Cybersecurity: a general framework in the maritime and military world

Ciberseguridad: un marco general en el mundo marítimo y militar

DOI: https://doi.org/10.25043/19098642.242

Ferney Martínez [1]
Francisco Guevara [2]
Luís Enrique Sánchez [3]
Antonio Santos-Olmo [4]

Abstract

In recent decades, the production of information in studies and research papers on the subject of cybersecurity have addressed the convenience of developing cyberdefense capabilities regardless of whether the scope is industrial or military, corporate or State. However, despite the generation of policies to contribute to the synergy of protection, cybersecurity threats continue to grow, affecting all organizations regardless of their size. The article deals with the existing guidelines, policies and environments within the international framework of cybersecurity in the maritime environment and identifies how these are taken through particular measures to the environments of military maritime units.

Key words: Maritime cybersecurity, ships – military vessels, maritime risk management, cybersecurity threats

Resumen

En los últimos años, multitud de trabajos de investigación relacionados con el tema de la ciberseguridad, han demostrado la necesidad de desarrollar capacidades de ciberseguridad y ciberdefensa, con independencia del ámbito de actuación (civil, militar, corporativo, industrial o gubernamental). Sin embargo, y a pesar de la aparición de nuevas políticas para contribuir a la protección de las amenazas de ciberseguridad, estás no han conseguido doblegar el creciente número de amenazas a las que se ven sometidos los sistemas, y que afectan a todas las organizaciones sin importar su tamaño. Por ello, en el presente artículo se analizan los lineamientos, políticas y entornos existentes dentro del marco internacional de la ciberseguridad en el entorno marítimo y se identifican como estas son implementadas, mediante medidas particulares a los entornos de unidades marítimas militares.

Palabras claves: Ciberseguridad marítima, barcos – buques militares, gestión de riesgos marítimos, amenazas de ciberseguridad.

Date Received: November 18th, 2022 - *Fecha de recepción: 18 de noviembre de 2022*
Date Accepted: February 10th, 2023 - *Fecha de aceptación: 10 de febrero de 2023*

[1] Security and Audit Group, University of Castilla-La Mancha, Spain. Email: Ferney.martinez@alu.uclm.es
[2] COTECMAR and Design Program Research Group (PRODIN), Cartagena, Colombia. Email: Fguevara@cotecmar.com
[3] Security and Audit Group, University of Castilla-La Mancha, Spain. Email: LuisE.sanchez@uclm.es
[4] Security and Audit Group, University of Castilla-La Mancha, Spain. Email: Antonio.Santosolmo@uclm.es

Introduction

The digital transformation that different sectors have undergone leads to the incorporation of new technological advances and modes of operation in their infrastructures, for the maritime field this includes ships, ports and other facilities [1]. The above, allows cybercriminals to focus their efforts to carry out attacks against companies in the maritime industry, leading experts to consider cyber threats as a major obstacle to the digitalization demanded by the sector [2], at the same time, the digital attack surface is increasing and incidents can have serious consequences for important sectors with an impact at all levels [3].

Although greater interconnectivity between ships, personal devices and onshore infrastructure has improved operational efficiency and physical security, it also increases the risks of cyberattacks [4], making it necessary to focus efforts on the identification of technical issues, legal frameworks, among others, with a maritime impact, without neglecting issues such as blackmail, extortion, and ship hijacking, among others [5]. All this makes it necessary for the different stakeholders to join efforts to prevent and build capabilities to respond to technological incidents.

In the maritime sector, regardless of whether its scope is military or civilian, the integration of radar systems, Automatic Identification System (AIS) and Electronic Chart Display and Information System (ECDIS) through digital technologies, provides several benefits for maritime operations, it also makes ships prone to have greater vulnerabilities on board, increasing the risk to cyberattacks [6].

In addition to the risks identified that are to be mitigated, there are those that are continuously generated as a result of a society where digital interconnection prevails every day, but due to the cultural and work dynamics, preventive procedures are put aside, which makes it more important to have risk management procedures in place in order to identify that personnel management and its technological culture is one of the most predominant aspects to close the vulnerability gap.

This document analyzes the international guidelines and/or policies that have been issued as part of the maritime cybersecurity mitigation measures and the way they have been addressed by the Colombian Navy, with an emphasis on an approach to the security culture and the management of human factors in the existing measures. Based on the above, some general recommendations and lines of work are proposed that seek to strengthen different aspects of this important issue.

