies are integrated into the organization's mission, promoting asset protection and business continuity. Finally, Collaboration and Cooperation among different organizations, whether within the same sector or across sectors, enable the effective exchange of information and resources, thereby bolstering the collective security posture through joint efforts among maritime organizations, government agencies, and other key stakeholders in the operational environment.

These pillars create a comprehensive foundation that integrates both technical and human aspects, aiming to strengthen resilience against cyberattacks in the maritime sector, particularly considering the central role of the human factor.

Proposed Application and Participants

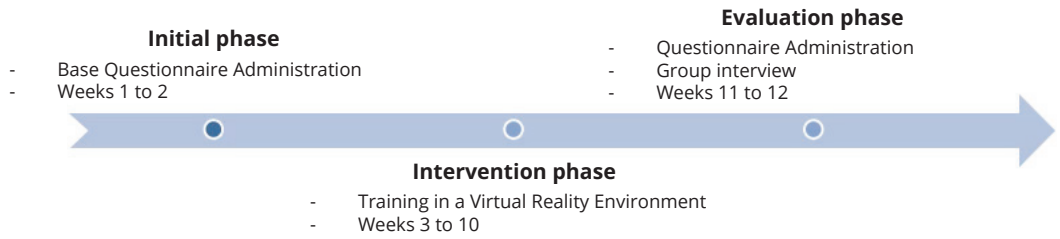
The proposed study will be conducted in three phases and will include a sample of 64 participants. To estimate the mean sample size, the standard deviation of the total score on the CIDI-SC scale from the study reported in [13] will be used, with a confidence level of 95%. This calculation will be performed using the Epidat 3.1 program. The sample will consist of men and/or women between 20 and 45 years of age who are employed in activities related to the maritime sector, such as port operators, vessel crew members, and administrative personnel. This study aims to evaluate the impact of cybersecurity training in the maritime sector, with a focus on improving awareness and response capacity to cyber threats. The role of the human factor will be analyzed through training in simulated environments and psychological assessments, which will be framed according to the considerations detailed in Table 3.

The intended approach aims to provide a comprehensive framework for identifying and increasing the level of awareness of cyber risks among individuals involved in the various processes of the maritime supply chain. This will be achieved through a combination of information-gathering activities, the use of interactive tools, and biofeedback techniques. To this end, an initial sample of participants is proposed within a three-phase research design. The objective is not only to identify initial gaps in knowledge and attitudes toward cybersecurity but also to strengthen the capacity to respond to complex situations. The hypothesis suggests the use of simulation-based interventions, as they contribute both to improving participants' awareness of cyber

Table 3. Summary of the Proposed Framework.

Description	Activities
Inclusion criteria:	Participants must have received prior basic cybersecurity training and have regular access to computer systems connected to networks.
Exclusion criteria:	Individuals presenting psychological conditions that may affect their performance, including diagnosed mood or personality disorders, will be excluded.
Initial Phase:	Administration of surveys to measure baseline cybersecurity knowledge. Identification of risk profiles by assessing attitudes and risk awareness using the Risk Perception Questionnaire (PRQ) [14]. Evaluation of cognitive biases and attention using the Barratt Impulsiveness Scale (BIS-11) [15] to assess impulsivity and selective attention. Assessment of coping strategies and stress using the Connor–Davidson Resilience Scale (CD-RISC) [16] and the State–Trait Anxiety Inventory (STAI) [17].
Intervention Phase:	Training in a virtual reality environment that simulates critical cybersecurity situations in maritime contexts. Simulations will include attacks targeting the Automatic Identification System (AIS) and the Electronic Chart Display and Information System (ECDIS). Biofeedback technologies will be used to analyze participants' emotional responses to stressful situations.
Evaluation Phase:	Technical Controls: Installation and configuration of security systems (firewalls, multi-factor authentication), periodic penetration testing, and patch management and software updates.
Evaluation Phase:	Application of the instruments used in the initial phase to measure changes in knowledge and response capabilities, followed by a group interview. Comparative analysis of pre- and post-intervention data.
Hypotheses and Expected Results:	Hypothesis 1: Participants are expected to show a low initial level of attention to cyber risks in maritime environments.
	Hypothesis 2: The intervention based on simulations and biofeedback will significantly increase awareness and capacity to respond.
	Hypothesis 3: Emotional self-regulation will improve with repeated exposure to critical scenarios, reducing operational errors.
	Expected Results: The findings are expected to provide a foundation for designing more effective training programs tailored to the maritime sector's specific needs.

