OBSERVARE
Universidade Autónoma de Lisboa

e-ISSN: 1647-7251
Vol. 11, Nº. 2 (November 2020-April 2021)

JANUS.NET
e-journal of International Relations

THE IMPACT OF CYBERSECURITY ON THE REGULATORY LEGAL FRAMEWORK FOR MARITIME SECURITY

DUARTE LYNCE DE FARIA
duarte.lynce.faria@gmail.com
Holder of Ph.D. in International Private Law from the University of Extremadura and in Corporate Law from the Faculty of Law of Lisbon with a research thesis in Maritime Law. Holder of a Master Degree and a Bachelor Degree in Law, Faculty of Law of Lisbon and of a Bachelor Degree in Military-Naval Sciences from the Navy Academy. As a Navy Officer he attended several courses in naval operations, communications and electronic warfare and performing duties on board ships and ashore, namely, at the Portuguese Navy Staff. He is a visiting professor at the Faculty of Law at Nova University of Lisbon, the Navy School and at the Navy Higher School Infante D. Henrique, a lecturer at the Military University Institute and a researcher at CEDIS, CINAV and at CIDIUM. He held several management positions at the Maritime and Port Institute (IMP), in the Administration of the Ports of Setúbal and Sesimbra (APSS, SA) and in the Administration of the Ports of Sines and Algarve (APS, SA).

Abstract

The concepts of maritime safety and maritime security were based, originally, on different aims, objectives, and perspectives. However, currently, most of the international maritime safety conventions have started to cover both aspects. In the analysis of most incidents and accidents at sea, it is quite difficult to delimit safety and security matters and, normally, after a breakdown, it is useless to do it since the planning and response to risks are usually given in an integrated manner. On the other hand, we are witnessing a progressive extension of the concept of maritime safety to include protection (or security) matters simultaneously with the emergence of a new type of threats that are always present from the moment computers are connected to networks anywhere the world: cyber threats! With ships equipped with new advanced technologies, protection against cyber-attacks is more important than ever. These technological advances have become an easy and high-priority target for cyber criminals. With this behaviour, they can pursue their purpose of attacking ships' systems and, from them, different systems ashore. The digitization of the maritime industry took place very quickly. However, it has become essential for seafarers not only to understand and adopt these new technologies, but also to take a cautious attitude towards certain events that can follow in the wrong direction in a short period of time. A new stage of maritime readiness is envisaged, which needs a robust and well-defined "code" that broadens and concretizes a "new" concept of maritime safety in the broad sense that reinforces international maritime conventions and their application. The responsibilities of the "Flag States" and "Port States", under the terms of the United Nations Convention on the Law of the Sea (UNCLOS) and international maritime conventions as laid down in the different Memoranda of Understanding (MoU) at world level and in the documents of the IMO and other international organizations (such as the European Union), should be updated and start to consider, also, maritime security matters. In addition, it is essential to support close cooperation in the fields of maritime safety and maritime security with a view to drawing up a new and robust "Maritime Code". This will be the guideline pursued, with the intention, at this moment, to "shake and roll" this matter towards a new regulatory stage.

Keywords
Maritime safety; Maritime security; Cybersecurity; Flag State; Port State.

How to cite this article

Faria, Duarte Lynce de (2020). "The impact of cybersecurity on the regulatory legal framework for maritime security". In Janus.net, e-journal of international relations. Vol. 11, No. 2 Consulted [online] at date of last visit, DOI: https://doi.org/10.26619/1647-7251.11.2.10

Article received on March 21, 2020 and accepted for publication on September 23, 2020

THE IMPACT OF CYBERSECURITY ON THE REGULATORY LEGAL FRAMEWORK FOR MARITIME SECURITY[1]

DUARTE LYNCE DE FARIA

I. Introduction[2]

When in July 2017, the world's largest shipping company in container transport (the Danish "MAERSK") suffered a cyber-attack that completely paralyzed its information technology systems for several weeks, the maritime-port sector "woke up" to the huge impact of this new threat.

The damage amounted to 250-300 million dollars[3] and involved the reinstallation of 45.000 workstations and 4.000 servers worldwide. The "culprit" was the "NotPetya" ransomware. Moreover, this malware had already attacked the Dutch company TNT Express in June 2017, as recognized by the FedEx (NYSE: FDX)[4].

In fact, with ships equipped with the most modern technologies for the bridge, the engine room and the whole vessel in general, the threat of cyber-attacks is more important than ever since most of the new systems work automatically and are extremely dependent on IT and data flows.

[1] Article translated by Carolina Peralta.

[2] This article was close to its conclusion when the COVID-19 pandemic broke out. In addition to compelling to (re)think the global world - with its strengths and weaknesses, its opportunities and threats (in a true SWOT analysis) - it is important to mention that "infectiology" can also far exceed the health domain. The example of the virulence of different malware at the level of all systems connected to the network can also, in times of crisis such as the one we are going through, drastically limit the response of health equipment and civil protection that require the adoption of pre-planned responses associated with different systems. For this reason, it is also necessary to plan the adoption of alternative measures, albeit with less efficiency, but with greater resilience to the fragility that some systems still present, particularly in these periods of greatest danger to mankind.

[3] Direct costs. According to more recent estimates, total costs may have reached 600 M €. Let us check the threats to cybersecurity in 2020. In a recent article entitled *"2020 Vision: Check Point's cyber-security predictions for the coming year"*, of 24 October 2019, in *https://www.checkpoint.com, blog.checkpoint.com, https://usercenter.checkpoint.com/usercenter/index.jsp,* the situation related to cybersecurity has been described as follows:
1. A new cyber 'cold war'; 2. Fake news 2.0 at the U.S. 2020 elections; 3. Cyber-attacks on utilities and critical infrastructures will continue to grow; 4. High profile US brands, beware of cyber-attacks targeting high-profile American companies; 5. Increased lobbying to weaken privacy regulations.
Regarding the perspectives related to cybersecurity technology, the main threats and forms of action expected for 2020 are as follows 2020:
1. Targeted ransomware; 2. Phishing attacks go beyond email; 3. Mobile malware attacks step up; 4. The rise of cyber insurance; 5. More IoT devices, more risks; 6. Data volumes skyrocket with 5G; 7. AI will accelerate security responses.

[4] See news *in* John Gallagher*, Freight Wave,* 29-03-2019.

These are just two examples of targets at the mercy of cyber-attacks. As in other economic sectors, the maritime-port sector tends to increasingly rely on technology for being more competitive, more efficient in the management of its resources or responsible for complying with standards or policies.

On a global scale, there is an increasing procedural integration of the actors in the logistics chains and, consequently, of the ports, using services based on information systems.

The "Single Logistics Window" (commonly known in Portugal as "JUL"- "Janela Única Logística") - developed by Portuguese ports establishes the connection on an electronic platform between each port and authorities, shipping agents, freight forwarders and port, rail, road and logistics operators, securing the flow of goods traffic and passenger movement without the production of paper documents. This is a good example of this type of systems and of the level of integration of optimization provided for ports and other platforms included in the logistics chains.

These new technological advances have become an easy target for criminals[5]. There are several cybersecurity challenges that ports and associated platforms must face, whatever the type of technology or information system shall be used in the various activities.

The threats are so many, from interception of communications to service blocking, malware, identity theft, data theft or manipulation and information leakage, among others. The impacts can also be of various kinds and harmful, such as, for example, total paralysis of operations, death or injuries to people, kidnapping, cargo theft and financial or reputation losses, which must be avoided at all costs.

It is critical to prevent criminal entry into the ship's systems by unauthorized and uncertified persons, which implies an effective control of the access of a crew member who uses, for example, a free "Wi-Fi" network for telephone calls and emails next to land. Vulnerability is the immediate result of the almost permanent interconnection that today a modern ship has, which means that, due to the use of the same equipment as the ship's systems with unauthorized access to common networks, the onboard systems can be easily "infected" and thus compromised (for example, the opening of a phishing e-mail attachment or hyperlinks or a previously "infected" media news[6]).

The impacts of this unauthorized and criminal access can be very serious: disruption of the network, absence of information flows between the ship's control systems, unauthorized access to control and IT systems, unauthorized changes to the system parameters, harmful consequences on the environment, maritime safety on board jeopardized and the ship's critical and emergency procedures, and, if nothing is done in a timely manner, a security problem can quickly become a safety one[7]*.*

[5] Since the introduction of new technology in each process increases the risk of human failure and the vulnerability degree.

[6] *Infected removable media.*

[7] Some authors are also beginning to envisage the chances of an occurrence of "safety" becoming a "security" incident in the maritime sector. These are, for example, sea events (stranding, collision, open water, etc.) that imply that a set of threats to the IT systems - now being degraded - materialize, preventing them from contributing to reducing on-board breakdowns.

Another very popular mode of action is the spoofing of the GPS[8] signal through ground stations - that can also take advantage of the differential GPS systems ashore (which use the platforms of many lighthouses) that have been designed to improve the accuracy of that positioning system - as reported in 2018 in the Eastern Mediterranean, the Black Sea and the Persian Gulf.