Context

In recent years, several studies and researches have characterized cyberspace as a military domain, which is why States seek day by day to build and/or increase their military capabilities through the alignment of policies for the acquisition of resources, allocation of personnel, etc. However, this environment has its own climate, characteristics and questions that necessarily modify the use of techniques that are addressed in traditional warfare scenarios.

Different bodies have taken the initiative to generate guidelines, policies and preventive measures focused on the protection of onboard systems and their entire IT infrastructure, such as the provisions of the International Ship and Port Facility Security Code (ISPS) [7], the International Ship Safety Management Code (ISM Code) [8], the provisions issued by the International Maritime Organization (IMO) on Maritime Cyber Risk Management (MSC-FAL.1/Cir.3) [9] and different recommendations and standards issued by the industry (such as ISO, NIST, etc.) for the mitigation of vulnerabilities and cybercrime.

It is worth noting that maritime security system assessments have focused on identifying risks, but have not taken the critical (and costly) next step of directly addressing the vulnerabilities present specifically in the maritime sector. While such risk assessments are important, it is still in the process of detailing safety issues in the systems that control ships and their ports of call [10].

Guidelines

Studies developed in recent years indicate that there are prudent measures that individuals, organizations and nations can implement to improve their cybersecurity. These best practices lead us to the four areas vulnerable to cyber incursions: Software, Hardware, Policies and People [11].

The programs and equipment are the most addressed from the technical area, which is why policies and people are developed in greater detail.

Policies and People

Main International Organizations:

OAS - Organization of American States

Its origin dates back to the First American International Conference, held in Washington, D.C., from October 1889 to April 1890 [12].

The regional efforts of the OAS-led Cybersecurity Program are multifaceted and focus on three axes, as summarized at Table 1:

Table 1. OAS Cybersecurity Program. Taken: [13]

Cybersecurity Program		
I	**II**	**III**
Policy development:	**Capacity building:**	**Research and awareness raising:**
The Program assists OAS member states in developing national cybersecurity strategies that involve all relevant stakeholders and are tailored to each nation's legislative, cultural, economic, and structural situation of each Member State.	The Program helps to establish national computer security incident response teams (CSIRTs) and provides tailored technical assistance and training opportunities. Additionally, it has the CSIRTAmericas network, which provides intelligence on cyber threats and trends in the region.	The Program develops technical documents, toolkits, and reports to guide policymakers, CSIRTs, infrastructure operators, private organizations, and civil society by highlighting current developments and identifying key cybersecurity issues and challenges in the region.

NATO

The purpose of the North Atlantic Treaty Organization - NATO is to guarantee the freedom and security of its members through political and military means.

Although there has been an increased awareness on maritime cybersecurity in the industry, the results of several surveys show that there is still room for improvement from the technological and organizational point of view [14], which has driven NATO to direct the field of cybersecurity and adopt the guidelines indicated in Table 2, which directly impact the military field.

The achievement of adequate security policies and measures is useless unless they come hand in hand

Table 2. NATO policy on cyber defense. With information: [15]

NATO policy on cyber defense			
Developing the NATO cyber defense capability	**Increasing NATO cyber defense capacity**	**Cooperating with partners**	**Cooperating with industry**
NATO's Computer Incident Response Capability (NCIRC) protects NATO's own networks by providing centralized, round-the-clock cyber defense support.	NATO continues to improve the state of its cyber defense through education, training and exercises. NATO conducts regular exercises, such as the annual Cyber Coalition Exercise, and is also enhancing its capabilities for education and training.	Engagement with partner countries and other international organizations to improve shared security by identifying common approaches. NATO works with, among others, the European Union (EU), the United Nations (UN) and the Organization for Security and Cooperation in Europe (OSCE).	The private sector is a key player in cyberspace. Information sharing, exercises, training and education are just a few examples of areas where NATO and industry are working together.

with the achievement of a cybersecurity culture based on awareness raising, teaching and learning; the entire cyber risk environment is framed in initiatives of different organizations such as NATO and the UN that are segregated to organizations in the maritime field for its application from the civil and military sector.

IMO: International Maritime Organization

The United Nations Organization, based in the United Kingdom, is responsible for the safety and security of navigation and the prevention of pollution at sea.

It is the global authority responsible for setting standards for safety, security and environmental performance to be observed in international shipping. Its main function is to establish a regulatory framework for the maritime transport sector (80% of the world's shipping industry moves by sea) that is fair and effective, and that is adopted and applied internationally [16].