Fig. 2. Proposed Timeline for the Development of Major Activities



risks and to enhancing their emotional self-regulation to provide adaptive responses.

Furthermore, the importance of designing a proposal tailored to the specific needs of the maritime environment is emphasized. The expected results will be essential for the development of more specific and effective training protocols in the future, thereby providing additional tools that may serve as references for the prevention and mitigation of cyber risks in the maritime domain.

Fig. 2 illustrates the timeline for key activities within the cybersecurity training and improvement project. Each activity is designed to be evaluated and implemented in a phased manner, from the initial assessment stage to the final implementation and review phase. This approach enables structured and progressive training, ensuring the continuous adaptation and improvement of personnel as critical skills for resilience against cyberattacks are developed.

Conclusions

This research highlights the need for interdisciplinary maritime cybersecurity that integrates emerging technologies, continuous training, and a comprehensive approach to the human factor to ensure resilience against cyberattacks in an increasingly digitalized environment. The interaction between technical and psychological aspects is emphasized, proposing awareness programs that incorporate practical simulations and technologies such as biofeedback, which enable the development of critical skills within operational teams. In addition, the findings underline the importance of adopting international standards such as ISO/IEC 27001 and frameworks such as the NIST Cybersecurity Framework, which provide structured guidance for implementing technical, cultural, and organizational measures.

The comprehensive cybersecurity strategy presented is organized around four fundamental pillars. The first one, Threat and Control Taxonomy, prioritizes threats to design effective mitigation strategies. The second one, Human Talent and Organizational Culture, reinforces continuous training and personnel awareness as the foundation for addressing risks. Thirdly, Alignment with Strategic Objectives ensures that cybersecurity policies are integrated into the organizational mission, thus protecting assets and ensuring operational continuity. Finally, Interinstitutional Collaboration and Cooperation promote the exchange of information and resources among maritime organizations, government agencies, and key stakeholders to strengthen the collective security posture.

In conclusion, this proposal underscores the fact that cybersecurity is a collective responsibility that combines technological innovation with human dynamics, highlighting the human factor as a central element in addressing the sector's challenges. Empirical validation of these strategies and integration of emerging technologies with interdisciplinary approaches will be essential to protect strategic

assets and ensure sustainable operations in an increasingly complex global environment.

Looking ahead, three key lines of work are identified that have the potential to transform cybersecurity in the maritime sector. First, the empirical validation of the proposed methodology in real operational environments is essential to evaluate its effectiveness in addressing specific incidents, enabling the adjustment and optimization of the proposed tools for practical implementation. Second, the integration of emerging technologies such as artificial intelligence and machine learning represents a crucial opportunity to personalize interventions, detect anomalous behavioral patterns, and strengthen real-time threat response capabilities. Finally, the longitudinal evaluation of the impact of cybersecurity training programs will help to understand how initial interventions influence organizational resilience over time, identifying areas for improvement and securing the sustainability of cybersecurity efforts. Altogether, these lines of work establish a robust framework for strengthening cyber defense in a strategic sector that is highly dependent on technological connectivity.

Acknowledgments

This work has been funded by the Di4SPDS projects (CHIST-ERA grant - PCI2023145980-2) funded by MCIN/AEI and co-funded by the European Union; AETHER-UCLM (PID2020-112540RB-C42) funded by MCIN/AEI; ALBA-UCLM (TED2021-130355B-C31) funded by MICIU/AEI/10.13039/501100011033 and the European Union NextGener-ationEU/PRTR; and MESIAS (2022-GRIN-34202) funded by FEDER. We also acknowledge the support from the Science and Technology Corporation for the Development of Naval, Maritime and River Industry, COTECMAR, as well as the personnel of the National Navy of Colombia for their participation, willingness, and commitment in this work.

Contributions

- Ferney Martínez Ossa: Author (Research, analysis, design, methodology, writing)
- Yury Natalia Rojas: Co-author (Research, analysis, design, methodology, writing)
- Luis Enrique Sánchez Crespo: Review
- Antonio Santos-Olmo: Review.

Funding source

This work has been funded by the Di4SPDS projects (CHIST-ERA grant - PCI2023145980-2) funded by MCIN/AEI and co-funded by the European Union; AETHER-UCLM (PID2020-112540RB-C42) funded by MCIN/AEI; ALBA-UCLM (TED2021-130355B-C31) funded by MICIU/AEI/10.13039/501100011033 and the European Union NextGener-ationEU/PRTR; and MESIAS (2022-GRIN-34202) funded by FEDER. We also acknowledge the support from the Science and Technology Corporation for the Development of Naval, Maritime and River Industry, COTECMAR, as well as the personnel of the National Navy of Colombia for their participation, willingness, and commitment in this work.