In 2019, "aggressive" spoofing of the GPS signal in 20 coastal areas of the PR of China, including the ports of Shanghai, Fuzhou (Huilutou), Qingdao, Quanzhou (Shiyucun), Dalian, and Tianjin was reported[9] by several entities and in particular by the US Coast Guard. The November 2019 MIT Technology Review magazine featured an article on this phenomenon, where the analyst Bjorn Bergman evaluated a substantial amount of information contained in the AIS (Automatic Identification System) of ships. In this analysis, he identified at least 20 locations close to the Chinese coast where the spoofing occurred in similar ways during 2019, some of which in oil terminals.

The organization C4ADS (Center for Advanced Defense Studies), based in Washington DC, also found that the spoofing of the signal was maintained for some time in those same areas[10].

These occurrences were more persistent in the port of Dalian, in northern China, next to North Korea. It can be suspected that, given the chosen moment - when the US sanctions prohibiting the purchase of Iranian oil were in force- and it was proved, by third parties, that China had received that product, it would have been an operation to avoid the exact location of the ships involved in the oil transfer. In other cases, the spoofing of the GPS signal may also be related to important official visits, a resource also used by Russia to protect (i.e., cover up) official VIP visits.

This type of "mass" spoofing is easier to detect in coastal areas where there is a wide availability of AIS data provided by terrestrial or satellite channels, and may be caused by the spoofing of a satellite signal and another type associated with a land station or device.[11]

[8] The Global Positioning System (GPS) is a satellite navigation system designed to indicate the position of a mobile receiver from the simultaneous reception of at least three satellites. Two such systems are in operation: The North American GPS and the Russian GLONASS. However, two other systems are being launched: the European Union GALILEO and the Chinese COMPASS (or Beidou-2). The North American system is managed by the United States Government and began to be used exclusively by the military (however, the accuracy of the encrypted system for military use, namely, to aid in the direction of cruise missiles, was maintained). Its civilian use can quickly be altered or even lead to its blocking in periods of tension or crisis, including giving incorrect positioning information ("spoofing" from an internal source), as can happen with the use of differential GPS stations (which are able, in normal operation, to increase the accuracy of the geographical position of the receiver) for the introduction of errors in the positioning of the vehicle. GPS spoofing is the deliberate introduction of signals in the mobile receivers by other stations and which aims to indicate a wrong geographical position. This GPS spoofing signal usually coincides with unauthorized access to the IT systems that seeks to hide the user's true identity.

[9] See the article by Goward, Dana A., *"Patterns of GPS Spoofing at Chinese Ports",* MAREX, *in Daily Collection of Maritime Press Clippings 2019-356,* pp. 31-32*.*

[10] C4ADS is a private non-profit organization that aims to analyse and report data in a context of conflict or transnational security issues.

[11] See the U.S. Coast Guard's account of situations related to the spoofing of the GPS signal in *https://navcen.uscg.gov/?Do=GPSReportStatus.* See also the article in China, "The American Club",*" Mass Global Positioning System (GPS) spoofing at ports in The People's Republic of China" in* "Daily Collection of Maritime Press Clipping 2010-002", p. 25.

The spoofing of electronic signals goes back to the time of the "Cold War", together with jamming and counter-jamming measures, and ECM and ECCM measures (Electronic Countermeasures and Electronic Counter Countermeasures, respectively). Thus, the transmission of false radar echo to mislead the opponent on his radar console was classified as deception jamming.[12]

When the GPS system went into production, it was easy to see that its code was vulnerable to spoofing since it was an open code,[13] reproducible by anyone, through a simulator (i.e., the spoofing of the GPS signal). Naturally, this was the reason for the GPS system to also transmit an encrypted military signal (the so-called "P (Y) code"), in addition to allowing much higher precision in the conduct of military operations, particularly directing weapons.

However, as the GPS system started to have a universal civilian use, the vast majority of receivers are not capable of receiving coded signals and the development of coding for civilian purposes is not easy to harmonize and decide for system management. However, there are currently vulnerable critical infrastructures that should deserve special attention regarding the reception of GPS signals, particularly regarding the vehicles that use them daily[14].

It turns out that the exponential growth in the market of certain specific transmitters (acronym SDR – "Low Cost Software Defined Radio") has currently made spoofing available to anyone who can simulate satellite transmission on the very same frequencies and signal characteristics. The time when communication frequencies with satellites were only available to the military is long over…. and there are even instructions on the Internet on how to spoof the radio control signals of drones.

These new threats clearly demand a reflection on how to approach "safety at sea" because, on one hand, the traditional divisions between "safety" and "security" are not closed and are mutually influential and, on the other, they themselves demand the consecration of a new instrument that fits them and also benefits from the strategic (and sovereign) thinking of States regarding the "use of the sea".

Although the concept of "safety at sea" is not a new one, the role of the maritime environment in the safety of States today assumes a strategic relevance that has been reinforced since the beginning of this decade, in an increasingly holistic view, particularly at European Union level[15]. In fact, it is "over the sea and in the ports" that most of the

[12] See *https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/.* It happens, however, that what was restricted to the military field - list of threats, contingency plans, timely detection and cancellation/limitation of damages - is now shared by the entire society. Therefore, it is necessary to face a new reality, especially in the scope of the so-called soft kills, i., e., the use of equipment and systems that neutralize threats without physically destroying them through, namely, their disruption and that should also be used outside the strictly military field.

[13] See Kaplan, Elliott D., and Hegarty, Christopher J., *"Understanding GPS Principles and Applications",* 2nd Edition, ARTECH HOUSE, Boston-London, Norwood, MA, USA, 2006.

[14] To mitigate this situation, the European Union, within the framework of the GALILEO system, will provide a set of additional services, called Public Regulated Services (PRS), which aim to provide, to state entities and providers of essential services and critical infrastructure, a signal of geolocation more resistant to spoofing and jamming.

[15] See Pedra, José Rodrigues, *"A União Europeia e a Segurança no Mar", in* Cajarabille, Victor Lopo and others, "A Segurança no Mar – uma visão holística", Mare Liberum, Aveiro, 2012, pp. 143-162. The author makes a brief reference to the concept of "Security at Sea" based on the work of Grove, Eric, "Maritime Strategy

trade essential for the well-being of the population is to be found, with special reference to the imports of hydrocarbons (or energy sources in general) and as an alternative to land-based assets.

It is, therefore, desirable that the conceptual paradigm is progressively changed and expanded, i.e., on one hand, traditional maritime safety will have to be strengthened with measures to protect against illicit and disruptive attacks and, on the other, in legal terms, the "excusable" or "negligent" conduct of the crews should be less and less applied in view of the existing regulations - which include codes of good practices - and the serious consequences that can result from them. Those measures have a precautionary or preventive nature, but also reactive features, both in limiting the damage and in adopting alternative procedures provided for in contingency plans.

This approach will necessarily have consequences regarding the characterization of the reaction to and the combat of serious maritime accidents (such as, for example, oil spills in the jurisdictional spaces of a State), which is considered to have a strong security component since its origin, i.e., considering "wilful" (and not "negligent") the conduct of the crew that violates the rules of maritime safety resulting in the creation of a "danger" or "damage", legally qualified as "serious”.

So, it looks that by extending the "malicious" conduct of the agent (and by reducing the "negligent" acts which, at times, exonerated or limited the liability of agents and companies), the way for the great majority of large maritime disasters is paved. This includes, for example, oil spills from ships, which will be considered from their origin an event in the scope of "security" and, consequently, as an increased regulatory role within the scope of the States[16].

and European Security", London, Brassey's, 1990, which, reminiscent of the nuclear deterrence strategy of the Cold War, refers to the importance of the sea for European security. However, it is with the presentation of the Maritime Strategy for the Atlantic in 2011, together with the Green Paper for European Integrated Maritime Policy and the European Integrated Maritime Policy that this strategic perspective for the use of the sea is reborn. More than the value of communication and transport, the sea is a source of essential resources and an indispensable means for the control of activities on land with the very projection of power and defence in advance and "in depth" that are essential to assert the European interests. See Pedra, José Rodrigues, *op. cit,* pp. 149-155. On the other hand, this strategic relevance has also emerged as a result of the impact that the exploration and exploitation of marine resources have impacted progressively in the economies of States, faced with the growing scarcity and limitation of access to terrestrial resources. This situation has placed on the international agenda the countries' disputes regarding the delimitations of the contiguous seabed and the candidacies for the extensions of the continental platforms. Among others, see Duarte, António Rebelo, *"Políticas e Estratégias Marítimas da Europa e de Portugal",* Cadernos Navais, no 48, April-June 2018, Centro de Estudos Estratégicos da Marinha, in www.marinha.pt.