As part of the strategies, it issued the Guidelines on Maritime Cyber Risk Management in 2017 to strengthen cyber security in consideration of the digitization of ships. As part of these guidelines, the IMO recommended that each flag state integrate and manage cyber risk issues in the vessel's safety management system (SMS) in accordance with the International Safety Management Code (ISM Code) [17], issued Circular MSC-FAL.1/ Circ.3 Guidelines on the effective management of maritime cyber risks [9], and Resolution MSC.428 Management of maritime cyber risks in safety management systems [18].

TMSA: Oil Companies International Marine Forum

Another organization that has reacted to these changes and quickly updated its guidelines to the new circumstances is the OCIMF (Oil Companies International Marine Forum), a voluntary association of companies involved in the maritime transportation of crude oil, oil and gas, whose mission is to be the leading authority on the safe and environmentally responsible operation of oil tankers, terminals and offshore support vessels; its TMSA (Tanker Management and Self Assessment) program provides such companies with means to improve and measure their SMS, including in it cybersecurity aspects and requirements applicable to these sectors [19], which include the following:

1. Patch and software management procedures.
2. Processes and guidelines for the identification and mitigation of cyber threats.
3. Password management procedures.
4. Development of a cybersecurity awareness and training plan for all personnel involved.

IMCA: International Maritime Contractors Association

IMCA (International Maritime Contractors Association) represents the majority of contractors and production chains associated with the offshore maritime construction industry and its main objective is to help organizations prioritize defense against today's most common and damaging attacks on IT infrastructures [20].

It has also updated its recommendations on cyber threats, which are included in its Security Measures and Emergency Response Guidance - IMCA SEL 037/M 226 [21], consisting of 20 controls and sub-controls focused on various technical measures and activities. The following are included:

- Active management of device inventory and authorized and unauthorized software.
- Bastioning of end devices and network devices.
- Assessment of the team's cybersecurity skills and training program.
- Penetration testing to assess the strength of an organization's defenses.

National Navy of Colombia

The National Navy of Colombia, in order to secure the information that is stored, processed and transmitted in the different computer assets and data centers, issued the information security policies, framed in its Permanent Directive 2014-18 [22], which defines and establishes the mechanisms for measuring information risk, the roles and

responsibilities at each level of the generation and custody of information, which measures must be implemented to secure the information and the media in which it is stored and processed, and the means for the transmission of this information between data centers and terminal stations.

Similarly, and for the proper implementation of the directive, the Digital Security Manual [23] has been established, which defines the guidelines and procedures for the implementation of the security directive of the units of the Navy of Colombia; therefore, the units of the naval fleet must implement all the necessary measures for the assurance of the information and systems used for processing, among others; this manual covers, inter alia, aspects such as:

- Assessment and treatment of information security risks.
- Asset management.
- Physical and environmental security: Measures to prevent unauthorized access to facilities,
- information generation, processing and transmission equipment, protection against external and environmental threats.
- Safety of operations: Defines system and asset protection measures, information backup copies, systems and operational software assurance, among others.
- Management of information security incidents: establish criteria for treatment, registration of the incident and handling, update of risks and their management.

Fig. 1 shows the main information assets on which the protection mechanisms related to the policy are established [22], the same assets that are found in all naval units and must be protected in accordance with the information security guidelines, thus protecting the systems from possible attacks on the information or the systems used for its generation, processing and/or transmission, attacks that will not only put the information at risk, but also the integrity of the ships and their crews.

The maritime sector needs a clear identification and understanding of the threats to which it is exposed, especially in the transport and tourism sector, since the military sector, due to its own operational conception, has implemented complementary methodological strategies for risk management.

Fig. 1. Information assets. Source [23].