References

[1] F. SÁNCHEZ VERA, J. E. MARTÍNEZ GUIRAO, and A. TÉLLEZ INFANTES, “La seguridad en el ciberespacio desde una perspectiva sociocultural,” methaodos revista de ciencias sociales, vol. 10, no. 2, pp. 243–258, Oct. 2022, doi: 10.17502/MRCS.V10I2.577.

[2] ... A. P.-R. general and undefined 2022, “La gestión de los riesgos cibernéticos en los sistemas de seguridad en buques y empresas navieras,” armada.defensa.gob.es, Accessed: May. 23, 2024. [Online]. Available: https://armada.defensa.gob.es/archivo/rgm/2022/03/rgmmar2022cap03.pdf

[3] STEVE MORGAN, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025," Special Report: Cyberwarfare In The C-Suite. Accessed: Nov. 20, 2024. [Online]. Available: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

[4] E. ABAD-SEGURA, M. D. GONZÁLEZ-ZAMAR, J. C. INFANTE-MORO, and G. R. GARCÍA, "Sustainable management of digital transformation in higher education: Global research trends," Sustainability (Switzerland), vol. 12, no. 5, Mar. 2020, doi: 10.3390/SU12052107.

[5] IBM Security, "Cost of a data breach 2024 | IBM." Accessed: Nov. 9, 2024. [Online]. Available: https://www.ibm.com/reports/data-breach

[6] Ponemon Institute, "The economics of cybersecurity training programs." Accessed: Nov. 10, 2024. [Online]. Available: https://www.ponemon.org/

[7] G. RUBIO, "The use of AI for cybersecurity," Revista da UI_IPSantarém, vol. 9, no. 4, pp. 91–97, Dec. 2021, doi: 10.25746/RUIIPS.V9.I4.26214.

[8] H. ALDAWOOD and G. SKINNER, "Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues," Future Internet 2019, Vol. 11, Page 73, vol. 11, no. 3, p. 73, Mar. 2019, doi: 10.3390/FI11030073.

[9] R. MONTAÑEZ, E. GOLOB, and S. XU, "Human Cognition Through the Lens of Social Engineering Cyberattacks," Front Psychol, vol. 11, p. 528099, Sep. 2020, doi: 10.3389/FPSYG.2020.01755/BIBTEX.

[10] M. ALSHAIKH, "Developing cybersecurity culture to influence employee behavior: A practice perspective," Comput Secur, vol. 98, p. 102003, Nov. 2020, doi: 10.1016/J.COSE.2020.102003.

[11] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," Feb. 2024, doi: 10.6028/NIST.CSWP.29.

[12] Internacional Organization for Standardization, "ISO/IEC 27001:2022 - Information security management systems," 3. Accessed: Jul. 10, 2024. [Online]. Available: https://www.iso.org/standard/27001

[13] R. C. KESSLER *et al.*, "Clinical reappraisal of the Composite International Diagnostic Interview Screening Scales (CIDI-SC) in the Army Study to Assess Risk and Resilience in Servicemembers (Army STARRS)," Int J Methods Psychiatr Res, vol. 22, no. 4, pp. 303–321, Dec. 2013, doi: 10.1002/MPR.1398.

[14] ANA TERESA CARBONEL and ANTONIO TORRES, "Evaluación de percepción de riesgo ocupacional." Accessed: Nov. 12, 2024. [Online]. Available: http://scielo.sld.cu/scielo.php?pid=S1815-59442010000300003&script=sci_arttext&tlng=en

[15] S. G. LILIAN and C. S. ANDREa, "Confiabilidad y validez de la escala de impulsividad de Barratt (BIS-11) en adolescentes," Rev Chil Neuropsiquiatr, vol. 51, no. 4, pp. 245–254, 2013, doi: 10.4067/S0717-92272013000400003.

[16] K. M. CONNOR and J. R. T. DAVIDSON, "Development of a new resilience scale: the Connor-Davidson Resilience Scale (CD-RISC)," Depress Anxiety, vol. 18, no. 2, pp. 76–82, 2003, doi: 10.1002/DA.10113.

[17] Colegio de Psicólogos, "Test psicológico stai: cómo se califica y qué es." Accessed: Nov. 15, 2024. [Online]. Available: https://colegiodepsicologossj.com.ar/test-psicologico-stai/