[16] At this point, it is appropriate to invoke a matter that also initiated its doctrine in Criminal Law and which, later, moved into the domain of International Law. It was about, in the criminal sphere, to legitimize, for example, the action of a severely disabled person (i.e., paraplegic) when he knew, with almost absolute certainty, that someone would come and murder him in the place where he was alone and without access to any contacts. And the question was whether it would be legitimate for the putative victim to neutralize the agent, shooting him in advance before entering the place where he was (for example, through a window). This example shows the difference, in International Law, between the "preventive" attack and the "preemptive" attack, legitimizing, in the latter case, the anticipated intervention in face of the intention (and evidence) of an imminent attack. Thus, the "preventive" attack falls to have legal legitimacy, given its arbitrariness and placed at the service of an "right of force" of impossible scrutiny, aiming only at pursuing a strategy to avoid changes in the balance of power that could favour the adversary. According to article 51 of the Charter of the United Nations, the "right of self-defence" is only recognized in the case of an armed attack and, with that extension, an attempt was made to include the intention of "armed attack". Now, in this case, the "imminent attack" (or to put it another way, the "real threat") exists from the moment

II. The influence of national security and sea environment on the concept of "Safety at Sea"

The word "security" has numerous meanings, albeit with a common sense, both within the scope of the activity itself and with regard to the result: *the protection (or guarantee) of a certain right or asset in the face of risks or obstacles that they come across*. This means that, in the absence of obstacles to its exercise, it is unnecessary to adopt additional guarantees[17].

Several security classifications can also emerge according to different criteria, namely, the protected subject (or target entities), the assets or materials to be protected, the territorial scope of intervention, the structures that ensure it and the intensity of the disturbance carried out (i.e., the effect of threats, risks and dangers on said assets or rights)[18].

In addition to these criteria, "security" can also appear on several other forms – in conjunction, sometimes, with the word "safety", but really with a "protection" sense - depending on its specific object[19], including energy security, safety at sea, maritime safety, air safety and transport safety. In this small list, it is a question of delimiting security depending on the activity carried out, which, in some cases, involves different transport segments (land, river, sea and air) and, in others, certain essential equipment and networks that interconnect them (energy security and cybersecurity, for example).

The security activity that is projected in the territorial scope of action of the resources in a given State must obey an upper spatial and material dimension called "national security" (alongside local, regional, international and global security). This concept arose in defence matters, prevailing the word "security" or "protection" against wilful and illegal acts.

It is clear that, nowadays, traditional "national security" is no longer just prosecution against criminal acts, but also embraces the prevention and solution of natural risks, within the scope of civil protection, increasing it in the sense of "safety" without, however,

the ship's IT systems connect to the outside and, thus, it will be up to the Flag State to update its regulations and procedures to take into account the "preemptivity" of the exercise of the ship and the company. See, *inter alia,* Santos, Sofia, *"Defesa preemptiva"* e *"Defesa preventiva"* in Gouveia, Jorge Bacelar and Santos, Sofia (coord.), "Enciclopédia de Direito e Segurança", Almedina, Coimbra, 2015, pp. 102-105.

[17] See Gouveia, Jorge Bacelar, *"Direito da Segurança Cidadania, Soberania e Cosmopolitismo",* Almedina, Coimbra, 2018, pp. 89 and following. The author supports the concept of a new branch of law: Security Law, and its dogmatic roots and autonomy and the analysis of State and international security entities that emerged. "Security Law" is defined as the "system of legal rules and principles that define the organization and functioning of security structures, establishing their powers and limits, with a view to protecting the fundamental legal rights and assets of citizens and political communities" (up to p. 119). This article is being framed on it, especially since in the future we will seek to "let go of the ropes and lines of the "new" Maritime Safety Law - that should embrace the security matters (as SOLAS Convention did with the ISPS Code). In our point of view, this is the moment to "grant" it its autonomy, in confrontation with the "Law of the Sea" and with "Maritime Law". However, the maritime world has started with the "safety" concept (rather than "security") and so it is easier to keep the word "safety" but now including "security" matters.

[18] *Ibidem,* pp. 90-91.

[19] *Maritime Law* deals with a specific object (the activity of maritime transport) within the scope of Commercial Law, which is more general but has not diminished its classification as a branch of Law. See also *ibidem* pp.93-96.

neglecting its "supra-state dimension, in line with the magnitude of the risks of terrorist attacks that are no longer national, localised, public and with conventional weapons, thus reinvigorating it in its sense of "security"[20]. Thus, "national security" is associated with national defence which, of course, interacts with political and strategic options above "security at sea" itself.

The concept of "national security"[21] embodies a strategy of the state itself traditionally focused on military threats to its border or other unconventional threats, such as climate change and global economic and financial crises, including those of a hybrid nature which, in the maritime domain, can have quite different implications[22]. For there to be a minimum definition of "national security", a relationship with the strategy is required

[20] *Ibidem,* p. 96.

[21] In the Portuguese legal framework, the concept of "National Security" was not formally defined. However, regarding doctrine, see Gouveia, Jorge Bacelar, *"Direito da Segurança Cidadania, Soberania e Cosmopolitismo",* Almedina, Coimbra, 2018, pp. 92 and following and Couto, Abel Cabral, *Elementos de Estratégia, Volume I,* IAEM, Lisbon, 1988, pp. 172 and following. See also Garcia, Francisco Proença, *"Defesa Nacional"* in Gouveia, Jorge Bacelar and Santos, Sofia (coord.), "Enciclopédia de Direito e Segurança", Almedina, Coimbra, 2015, pp. 99-101. This author discusses the difference between the concepts of National Defence and National Security, proposing that the latter be adopted "resulting from a set of state policies duly articulated, in the military aspect but also in other sectoral policies such as the economic, cultural, and educational system, which includes coordinated actions of internal and external security, whose frontier is currently blurred". On the blurring between internal and external security, see Santos, Ana Miguel dos, *"Uma segurança interna cada vez mais europeia? Uma segurança externa cada vez mais nacional?"* in RDeS - Revista de Direito e Segurança, Ano VI, Jul-Dec 2018, pp. 27-51, Guedes, Armando Marques, *"Segurança externa"* e *"Segurança interna", in* Gouveia, Jorge Bacelar and Santos, Sofia (coord.), "Enciclopédia de Direito e Segurança", Almedina, Coimbra, 2015, pp. 411-418 and 425- 431 and Lourenço, Nelson, *"Segurança interna", ibidem,* pp. 431-433. Regarding the concept integrated in the Constitution, see Gouveia, Jorge Bacelar, *"Direito Constitucional da Segurança", ibidem,* pp. 13-136. We chose this collection as it started to conceptualize "safety at sea", which should cover "matters of maritime safety and maritime security and, in spatial terms, on ships and ports.*"* (p. 435) in the article *"Segurança no mar", ibidem,* pp. 433-439. However, the "Strategic Concept of National Defence" (CEDN), approved by Resolution of the Council of Ministers no. 19/2013, of 21 March, although based on the concept of "national security", includes very important elements on the relevance of the sea in this context, considering, namely, that "as a strategic asset, the sea must be integrated in a broad perspective of national security and defence". Another component that may influence "safety at sea" concerns the definition of sectoral strategies. At national level, the "National Strategy for the Sea for the period 2013-2020" (ENM), approved by Council of Ministers Resolution no. 12/2014, of 23 January, emphasizes the use and preservation of the sea as a national asset, which reinforces the strategic relevance of "safety at sea". See note 13. The new National Strategy for the Sea - ENM 2021-2030 (in https://www.dgpm.mm.gov.pt/enm) is currently under public discussion - of which the following framework is cited on pp. 3-4:
"Portugal started to monitor the economic relevance of the Sea in its national economy through a Satellite Sea Account, which resulted from a protocol between the National Statistics Institute (INE) and the Directorate-General for Sea Policy (DGPM) signed in 2013. According to estimates by the European Commission, in 2018, gross added value (GVA) in the blue economy represented 3.2% of the GVA in the national economy. The employment value generated represented 5.5% of national employment. These figures are among the highest in EU Member States. The sustainability of the blue economy depends on the conservation of the marine environment, and the services of its ecosystems, as well as the safeguarding of the maritime cultural heritage. The National Maritime Spatial Situation Plan, the Strategic Guidelines and Recommendations for the Implementation of a National Network of Marine Protected Areas approved in 2019, as well as the assessment of the Good Environmental Status of Marine Waters recently reported in compliance with the Marine Strategy Framework Directive, represented important milestones to ensure our commitment to the defence of marine ecosystems and nautical and underwater cultural heritage. Portugal should definitely assume the competitive advantages of its geostrategic position, its technological skills and its maritime tradition, minimizing administrative or fiscal barriers that prove to be harmful to it, and exercising the authority of the state at sea. The standards we set in the sustainable management of our sea will be a decisive contribution to the sustainability of the planet, in a future that we wish bluer for generations to come".