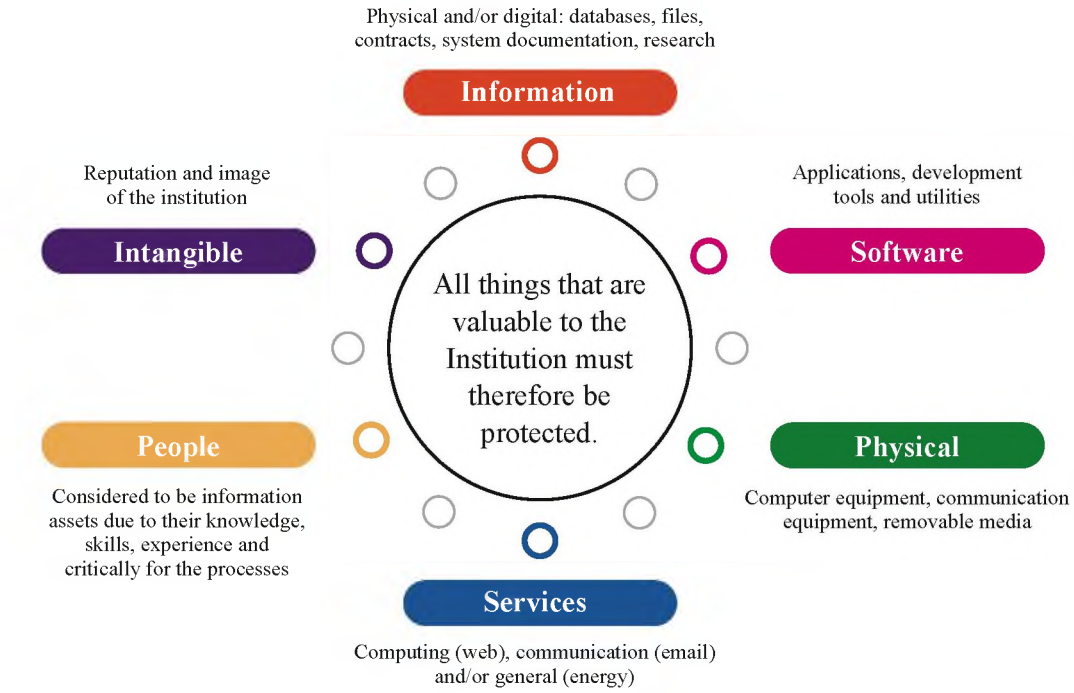


Table 3. Main existing security framework(s) for addressing cybersecurity in the maritime industry

	NIST	ISO	MITRE	COBIT	BSI IT-Grundschutz	OWASP	ENISA
ORIGIN	United States Government	International Organization for Standardization	Mitre Corporation	Information Systems Audit and Control Association: ISACA	Federal Office of Information Security	OWASP Foundation Non-profit organization	European Union Agency for Cyber-Security
OBJECT	A set of guidelines used to minimize organizational cybersecurity risks.	Details specific security controls, internal policies and standardized protocols that are recommended to protect data from misuse or theft	To represent adversary tactics used in a security attack. Documents procedures, techniques and tactics that can be used for advanced persistent threats.	To research, develop, publish and promote an authoritative, up-to-date international set of generally accepted information technology control objectives for day-to-day use.	To provide practice-oriented minimum standards and recommendations for action in the area of computer and web security.	OWASP is a computer security community that works to create articles, methodologies, documentation, tools and technologies that are released and can be used free of charge by anyone.	To improve information security in the European Union. To contribute to the development of an information security culture for the benefit of citizens, consumers, businesses and public sector organizations in the European Union.
METHOD	Identify, protect, detect, respond and recover	Plan, do, check and act	Use of tactics, techniques and procedures on a common basis	Planning and organizing, acquire and implement, deliver and support, evaluate and monitor	Methods, Instructions, Recommendations and Aids - Self-help.	Open and collaborative code.	Development of guidelines, best practices, risk analysis and assessment, and awareness.
USER	Individual companies and other organizations	Companies and organizations	Industrial environments	Governments and businesses.	Companies and organizations	Companies, educational organizations and individuals	European Union States and private sector
PURPOSE	The NIST Framework categories are focused on optimizing risk management and improving the security of systems and assets. They evaluate the actions and policies that are compared with the planning, objectives and resources for continuous improvement.	This family of ISO 27000 standards seeks to guide an organization in the implementation of an Information Security Management System (ISMS) using the ISO 27001 standard together with others. E.G. IEC 61162-460, ISO 16425:2013, IEC 62443-4-1:2018, etc.	Structured list as a way to describe and classify the known trends of attackers orderly recording in matrices the tactics and techniques used providing a taxonomy of the actions that are carried out both on the offensive and defensive side in cybersecurity aspects.	Defines the components for creating and sustaining a governance system: processes, organizational structures, policies and procedures, information flows, culture and behaviors, skills and infrastructure, elements known in the model as Catalysts.	This methodology for information security management systems (ISMS) encompasses technical, organizational, infrastructure and personnel aspects in equal measure. It provides a systematic approach to information security that is compatible with ISO.	One of the fundamental principles of OWASP is that all of its materials are freely available and easily accessible on its website, making it possible for anyone to improve the security of their own web applications. The materials offered include documentation, tools, videos and forums. Perhaps its best-known project is the OWASP Top 10.	To provide support and resources to the member states and the institutions of the European Union in relation to cybersecurity. This includes sharing best practices, promoting collaboration among stakeholders, and providing technical assistance in the development of cybersecurity policies and strategies.
CERTIFIES	No	Yes	Yes	Yes	Yes	Partial/ Courses	No
REFERENCE	[24], [25]	[26]	[27]	[28], [29]	[30]	[31]	[3]