[22] See The European Centre of Excellence for Countering Hybrid Threats, *"Handbook on Maritime Hybrid Threats – 10 Scenarios and Legal Scans"*, November 2019.

and, more concretely, one that essentially contributes to the achievement of political-strategic objectives.[23]

Accordingly, "safety at sea" - as defined above - only partially has something in common with "national security" because it continues to have a transnational aspect, regardless of the state concerned. However, it will be, essentially, the "security" requirements that can model "safety at sea" through "national security" instead of the "safety" matrices that tend to be perennial and technical, aiming at improving navigability conditions of the medium used, without prejudice to considering natural phenomena.[24]

In fact and in the vast majority of cases, only "security" is of interest to the political-strategic framework, involving other international States or actors, which means that it falls within the scope of the sovereignty of States and their corresponding unilateral enforcement mechanisms".

In contrast, regarding "safety", maritime safety rules derive from international conventions and coercibility results from international law (or international agreements such as the MoU in the context of Port State Control).[25]

Another component that may influence "safety at sea" concerns the definition of sector strategies. Today, it is essential to articulate the issues of the "sea" with those of the "ports", with "transportation" and "logistics", whether in a more vertical and/or transversal view of sea matters.[26]

On the other hand, threats and risks exist in military or civil documents - because they result from the analysis of civil components (namely, of an economic, cultural, scientific, technological, or environmental nature) or in strictly military - but they have repercussions in terms of strategic policy of any maritime country and thus, ultimately, in national security.

[23] See Fernandes, António Horta.*, "Conceito Estratégico de Defesa Nacional (CEDN) ou Conceito Estratégico de Segurança Nacional (CESN)? Um falso dilema",* Observatório Político, wp #43, April 2014, in *http://www.observatoriopolitico.pt/wp-content/uploads/2014/04/WP_43_AHF.pdfla,* p. 4 and following, and Branco, Carlos, *"Porquê uma Estratégia de Segurança Nacional?",* Opinião, *Expresso*, 2018-05-11. For all, Cajarabille, Victor Lopo, *"Enquadramento Estratégico",* in Cajarabille, Victor Lopo et all, *"A Segurança no Mar – uma visão holística",* Mare Liberum, Aveiro, 2012, pp. 21-35. See Escorrega, Luis Falcão, *"A Segurança e os "Novos" Riscos e Ameaças: Perspetivas Várias"*, Revista Militar, no. 2491, August/September 2009 (https://www.revistamilitar.pt/). This author is of great use to us because he admits that the modern concept of "threats" encompasses traditional "risks" and "threats" (p. 14). See also Duarte, António Rebelo, *"Políticas e Estratégias Marítimas da Europa e de Portugal"*, Cadernos Navais, no. 48, April-June 2018, Centro de Estudos Estratégicos da Marinha, in www.marinha.pt. This author reinforces the development of "maritime security" under the terms of the Maritime Security Strategy, approved by the European Council on 24 June 2014, and its framework within the framework of the Common Security and Defence Policy (ESDP), with a description of the risks and threats to European maritime security, reinforcing the importance of "security" in that Strategy.

[24] See note 18 and the reference text.

[25] In Spain, the Maritime Security Committee reports to the National Security Council. In turn, in the United Kingdom, the "Ministerial Working Group on Maritime Security" reports to the "National Security Council". See *"Estrategia de Seguridad Marítima Nacional",* Gobierno de España, 2013 and *"The UK National Strategy for Maritime Security",* MOD UK, May 2014.

[26] The political and strategic options in terms of "Defence and Security" must be followed permanently when addressing sea matters, all the more so since the protection, inspection, prospection and sustainable exploitation of its resources require suitable means for this purpose, listing them permanently and avoiding its predation.

Having in mind the concepts of "safety" and "security" ("protection"), it is important to stress that "safety at sea" will always depend on the (global) strategy of the State[27], although its holistic perspective is based on the deepening of the technological conditions of activities at "sea" - in particular, in the context of maritime transport and ports - and the degree of demand in compliance with good practices and the consequent accountability of crews, companies and port operators.[28]

[27] The introduction of the word "security" in conceptual documents emerges when the "strategy" based on a certain "concept" is developed. At national level, the "National Defence Strategic Concept" and the "National Defence and Security Strategy" are the main references.

[28] In traditional terms, "safety" is related to the minimization of "risks" (from navigation) whereas "security" aims to combat intentional "threats" - although not exclusively - starting with a simple oil spill. In other words, "security" has as its essential core the threat and the intention to cause damage and, for this very reason, it is necessary to state its human origin ("threat actors"). Rather, "safety" focuses on the "risk" of maritime activities, that is, natural or unintended events that have serious consequences and are likely to materialize (i.e., traditionally, unexpected breakdowns, natural elements, etc.).

Our challenge is to prove that, nowadays, "risk" tends to be reduced to the so-called "natural" situations, since the conduct of a ship's crew that was exposed to a "danger" or "serious" damage can, in most cases, must be assumed as a "wilful" (i.e., beyond "negligent") performance for violation - although not intentionally - of maritime safety rules. If so, it is an "upgrade" of these conducts - considered, until today, "negligent" – being assumed as "threats" and, therefore, also, a matter of "security".

Also in this field, the prevention and combat (or minimization) of damages resulting from occurrences of "security" and "safety", although with different conceptual origins, tend to increasingly overlap and articulate, in the actions, which is evident when moving towards global connections such as those that result from the fact that we live in a digitally interconnected world, whether physically or virtually, and thus permanently retaining its cybersecurity. On the website of the North American company CISA (Cybersecurity and Infrastructure Security Agency), created in 2018, it appears that one starts from the concept of "safety" to go to the one of "security" in a very simple way, stating that: "Being online exposes us to cyber criminals and others who commit identity theft, fraud, and harassment. Every time we connect to the Internet-at home, at school, at work, or on our mobile devices, we make decisions that affect our cybersecurity. Emerging cyber threats require engagement from the entire American community to create a safer cyber environment-from government and law enforcement to the private sector and, most importantly, members of the public*"*. However, it is important to reiterate that it was the cyber threat and, consequently, cybersecurity, that came to leverage the thesis of the concentric relationship between "safety" and "security" and that a recent presentation on the repositioning of cyber threats in Operational Technologies (OT) systems - (Lisbon, at the PwC, on 5 February 2020). Its author (Rafael Maman), an Israeli expert in the area of cybersecurity who addressed the matter in a personal capacity, mentioned the following: "Corresponding to a shift in the cyber risk equation: traditional IT risks – data privacy, IP theft, etc. – are augmented by higher-order risks – to unman life, disruption of critical operations, environmental disasters, etc.(it should have as a consequence that) governments and industrial enterprises recognise the importance of OT Security for Critical Infrastructure protection and the risks involved, and initiate proactive action*"*.

With this qualitative change in the cyber risk equation, it is increasingly important to identify the fundamental differences between cybersecurity in IT and OT, in all its dimensions - including the legal one - precisely because it is in the OT domain that the interdependencies between "safety" and "security" are more relevant, given that the OT links the cyber world to the physical one. As a direct consequence, the permanent presence of the risk of cyber-attacks to critical infrastructures and essential services (which include maritime transport and ports) implies that "security" must always be considered. In our case, the creation of conditions for safe navigation, in the present times, must always take cyberspace into account and, therefore, the representative figure that is proposed, consisting of two concentric circles in which the central one corresponds to "safety". In this light, Rafael Maman goes even further when considering that the micro trends of cyber threats present the following evolution: "From "military-grade cyberweapons" to "industrial-grade ransomware". What used to be considered cyber warfare weapons used by the armed forces can now be used to disrupt critical industries and essential services by any actor technologically able to do it. In Maman's "The Reshaping Cyber Threat Landscape of Operational Technology", presentation at the "Conference organized by the PwC "Cybersecurity - The Challenges of Operational Technology (OT)", Lisbon, 5 February 2020.

On the other hand, since the beginning of the century, the vast majority of incidents of appreciable size in sensitive industries have deliberate attacks (cyber and other), collateral damage from attacks or the poor functioning of systems as associated causes, not being possible, in most cases, to isolate sources according to the traditional "safety/security" bipartition or, if possible, it will lose all interest due to the need for an

"Safety at sea", when encompassing those two concepts, unfolds into two types of dangers: the "threats" and the "risks" that involve the use of the sea, either in ships or in ports.

"Threats" are essentially of two kinds: generic offenses at sea and specific offenses that influence freedom of navigation. The first includes, in particular, trafficking in narcotic drugs and psychotropic substances, general and arms smuggling, the proliferation of weapons of mass destruction, the illegal exploitation of marine resources, the platform or underwater cultural heritage, attacks (including pollution) and illegal immigration. The second includes terrorism, piracy, cyber-attacks on information systems and other criminal activities classified as such by international law.

In turn, "risks"[29] tend to be accidental or natural and identify mostly (but not exclusively) with "maritime transport security" and "port security". The potential associated damage (or the condition of creating a "hazard") can affect ships and vessels, people on board, platforms or infrastructure at sea (and, equally, aircraft and submarines) and the environment in particular through pollution accidents.