Cybersecurity frameworks play a key role in providing structured and detailed guidance for the protection of critical systems, risk management and incident response. These frameworks enable maritime organizations to build robust cybersecurity capabilities, identify vulnerabilities and implement appropriate controls to mitigate associated risks. In addition, by following internationally recognized frameworks, maritime organizations can establish common and standardized practices, which facilitates collaboration and sharing of threat information in the sector seeking to foster resilience processes in an increasingly challenging environment. Table 3 presents a summary of some of the existing cybersecurity frameworks that, from an industrial point of view, have been applied in the maritime field to encourage their implementation in risk management.

Policy Consolidation

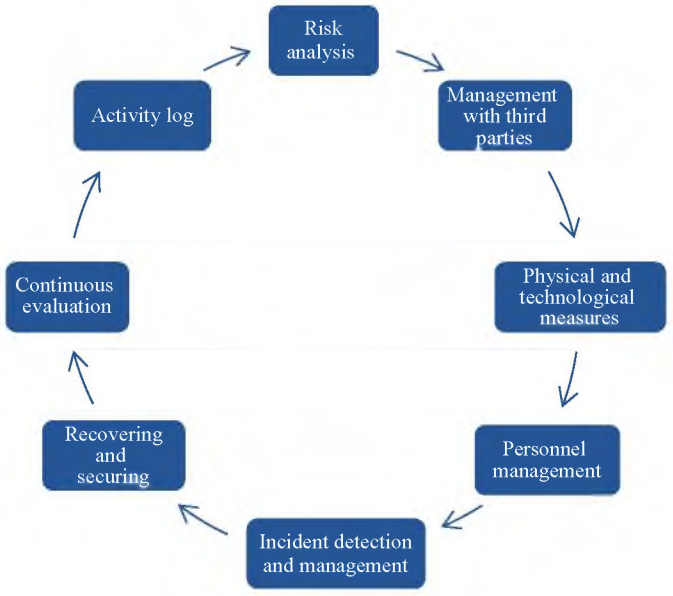
Maritime operators, from an industrial and commercial point of view, are required from January 2021 to comply with a series of security requirements and obligations, and must approve security policies for networks and information systems based on the principles of comprehensive security, risk management, prevention, response and recovery, lines of defense, periodic reassessment and segregation of duties [32]. Military vessels, due to their own operational nature, adopt some of the recommendations and integrate them as part of the technological threat mitigation process by carrying out some of the recommended activities, highlighting the cycle proposed in Fig. 2.

Conclusions

The main conclusions of this article are presented below:

- Cybersecurity is a race between attackers and defenders, where the advantage goes to the attacker, because they can choose the attack methodology and have the time to choose the best way to do it. Since we cannot be completely sure, we must take all the knowledge that we can add between the events that have occurred and the technological analysis of our organization.
- The exponential use of data for analysis and decision making, smart ships, the "industrial internet of things" IIoT, among other factors, is increasing the amount of information available for organizational use as well

Fig. 2. Basic aspects to fulfil. Source: own design



as for cyberattackers. Although there are working frameworks, official references and technological tools, cyber risk management in the maritime field still lacks working spaces from the organizational, technological and user spheres for maritime cybersecurity to become an inherent part of ships at all levels, ranging from onshore managers to ship personnel, led by their captain and those tasked with cyberthreat technology.

- The continuous technological evolution means that all the measures taken for the mitigation of risks aboard ships are constantly evaluated, according to the policies and reports that are permanently generated by the different stakeholders involved in the operation and maintenance of systems, but this must go hand in hand with adaptation, depending on the application environment.