This tendency to associate "safety" (in the strict sense) with "risks" and "protection" with "threats" has the great advantage of being able to learn from areas that, until recently, evolved autonomously and that the 9/11 forced to be closely associated. This resulted from the need to adopt measures applicable to ships and port facilities in the scope of "protection" and to identify security threats and take of accident prevention measures, which started to take place, cumulatively and in coordinated from, in accordance with the ISPS Code[30].

Another circumstance that occurs with the deepening and development of maritime safety rules - translated, in essence, into the relevant IMO conventions - concerns the progressive exhaustion of exemption clauses and limitation of liability in maritime

integrated response. See https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents.

For this reason, the intention is not only to prove that the crew conduct that violates the rules of maritime safety and causes a "danger" or "damage" qualified legally as "serious" falls within the scope of "wilful misconduct", and within the representation by two concentric circles.

The traditional division between neutralizing threat agents ("security") and helping to contain negative consequences ("safety"), in our opinion, may contribute to a common and consolidated plan that will form part of the maritime safety rules aboard, no matter their different origin or the measures to limit damage. The European Security Strategy and the Report on the Implementation of the European Security Strategy also highlight a set of "threats" with implications for the use of the sea, including illegal activities, organized crime, piracy, terrorism, proliferation weapons of mass destruction, regional conflicts, fragile States, maritime pollution, energy security and climate change. This means that this focus is essentially on "security". See http://www.consilium.europa.eu/uedocs (search for the respective titles). On the contrary, the EMSA (European Maritime Safety Agency) performs activities within the scope of "safety" and it is for this reason that it is nevertheless invoked in a common and broad perspective of "safety" (i.e., "safety" plus "security").

[29] A "risk" is the product of the probability of the occurrence of a threat (or damage) by the severity (or intensity) of its effects. Traditionally associated with "safety", the ship's rules compliance hamper applying a waiver clause to any crew's conduct that violates the rules of maritime safety with serious consequences. The origin of these concepts is rooted in international law and, more specifically, in conflict resolution theory. In a succinct way and in this context, "threat" corresponds to a circumstance or event that endangers the pursuit of political and strategic objectives and "risk" is perceived as the degree of exposure to the threat in question.

[30] The acronym ISPS designates the "International Ships and Port Facilities Security Code" that constitutes chapter XI-2 of the SOLAS Convention since 2002.

transport contracts (and conventions) that allow, for example, a carrier to discharge its liability whenever proceeding without a wilful misconduct. As a paradigmatic example, there is the "nautical fault" in international conventions on maritime transport that exonerates the carrier for damage to the cargo (at least, since the 1920s).

It means that the progressive technological requirements and good conduct for safe navigation (i.e., the rules on "maritime safety") make the circumstances initially considered to be "negligent", much more restricted in the scope of civil liability (contractual and in tort), including those present in oil spills[31].

Accordingly, compliance with maritime safety standards, while minimizing "risks" (and errors), reinforces fighting "threats" and, at the same time, limits enforcing the exemption and liability limitation clauses present, for example and among others, in the conventions on pollution resulting from oil spills and in those concerning the maritime transport of goods[32].

It is understood, therefore, that the broad notion of "safety at sea" (or "maritime safety" in the wide sense which is, in fact, one of the most common expression nowadays) must rule the material aspects of (maritime) safety (in strict sense) and (maritime) security and, in terms of its spatial range, focusing on ships and ports[33]. Particularly, in terms of the object, "safety at sea" – in both aspects - covers maritime transport - in which the focus is the "ship" and her movement - and ports - which essentially rules the safety in

[31] This matter was defined as falling within the scope of "security", even in its origin, since, in the assessment made, in most cases with serious consequences, it results from a "wilful misconduct" of the crew.

[32] The "nautical fault" as an exemption (or waiver) clause is provided for in clause a) of paragraph 2 of article 4 of the International Convention for the Unification of Certain Rules of Law relating to Bills of Lading Knowledge, signed in Brussels on 25 August 1924 - known as "The Hague Rules". It specifically refers that the clause only applies to "Acts, neglect or default of the master, mariner, pilot or servants of the carrier in the navigation or in the management". Thus, if the "nautical fault" consists of a violation of the essential rules of maritime safety (in a broad sense), it can hardly justify the exoneration of the carrier/shipowner for damage to the cargo.
It should be noted that according to tort's doctrine and in accordance with the current conventions - particularly under the 1969 Liability Convention for Damage Due to Oil Pollution (Civil Liability Convention 1969 or CLC/69) and its 1992 amendment (CLC/92) - the owner of the ship is responsible for a navigation error that led to the vessel being stranded and the subsequent oil spill (case of the M/V "Exxon Valdez" with the spill of about 38,000 tons of crude on the Alaskan coasts). In fact, Article V/2 of the CLC/92 establishes that the owner can lose the ability to limit his liability as long as the damage due to pollution results from an action or omission attributed to him "committed with the intention of causing such damage or recklessly and in the knowledge that such damage could occur". This formula is very close to that used in paragraph 5 (e) of Article IV of the Visby Protocol of 1968 ("Visby Rules") to the Brussels Convention of 1924 referred to, which removes the limitation of liability if the action or omission had the intention of causing damage or was done recklessly and with the knowledge that damage would probably take place. It is a form not covered by "negligence act" but by a "wilful misconduct". See Coelho, Carlos, "*Poluição Marítima por Hidrocarbonetos e Responsabilidade Civil*", Almedina, Coimbra, 2007, p. 86 and following.
In conclusion: it is understood that wilful misconduct in the violation of the rules of maritime safety should remove the benefit of the exemption clause "nautical fault" by the carrier/shipowner.
In our work *"O Contrato de Volume e o Transporte Marítimo de Mercadorias – Dos granéis aos contentores, do "tramping" às linhas regulares",* Coleção Teses, Almedina, Coimbra, 2018, p. 73 and following, note 80, we have opened the discussion regarding this position although, at that time, without the generalization that we have made here.

[33] In terms of "value chain", the possibility of also covering agents and operators with responsibility in the logistics area is not ruled out as their performance is directly related to the information and communication systems, such as the Portuguese ports that use the modern "Port Single Window" (a "one stop shop" asset) or its upgrade, the new "Logistics Single Window" that now covers dry ports and land and logistic operators as well as freight forwarders.

areas under port jurisdiction, covering the various terminals, the adjacent land area and the contiguous wet area.

The "safety of maritime transport" (or "maritime safety in the strict sense") involves the set of measures in force for a safe navigation by ships, i.e., the conditions on board (qualification of the crew, stowage and cargo handling and, in general, the navigability conditions of the ship and its equipment), the navigation aid systems or the safe navigation in coastal waters, including, the ports.

On the other hand, "maritime transport protection" and "port protection" depending on the object - involve all physical safety[34] and other measures applicable in the area under port jurisdiction, regarding the ship's crew and passengers and other employees who operate in the ports, as well as the ships as carriers. Those measures are intended to secure normal trade activity according to the applicable technical rules[35].

III. The modern perspective of defence against cyber-attacks in the maritime sector

Therefore, it is expected that the contents of an autonomous "Maritime Safety Law"[36] should take into account both vectors of "safety" and "security", for several reasons: first, "safety" is the oldest[37], the most stable and the one that is dealt with in most IMO conventions; then, because the interpenetration between the two concepts is increasing; thirdly, because there are translations that no longer go back (the case of "cybersecurity"); and finally, because, nowadays, the two vectors tend to present themselves as two concentric circles - the "safety" (more interior) and the "security" that surrounds it.

[34] From this point of view, there is also the need to certify personnel who interact with IT systems according to the type of ship, ports of origin, type of goods, i.e., according to the standard of risk assumed for the ship, as it is done today to comply with maritime safety conditions in which, for example, the conditions for the replenishment of bunkers (fuel for ships) by barge in ports are evaluated.

[35] The Diplomatic Conference of the International Maritime Organization (IMO), meeting on 12 December 2002, amended the SOLAS Convention ("Safety of Life at Sea"), and adopted the International Ship and Port Facility Security Code (known as "ISPS Code"), which came into force on 1 July 2004. This new Code is an expression of the value of "protecting" maritime transport, terminals, and ports. It has been clarified that the SOLAS Convention includes several specific codes aiming at standardizing safety management on board (the case of the ISM Code - International Management Code for the Safe Operation of Ships and for Pollution Prevention, from 1992) or aimed at the rules for the investigation of maritime accidents or incidents (the CIA or Accident Investigation Code) that aggregates a set of IMO resolutions, with special reference to Resolution A.849 820) of November 1990 - which establishes the rules for the investigation of human factors in accidents and Resolution MSC.255 (84), of 16 May 2008, which contemplates the rules and recommendations to be adopted in investigations of maritime accidents or incidents.

[36] The autonomy of Security Law as a branch of law was defended by Gouveia, Jorge Bacelar in the work "*Direito da Segurança Cidadania, Soberania e Cosmopolitismo*", Almedina, Coimbra, 2018. In this work, in particular in the second part, which refers to the "explanation of Security Law as a new legal sector and in the context of the respective sources" (p. 17), the author takes a path which, to some extent, may make it difficult to "search some more complex points in depth" (p. 15). However, it was its scope and the innovative approach that, in our opinion, led to the emergence, among other special areas, of Maritime Security Law as a branch of Security Law and to cut off the old ties with the traditional law of the sea and maritime law.

[37] It is important to clarify that if it starts from an imminent commercial perspective, i.e., to establish the activity of maritime transport, it is necessary, in the first place, to use technologically safe assets. Only after that, it the importance of threat control can be assessed. Of course, in certain circumstances, it can be reversible, securing the aim of the minimum capacity for employing the assets.

In fact, the latter can strengthen (or weaken) the one at the centre[38], in a constant dialectic and interaction.

This proposed structure is in line with an increasingly present finding: "security" incidents can have serious consequences in terms of "safety", which means that it is necessary to consider security procedures as essential to prevent those incidents from having a serious impact on the "safety" framework, even including them in the mandatory international maritime safety management codes.

However, the strengthening of the importance of "security" did not affect, in conventional terms, an upgrade and revision of concepts, and, after all, such position was not expected. In fact, the SOLAS convention has begun its long journey in 1914, with an essential aspect of maritime safety together with the safety of human life at sea (which, incidentally, comes from its acronym SOLAS - Safety of Life at Sea), having embraced new subjects (the ISPS Code, for example), and the autonomy of others (for example, the case of the COLREG convention, which, in 1972, approved the Regulation to Prevent Collisions at Sea).

Thus, Maritime Safety Law, within the scope of International Law, has its own essential sources on the specific IMO conventions that are based on the traditional classification of "safety", gradually extending its regulation to "security" – as it happens with the ISPS Code annexed to the SOLAS Convention or, autonomously, with the SUA Convention[39].

This instrumental expansion of the traditional safety matter to maritime security (or "protection") will give response to the new risks and threats at sea and ports, which, however, still face the regulation difficulty in clear areas of the exercise of the sovereignty of States that traditionally would conflict with international law.

It is understood, however, that the new security environment requires a progressive capacity for harmonization and cooperation, including the employment of assets. Given the global dimension of risks and threats, this approach is of utmost importance. This is what happens currently with "maritime cybersecurity"[40], which is increasingly more important for ports, maritime transportation and assets.

[38] This means that "security" ("cyber") incidents can give rise to "safety" incidents, in a continuous interaction that should not be seen in an up and down approach. Thus, we are getting closer to the evolution of NATO's traditional "naval defence" mission towards a broad notion of "maritime security", whereby it is intended to "prevent the use of the sea for illegal activities and ensure freedom of navigation" cf. Pereira, Luis Sousa, *"A NATO e a Segurança no Mar"* in Cajarabille, Victor Lopo et all, *"A Segurança no Mar -uma Visão Holística", Mare Liberum*, Aveiro, 2012, p. 132. Our concept is not limited to the perspective of "naval defence" and requires a very significant "safety" component in the strict sense. However, for example, the Portuguese translation of NATO documents, such as the "Maritime Security Operations Concept" makes - once again - the term "security" correspond to the word "segurança" (and not "proteção"). In a recent paper (dated 30 August 2019), entitled *"Polemologia da Segurança Marítima – Golfo da Guiné como estudo de caso"* ("Maritime Security Polemology - Gulf of Guinea as a case study") (unpublished), written by Commander Luis Cuco de Jesus, within the scope of the Doctoral Degree in Law and Security of the Nova School of Law (Lisbon), this author uses the words "maritime safety" in order to elect legal mechanisms to suppress new threats at sea, which means that the proposed framework occurs, essentially and strictly, within the scope of "security".

[39] *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation,* 1988.

[40] Which, in fact, should be designated in Portuguese as *"ciberproteção marítima"* because it is a matter of "security". See also the article by Marques, António Gameiro, *"Cibersegurança no Setor Marítimo"*, in *Revista de Marinha*, no. 1004, Jul-Ago 2018, pp. 30-32. The author approaches this matter in a pioneering way, examining the developments in the European Union and the recently approved laws regarding cyberspace.

Accordingly, the interconnection between a security incident and a safety incident, including the impact of the former on the latter, is, in this context, a real probability, since it is not difficult to predict that spoofing in the ship's geographical position leads to deviation and the consequent stranding or collision.

In 2002, the ISPS Code recognized the role of port structures (terminals and ports) in the context of maritime protection and established mandatory requirements and recommendations applicable to ships and those facilities. However, the requirements may also cover cybersecurity measures relating to access control and certification of authorizations[41].

In fact, the ISPS Code requires terminals drawing up the so-called "Port Facility Security Assessment" (PFSA), which identifies structures and equipment, possible threats and countermeasures and the "Port Facility Security Plan" (PFSP), which identifies the procedures, measures and actions to be carried out at different alert levels. The PFSA must address the following aspects: physical safety, structural integrity, personal protection systems, procedural policies, radio and telecommunications systems - including computer systems and computer networks - and relevant transport infrastructure. The PFSP specifies conditions for access to infrastructure, restricted areas, cargo handling, delivery of supplies to ships, and monitoring of infrastructure protection conditions.

Also the SOLAS and FAL Conventions (Facilitation on International Maritime Traffic) define nine standard forms to be used in the exchange of information in the maritime ecosystem, especially between ports (or terminals) and third parties that have been mandatorily processed by electronic means since 9 April 2019, especially through the use of "single window systems" (or "one stop shop"). It is the standardization of information exchange that has a strong impact on IT systems and poses new challenges.

Regarding cybersecurity for the maritime "ecosystem", special for ships, it was not until 2017 that international recommendations begun to be more abundant.

The *IMO Facilitation Committee* (FAL) and the *IMO Maritime Security Committee* (MSC) wrote the action lines in risk management of maritime cybersecurity in the document MSC-FAL 1/ Circ.3[42]. Both structures recognize the urgent need to raise awareness of the threats and vulnerabilities of marine cyberspace and to make high-level recommendations for the management of cyberspace risks in relation to current and

See also, by the same author, "A Segurança do Ciberespaço em Portugal e no Setor Marítimo", *Cadernos Na*vais, no. 52, April-June 2019, Centro de Estudos Estratégicos da Marinha, *in www.marinha.pt.* Regarding the concepts of cybersecurity and information security, see Santos, Lino, *"Cibersegurança"* e *"Segurança da informação" in* Gouveia, Jorge Bacelar Gouveia and Santos, Sofia (coord.), *op. cit.,* pp. 63-67 and 422-425. This author states that "cybersecurity can be seen from two perspectives, regardless of whether the object of cybersecurity is the State, organizations or individuals: the security of cyberspace (in the physical sense of it as an autonomous entity) and the security of the "cyber" component of any system (cyberspace security of that system) "(p. 63). For its part and according to the same author, information security is indispensable to "guarantee confidentiality, integrity and availability of information at all times" (p. 422).

[41] See, more recently, the document ENISA *("European Union Agency for Cybersecurity")*, *Port Cybersecurity - Good practices for cybersecurity in the maritime sector,* Nov. 2019, ISBN 978-92-9204-314-8, DOI 10.2824/328515.

[42] See *"Guidelines on Maritime Cyber Risk Management"* (MSC-FAL.1/Circ.3) in http://www.imo.org/en/OurWork/*Security*/Guide_to_Maritime_*Security*/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf.

emerging threats and vulnerabilities, including key areas that are considered essential to support cyberspace management (identify, protect, detect, respond and recover).

These action lines constituted the basis for distinguishing between IT systems (information technologies, i.e., use of data as information) and OT (operational technology, i.e., IT systems are increasingly linked to the OT of companies, which requires a new management perspective in the use of data to control or monitor physical processes, in a constant and bidirectional cyber-physical interaction). They reveal that all organizations in the shipping industry are different and that the role of governments and Flag States in their regulation is essential. These should also be guided updated recommendations of the most relevant international instruments and good practices, aiming at the improvement of the protective measures.

It was up to each State to take the measures considered to be most appropriate, in an environment far from the progressive uniformity required by the global connection of the systems.

At European Union level[43], the important role of its specialized agency (ENISA - "European Union Agency for Network and Information Security") on the maritime sector has begun in 2011 with the publication of the report on maritime cybersecurity[44].

This document characterized the systems that the maritime community uses. In general, they are highly complex, with different technologies, numerous manufacturers and a huge dispersion of nationalities. It turns out that issues associated with security (or protection in order to prevent intrusion and disruption) are, generally, considered negligible, increasing the risk of cyber-attacks, amplified by easy connections to the Internet without adopting good practices.

But even more serious was the lack of capacity to deal with both incidents and even cyber-attacks, denoting a complete lack of coordination among the various actors in the maritime-port sector.

In general terms, future chapters of the SOLAS Convention regarding "security" may include actions to respond to cyber-attacks, particularly when part of the general measures for the protection of ships, ports and personnel.