Future Work

In order to continue developing the proposed issues and master the subject, the following future works are proposed:

- To identify possible existing gaps in frameworks, standards, guidelines, rules, etc. in order to propose an initial viable solution for the vessels built in and that are part of COTECMAR.
- To support the construction of a framework to characterize, measure and take actions to mitigate vulnerabilities using knowledge bases, expert input, etc. as backbone.
- Based on the items described above, to propose a case study to conduct a review of: 1. Cybersecurity practices currently applied and 2. Cybersecurity practices generated from the proposal.

Bibliography

[1] G. A. WEAVER, B. FEDDERSEN, L. MARLA, D. WEI, A. ROSE, AND M. VAN MOER, "Estimating economic losses from cyber- attacks on shipping ports: An optimization-based approach," Transp Res Part C Emerg Technol, vol. 137, Apr. 2022, doi: 10.1016/j.trc.2021.103423.

[2] A. AMRO, A. ORUC, V. GKIOULOS, AND S. KATSIKAS, "Navigation Data Anomaly Analysis and Detection," Information (Switzerland), vol. 13, no. 3, Mar. 2022, doi: 10.3390/info13030104.

[3] P. H. MELAND, K. BERNSMED, E. WILLE, J. RØDSETH, AND D. A. NESHEIM, "A Retrospective Analysis of Maritime Cyber Security Incidents," 519-530, vol. 15, no. 3, pp. 519–530, 2021, doi: 10.12716/1001.15.03.04.

[4] K. TAM AND K. JONES, "MaCRA: a model-based framework for maritime cyber-risk assessment," WMU Journal of Maritime Affairs, vol. 18, no. 1, pp. 129–163, Mar. 2019, doi: 10.1007/S13437-019-00162-2/FIGURES/14.

[5] T. P. AVANESOVA, L. K. GRUZDEVA, R. A. IUSKAEV, D. YU GRUZDEV, AND M. L. SOMKO, "Analysis of cyber-security aspects both ashore and at sea," IOP Conf Ser Earth Environ Sci, vol. 872, no. 1, Oct. 2021, doi: 10.1088/1755- 1315/872/1/012024.

[6] W. C. LEITE JUNIOR, C. C. DE MORAES, C. E. P. DE ALBUQUERQUE, R. C. S. MACHADO, AND A. O. DE SÁ, "A Triggering Mechanism for Cyber-Attacks in Naval Sensors and Systems," Sensors (Basel), vol. 21, no. 9, May 2021, doi: 10.3390/S21093195.

[7] INTERNATIONAL MARITIME ORGANIZATION, "The ISPS Code and Chapter XI-2 of the SOLAS Convention." https://www.imo.org/es/OurWork/Security/Paginas/SOLAS-XI-2%20ISPS%20Code.aspx (accessed Feb. 06, 2023).

[8] INTERNATIONAL MARITIME ORGANIZATION, "ISM Code and

Guidelines for Implementation of the ISM Code." https://www.imo.org/es/OurWork/HumanElement/paginas/ismcode.aspx (accessed Feb. 06, 2023).

[9] OMI, "GUIDELINES ON MARITIME CYBER RISK MANAGEMENT," MSC-FAL 1-Circ 3.docx, Jul. 05, 2017.

[10] S. PAPASTERGIOU, N. POLEMI, AND P. KOTZANIKOLAOU, "Design and validation of the Medusa supply chain risk assessment methodology and system," International Journal of Critical Infrastructures, vol. 14, no. 1, pp. 1–39, 2018, doi: 10.1504/IJCIS.2018.090647.

[11] K. NEWMEYER, E. CUBEIRO, AND M. SANCHEZ, "Cyberspace, Cybersecurity and Cyberwarfare," 2015, Accessed: Jan. 23, 2023. [Online]. Available: https://repositorio.esup.edu.pe/handle/20.500.12927/113

[12] ORGANIZATION OF AMERICAN STATES, "Executive Summary Maritime Cybersecurity," MARITIME CYBERNETIC SECURITY IN THE WESTERN HEMISPHERE , vol. 1, pp. 9–10, 2021, Accessed: Mar. 13, 2023. [Online]. Available: https://www.oas.org/es/sms/cicte/docs/La-seguridad-cibernetica-maritima-en-el-Hemisferio-Occidental-introduccion-y-directrices.pdf

[13] ORGANIZATION OF AMERICAN STATES, "OAS Cybersecurity Program," OAS : CICTE: Cybersecurity: Activities, Feb. 02, 2022. https://www.oas.org/es/sms/cicte/prog-ciberseguridad.asp (accessed Mar. 12, 2023).

[14] D. HEERING, "Ensuring cybersecurity in shipping: Reference to Estonian shipowners," TransNav, vol. 14, no. 2, pp. 271– 278, Jun. 2020, doi: 10.12716/1001.14.02.01.

[15] NORTH ATLANTIC TREATY ORGANIZATION - NATO, "NATO - A POLITICAL AND MILITARY ALLIANCE," 2.1 A Political and Military Alliance, 2016. https://www.nato.int/nato-welcome/index_es.html (accessed Mar. 12, 2023).

[16] IMO, "International Maritime Organization ," 2020. https://www.imo.org/es/About/Paginas/Default.aspx (accessed Mar. 25, 2023).

[17] B. XING, J. DAI, AND S. LIU, "Enforcement of opacity security properties for ship information system," International Journal of Naval Architecture and Ocean Engineering, vol. 8, no. 5, pp. 423–433, Sep. 2016, doi: 10.1016/J.IJNAOE.2016.05.012.

[18] INTERNATIONAL MARITIME ORGANIZATION, "MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS ," 2017. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf (accessed Mar. 28, 2023).

[19] OCIMF - Oil Companies International Marine Forum, "Tanker Management and Self Assessment 3 - A Best PracticeGuide," 2014. https://www.ocimf.org/es/publicaciones-y-promoci%C3%B3n/publicaciones/libros/tanker-management-and-self-assessment-3 (accessed Mar. 27, 2023).

[20] IMCA, "International Maritime Contractors Association," 2022. https://www.imca-int.com/about-imca/ (accessed Mar.13, 2023).

[21] IMCA, "Security measures and emergency response guidelines - IMCA," 2021. https://www.imca-int.com/product/security-measures-and-emergency-response-guidelines/ (accessed Mar. 13, 2023).

[22]COLOMBIAN MINISTRY OF NATIONAL DEFENSE, "Permanent Directive DIR2014-18," 2014. https://marinanet.armada.mil.co/system/files/

basicpagefiles/A_Directiva2014-18_SeguridadInformaci%C3%B3n.pdf (accessed Jan. 25, 2023).

[23] NATIONAL NAVY OF COLOMBIA, "Manual de Seguridad Digital," MANUAL DE SEGURIDAD DIGITAL ARMADA NACIONAL, 2022, Accessed: Jan. 25, 2023. [Online]. Available: https://marinanet.armada.mil.co/system/files/basicpagefiles/Manual%20de%20Seguridad%20Digital%20Armada%20Na cional.%20Segunda%20Edicion.%202022.%20V.%20Final%20Preliminar%20%20%28FP.%2018NOV2022%29.pdf

[24] R. TALAS, "Port security," Advanced Sciences and Technologies for Security Applications, pp. 161–172, 2020, doi: 10.1007/978-3-030-34630-0_10.

[25] Ž. TURK, B. GARCÍA DE SOTO, B. R. K. MANTHA, A. MACIEL, AND A. GEORGESCU, "A systemic framework for addressing cybersecurity in construction," Autom Constr, vol. 133, p. 103988, Jan. 2022, doi: 10.1016/J.AUTCON.2021.103988.

[26] IEC, "Spanish Standardization IEC 61162-460:2018 ," 2018. https://www.une.org/encuentra-tu-norma/busca-tu-norma/iec?c=63097 (accessed Mar. 11, 2023).

[27] The MITRE Corporation, "MITRE ATT&CK®." https://attack.mitre.org/ (accessed Mar. 26, 2022).

[28] A. C. AMORIM, M. MIRA DA SILVA, R. PEREIRA, AND M. GONÇALVES, "Using agile methodologies for adopting COBIT," Inf Syst, vol. 101, Nov. 2021, doi: 10.1016/J.IS.2020.101496.

[29] ISACA, "COBIT | Control Objectives for Information Technologies | ISACA," Mar. 19, 2022. https://www.isaca.org/resources/cobit

[30] "BSI - Federal Office for Information Security." https://www.bsi.bund.de/DE/Home/home_node.html (accessed Mar. 27, 2023).

[31] "OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation." https://owasp.org/ (accessed Mar. 27, 2023).

[32] ... 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: Jan. 23, 2023. [Online]. Available: https://armada.defensa.gob.es/archivo/rgm/2022/03/rgmmar2022cap03.pdf