In this regard, the following Community legislation deserves special mention:

- Regulation (EC) No. 725/2004 regarding the enforcement of the ISPS Code for ships and port structures;
- Directive No. 2005/65/EC regarding port security;
- Regulation (EC) No. 336/2006 on the enforcement of the ISM Code *(International*

[43] Page 3 of the European Union's Maritime Safety Strategy of 24 July 2014 reads: "Maritime security is understood as a state of affairs of the global maritime domain, in which international law and national law are enforced, freedom of navigation is guaranteed and citizens, infrastructure, transport, the environment and marine resources are protected*"*. This paragraph also contains the idea of the 2 concentric circles that correspond to "safety" and "security", that is, the guarantee of freedom of navigation in safe conditions for citizens, for infrastructures, for transport, the environment and marine resources. See COUNCIL OF THE EUROPEAN UNION, Brussels, *European Union Maritime Security Strategy*, 24-06-2014, doc. 11205/14.

[44] *https://www.enisa.europa.eu/news/enisa-news/first-eu-report-on-maritime-cyber-security.*

Safety Management Code) for the maritime sector – that excludes, however, the ports included in the above directive; and

- Directive 2010/65/EU, which stipulates the acceptance by Member States of standard forms ("FAL forms") to facilitate traffic. This Directive also introduces "SafeSeaNet" systems at national and European Union level in the legal system, promoting secure data traffic between the maritime administrations of each state and other authorities.

Briefly, Regulation (EC) No. 725/2004 and Directive No. 2005/65/EC constitute the legal reference framework that supports the assessment and plans for the protection of ports and port infrastructure, as well as ownership and maritime carriers' companies.

Meanwhile, in 2014, the document that approved the European Maritime Security Strategy (EUMSS), revised in 2018[45], was defined as an instrument to identify, prevent and respond to any challenge that may affect the protection of Europeans, activities and means in the maritime ecosystem including ports.

The EUMSS identifies threats and risks that are embodied in "terrorism and other intentional and unlawful acts at sea and in ports against ships, goods, crews and passengers, ports and port infrastructure and critical maritime and energy infrastructures, including cyber-attacks". The 2018 version of the Strategy essentially focused on the reporting procedure with a view to improving the alert and monitoring subsequent actions.

Only after Directive No. 2016/1148 on Security of Network and Information Systems (NIS)[46] came into force, the European Union started to have legislation to harmonize

[45] See the 2014 original version in *"The European Maritime Security Strategy"* in *https://ec.europa.eu/maritimeaffairs/policy/maritime-security_en.* It is clear that strategy documents on "safety" and/or "security" issues are almost invariably translated as "safety", an argument also in favour of proposing the "new" Maritime Safety Law as covering both aspects that are increasingly interrelated and whose limits are increasingly fluid. And its 2018 version in *https://www.consilium.europa.eu/en/press/press-releases/2018/06/26/maritime-security-eu-revises-its-action-plan/.* In 2016, Regulation (EU) 2016/679 ("General Data Protection Regulation"), which was intended to protect the personal data of natural persons and their communication, also naturally covered the maritime sector, but without any specialization.

[46] This Directive was transposed into Portuguese legislation by Law No. 46/2018, of 13 August, which establishes the legal regime for cyberspace security. Meantime, last September, the European Commission launched a public consultation as part of the review process of the NIS Directive with the aim of strengthening the resilience of networks and systems against cybersecurity risks. In this context, the Directive identifies "operators of essential services", including seaports. One of the problems identified by the Commission was the lack of harmonization on the part of the Member States in identifying those operators, which was also reflected in the selected seaports (for example, whether or not smaller ports should be excluded from the enforcement of the Directive). For this reason, it is also intended to revisit the terms foreseen for "sea ports" in the definition established therein that follows*:"Managing bodies of ports as defined in point (1) of Article 3 of Directive 2005/65/EC, including their port facilities as defined in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports".* One of the core issues to be considered concerns the obligation that the Directive imposes on the notification of cybersecurity incidents to the competent authorities. In our opinion, all operators that are part of a "network or system of essential services", should be covered by the Directive, regardless whether the seaport (or other network member) is large or small. Thus, the obligations carried out by an "essential services operator" should be mandatory for all, regardless of their classification as "operators".

national cybersecurity capacities, border collaboration and supervision of critical sectors within the Union.

This is the first European Union legislation on cyberspace security, aimed at increasing cooperation and creating a culture of security in sectors essential to society that rely heavily on IT.

Paragraphs 10 and 11 of the Directive are specific to the maritime sector:

> "*10.* In the maritime and inland waterway transport sector, safety requirements for companies, ships, port facilities, ports and maritime traffic services under Union legal acts cover all operations, including radio and telecommunication systems and information systems and networks. Part of the mandatory procedures to be followed includes notification of all incidents and, as such, should be considered as "*lex specialis*", insofar as these requirements are at least equivalent to the corresponding provisions of this Directive*".*

> *"11. When identifying operators in the maritime and inland waterway transport sector, Member States should take into account the international codes and guidelines - current and future – written by the International Maritime Organization in order to allow different maritime operators to follow a coherent approach".*

According to Article 4, paragraph 4 of the Directive, an "operator of essential services" is a public or private entity belonging to one of the types referred to in Annex II and which fulfills the criteria set out in Article 5, paragraph 2 (that is, an entity provides an essential service for the maintenance of crucial society and/or economic activities, and the provision of that service depends on information networks and systems; and an incident can have major disruptive effects on the provision of that service).

However, as regards the maritime and inland waterway transport ecosystem, the operators listed in Annex II are as follows:

- Inland waterway, maritime and coastal transport companies for passengers and goods, as defined, for maritime transport, in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council, not including ships operated by these companies;
- Port management entities within the meaning of Article 3, paragraph 1 of Directive No 2005/65/EC of the European Parliament and of the Council, including their port facilities within the meaning of Article 2, paragraph 11 of Regulation (EC) No 725/2004, and the entities that manage the works and equipment existing inside the ports;
- Maritime traffic service operators within the meaning of Article 3, clause (o) of Directive 2002/59/EC of the European Parliament and of the Council.

Finally, in 2019, the "European Cybersecurity Act"[47] strengthened ENISA's position vis-à-vis Member States and defined the framework for cybersecurity certification for ICT products, services and processes, demanding compliance with certain requirements.

In addition, several Member States have strengthened the enforcement of international and EU regulations and policies on cybersecurity, developing their own initiatives to improve cyberspace risk management through national legislation[48].

IV. Conclusions

Since old times, the sea has been a path for trade and, therefore, for globalization. Nowadays, this has led to the emergence of several risks and threats that require more demanding conditions for ICT products and associated services.

Cyber-attacks in the maritime-port sector have reinforced the need to approach the new maritime safety in a holistic way, integrating the two vectors ("safety" and "security"), which rely on the national strategy conducted by each State.

Thus, we can say that "safety at sea" is balanced between two concentric circles: "safety", from a technical nature, and "security", which reinforces the protection against wilful misconduct, strengthening resilience against those acts and detecting the systems' vulnerability, evaluating, preventing and deterring the threats.

The new stage attained by the European Union on cybersecurity was achieved by Directive 2016/1148 on the Security of Network and Information Systems (NIS), a new framework able to harmonize, among Member States, their national cybersecurity capacities, border collaboration and the supervision of critical and essential sectors in the Union.

A "secure navigation in cyberspace" requires, after all, facing and defeating new "obstacles" - accidental or deliberate – where the "unruled" globalization is the true enemy. It is the new Cape of Good Hope, in South Africa, that Portuguese navigator Bartolomeu Dias has "defeated" and overcome in the 15th century.

As the Cape was turned safely then, cyberspace should also be safe, with tight regulations and new instruments, as Pedro Nunes did with the "grown latitudes" chart[49], or with

[47] *https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.*

[48] Law "CIIP" in France - *https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/.*
UK specific port law - *https://www.gov.uk/government/publications/ports-and-port-systems-cyber-security-code-of-practice;*
"IT-Grundschutz" Law in Germany: *https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html;*
At national level: Law no. 46/2018 of 13 August transposed Directive (EU) No. 2016/1148 and the Resolution of the Council of Ministers No. 92/2019 of 5 June into national law and established the National Cyberspace Security Strategy.
It should be noted that cybersecurity was a relevant topic on the agenda of the NATO Summit in London, in December 2019.

[49] Even, at this stage, in small-scale charts, leaving for Gerardo Mercator, later, the glory of its generalization (Mercator chart). Pedro Nunes, as the first major cosmographer of the Portuguese Kingdom, appointed in 1547, born in Alcácer do Sal, nearby Sado river and Maths Doctor in Coimbra University, played a crucial role in the development of the study of the mathematical problems of nautical cartography that became essential in the methods and equipment used in oceanic navigation by the Portuguese. He was the first to

Bartolomeu Dias' courage and expertise, looking for new knowledge and navigation techniques, a step further to beginning, then, "Globalization"!

References

Branco, Carlos (2018). *"Porquê uma Estratégia de Segurança Nacional?",* Opinião, *Expresso* newspaper, 11 May.

Cajarabille, Victor Lopo (coord.) (2014). *"A Segurança nos Portos – uma visão integrada",* Mare Liberum, Aveiro.

Cajarabille, Victor Lopo et all (2012). *"A Segurança no Mar – uma visão holística",* Mare Liberum, Aveiro.

Cajarabille, Victor Lopo (2012). *"Enquadramento Estratégico",* in Cajarabille, Victor Lopo et all, "A Segurança no Mar – uma visão holística", Mare Liberum, Aveiro, pp. 21-35.

CISA, *"The Cybersecurity and Infrastructure Security Agency",* in www.cisa.gov.

Coelho, Carlos (2007). *"Poluição Marítima por Hidrocarbonetos e Responsabilidade Civil",* Almedina, Coimbra.

COUNCIL OF THE EUROPEAN UNION, *"European Union Maritime Security Strategy",* 24-06-2014, doc. 11205/14.

Couto, Abel Cabral (1988). *"Elementos de Estratégia"*, Volume I, IAEM, Lisbon.

CSIS, *"Center for Strategic & International Studies",* in https://www.csis.org.

Direção-Geral da Política do Mar (DGPM), ENM 2021-2030, *"Estratégia Nacional para o Mar",* interim document for public consultation, in https://www.dgpm.mm.gov.pt/enm.

Duarte, António Rebelo (2018). *"Políticas e Estratégias Marítimas da Europa e de Portugal",* Cadernos Navais, no. 48, April-June, Centro de Estudos Estratégicos da Marinha, in www.marinha.pt.

ENISA ("European Union Agency for Cybersecurity") (2019).*" Port Cybersecurity - Good practices for cybersecurity in the maritime sector",* Nov, ISBN 978-92-9204-314-8, DOI 10.2824/328515.

ENISA, *"The European Maritime Security Strategy"* (2014), in https://ec.europa.eu/maritimeaffairs/policy/maritime-security_en.

ENISA, *"The European Maritime Security Strategy"* (rev. 2018) in https://www.consilium.europa.eu/en/press/press-releases/2018/06/26/maritime-security-eu-revises-its-action-plan/.

conceptualize the difference between a "rhumb line" (loxodromic) and "orthodromic line", i.e., the constant heading (course) line was not the shortest distance between two points. In his *"Tratado em Defesa da Carta de Marear",* he argued that a nautical chart should have parallel circumferences and meridians "drawn as straight lines". But we could mention others and, more recently, Admiral Gago Coutinho and his amazing preparation - mathematical and cartographic - for the trip of the first aerial crossing of the South Atlantic, between Lisbon and Rio de Janeiro, in 1922.

ENISA, Report, in https://www.enisa.europa.eu/news/enisa-news/first-eu-report-on-maritime-cyber-security.

Escorrega, Luis Carlos Falcão (2009). *"A Segurança e os "Novos" Riscos e Ameaças: Perspetivas Várias",* Revista Militar, no. 2491, August/September (https://www.revistamilitar.pt/).

Faria, Duarte Lynce de (2018). *"O Contrato de Volume e o Transporte Marítimo de Mercadorias – Dos granéis aos contentores, do "tramping" às linhas regulares",* Coleção Teses, Almedina, Coimbra.

Faria, Duarte Lynce de (2015). *"Segurança no mar"* in Gouveia, Jorge Bacelar e Santos, Sofia (coord.), *"Enciclopédia de Direito e Segurança"*, Almedina, Coimbra, pp. 433-439.

Fernandes, António Horta (2014). *"Conceito Estratégico de Defesa Nacional (CEDN) ou Conceito Estratégico de Segurança Nacional (CESN)? Um falso dilema",* Observatório Político, wp #43, April, in http://www.observatoriopolitico.pt/wp-content/uploads/2014/04/WP_43_AHF.pdfla, pp. 4 and following.

Gallagher, John (2019), in "Freight Wave" (Revue), 29th of March.

Garcia, Francisco Proença (2015). "Defesa Nacional" in Gouveia, Jorge Bacelar e Santos, Sofia (coord.*), "Enciclopédia de Direito e Segurança",* Almedina, Coimbra, pp. 99-101.

GOBIERNO DE ESPAÑA (2013). *"Estrategia de Seguridad Marítima Nacional"*.

Gouveia, Jorge Bacelar and Santos, Sofia (coord.) (2015). *"Enciclopédia de Direito e Segurança",* Almedina, Coimbra.

Gouveia, Jorge Bacelar (2015). *"Direito Constitucional da Segurança" in* Gouveia, Jorge Bacelar and Santos, Sofia (coord.), *"Enciclopédia de Direito e Segurança",* Almedina, Coimbra, pp. 131-136.

Gouveia, Jorge Bacelar (2018). *"Direito da Segurança Cidadania, Soberania e Cosmopolitismo",* Almedina, Coimbra.

Goward, Dana A. (2019. *"Patterns of GPS Spoofing at Chinese Ports",* in MAREX, Daily Collection of Maritime Press Clippings 2019-356, pp. 31-32.

GPS WORLD, in https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/.

Guedes, Armando Marques (2015). *"Segurança externa"* e *"Segurança interna",* in Gouveia, Jorge Bacelar and Santos, Sofia (coord.), *"Enciclopédia de Direito e Segurança",* Almedina, Coimbra, pp. 411-418 and 425-431.

IMO, *"Guidelines on Maritime Cyber Risk Management"* (MSC-FAL.1/Circ.3) in http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20-Management%20(Secretariat).pdf.

Jesus, Luis António Cuco de (2019). *"Polemologia da Segurança Marítima – Golfo da Guiné como estudo de caso",* unpublished.

Kaplan, Elliott D. and Hegarty, Christopher J. (2006). "*Understanding GPS Principles and Applications*", 2nd Edition, ARTECH HOUSE, Boston-London, Norwood, MA, USA.

Lourenço, Nelson (2015). *"Segurança interna"* in Gouveia, Jorge Bacelar and Santos, Sofia (coord.), *"Enciclopédia de Direito e Segurança",* Almedina, Coimbra, pp. 431- 433.

Maman, Rafael (2020). *"The Reshaping Cyber Threat Landscape of Operational Technology",* presentation at the *"Conference organized by PwC, "Cybersecurity - The Challenges of Operational Technology",* Lisbon, 5 February.

Marques, António Gameiro (2019). *"A Segurança do Ciberespaço em Portugal e no Setor Marítimo",* Cadernos Navais, no. 52, April-June, Centro de Estudos Estratégicos da Marinha, in www.marinha.pt.

Marques, Antonio Gameiro (2018). *"Cibersegurança no Setor Marítimo", in* Revista de Marinha, no. 1004, Jul-Aug, pp. 30-32.

MINISTERY OF DEFENSE (MOD UK) (2014). "The UK National Strategy for Maritime Security", MOD UK, May.

Pedra, José Rodrigues (2012). *"A União Europeia e a Segurança no Mar", in* Cajarabille, Victor Lopo et all, *"A Segurança no Mar – uma visão holística"*, Mare Liberum, Aveiro, pp. 143-162.

Pereira, Luis Sousa (2012). *"A NATO e a Segurança no Mar" in* Cajarabille, Victor Lobo et all, *"A Segurança no Mar - uma Visão Holística"*, Mare Liberum, Aveiro, p. 129 and following.

Santos, Ana Miguel (2018). *"Uma segurança interna cada vez mais europeia? Uma segurança externa cada vez mais nacional?"* in RDeS - Revista de Direito e Segurança, Ano VI, Jul-Dec, pp. 27- 51.

Santos, Lino (2015). *"Cibersegurança"* e *"Segurança da informação" in* Gouveia, Jorge Bacelar and Santos, Sofia (coord.), *"Enciclopédia de Direito e Segurança",* Almedina, Coimbra, pp. 63-67 and 422-425.

Santos, Sofia (2015). *"Defesa preemptiva"* e *"Defesa preventiva" in* Gouveia, Jorge Bacelar and Santos, Sofia (coord.), *"Enciclopédia de Direito e Segurança",* Almedina, Coimbra, pp. 102-105.

THE AMERICAN CLUB 2010). *"Mass Global Positioning System (GPS) spoofing at ports in The People's Republic of China" in* Daily Collection of Maritime Press Clipping 2010-002, p. 25.

THE EUROPEAN CENTRE OF EXCELLENCE FOR COUNTERING HYBRID THREATS (2019). *"Handbook on Maritime Hybrid Threats – 10 Scenarios and Legal Scans",* November.

UNKNOWN (2019). *"2020 Vision: Check Point's cyber-security predictions for the coming year",* de 24-10-2019, in https://blog.checkpoint.com/2019/10/24/2020-vision-check-points-cyber-security.

US COAST GUARD (cyber report), in https://navcen.uscg.gov/?Do=GPSReportStatus.