Cybersecurity in the European Union port sector in light of the digital transformation and the COVID-19 pandemic

Manuela Bocayuva

Received: 29 November 2020 / Accepted: 11 May 2021 / Published online: 27 May 2021
© World Maritime University 2021

Abstract
The process of digital transformation, which is playing a fundamental role in the current COVID-19 worldwide panorama, has impacted all sectors of society, including the port sector. Albeit being a conservative sector, reluctant to change, it has been receptive to the opportunities offered by new information and communication systems and technologies, since they increase the efficiency of operation and, consequently, the competitive advantage of the port in the market. However, the digital era also brings new risks and threats, such as cyber-attacks. For various reasons, especially the lack of awareness about cybersecurity, such risks and threats are not being properly considered by the sector, leaving it vulnerable to attacks of this nature. In view of the importance of this sector to the EU Member States, given its status of critical infrastructure and its importance for the European economies, and the rise of cyber-attacks since the COVID-19 pandemic outbreak, it is vital to analyze the issue of cybersecurity in ports in view of digital transformation and understand the current situation.

Keywords Digital Transformation · COVID-19 · Ports · Cyber-attacks · Cybersecurity

1 Introduction
The port sector plays a fundamental role both at a national and international levels. Besides being central to the development of national economies (Faria 2018) and part of countries’ critical infrastructure, it is fundamental to the efficient functioning of the international trade logistics chain since about 90% of all international trade is carried by sea (International Chamber of Shipping 2019). Its importance is increasingly highlighted amid the COVID-19 crisis, given that the port sector plays a key role in moving

*Manuela Bocayuva
manuelabocayuva@gmail.com

1 NOVA School of Law, Lisbon, Portugal
goods such as medical and food supplies, supplying domestic markets, and keeping the economy moving during the pandemic.

In this regard, maritime transport offers the best cost benefit in terms of handling large volumes of cargo over long distances, with low prices and efficient services, which is why it is the most used mode for the international transport of goods. The current landscape of globalization requires that ports, in order to maintain their competitiveness in the market, provide services that facilitate transport, with agility, safety, and efficiency (Sanchez-Gonzalez et al. 2019). To this end, new technologies, especially automation and information and communication systems and technologies, have been used.

Nowadays, the majority of physical procedures in a maritime operation is performed using autonomous or semiautonomous mechanical physical systems and machineries controlled by advanced logistic software systems (Polemi 2018). In general, the maritime supply chains involve complex physical-digital systems, composed of a diversity of interconnected physical and digital assets that are controlled by a number of national and international and public and private stakeholders. They aim to provide timely and continuous transportation of goods and exchange of data between all the actors involved, from the producer to the final consumer (Polemi 2018).

Accordingly, there is a clear trend in the sector regarding the intensification of the digitalization process with the insertion and use of new information technologies and systems into these complex chains, increasing not only their efficiency, but also their dependence on digital technologies. If, on the one hand, the current COVID-19 crisis has revealed great heterogeneity concerning the level of digitalization in ports around the world, on the other hand, it will most certainly push even further this digitalization process (IAPH, ICHCA, TT CLUB, WPSP 2020).

Along with the benefits that it offers, digital transformation also introduces new risks and threats to the port activities, such as cyber-attacks. Ports could be attractive targets for cyber-attacks since they are the stage of high-value monetary transactions and entrance and exit of a large volume of goods. If a cyber-attack does come to pass, it would not only compromise the normal functioning of the port and, consequently, the supply of the domestic market, but also can generate major financial losses and impacts on the country’s economic development and safety. The port sector’s vulnerability to cyber-attacks is, thus, a matter of great concern.

In this regard, the European Union Agency for Cybersecurity (ENISA) published a report called Analysis of Cybersecurity Aspects in the Maritime Sector, in November 2011. This study was the first carried out within the European Union (EU) that sought to analyze the overall state of cybersecurity in the maritime sector (European Union Agency for Cybersecurity Agency 2011).

Despite the particularities of each maritime sector in the EU Member States, a common feature identified by the study was the general lack of attention to cybersecurity, due to the lack of awareness among the stakeholders, such as governments, port authorities, and transport companies, concerning the cyber vulnerabilities, cyber challenges, and cybersecurity risks specific to this sector (European Union Agency for Cybersecurity Agency 2011). However, the publication of this study failed to generate an adequate response to the problem, since no European strategy on the issue had been developed, adopted, and implemented at the time (Ahokas et al. 2017).
In November 2019, the ENISA published a new document regarding the subject entitled Port cybersecurity: good practices for cybersecurity in the maritime sector, which reached a similar conclusion and underlined several current issues, including the lack of cybersecurity mentality in the sector (European Union Agency for Cybersecurity 2019).

Given this scenario, this paper will address the issue of cybersecurity in the European Union port sector in view of the process of digital transformation and the COVID-19 pandemic. To that end, Section 2 will comment briefly about the process of digital transformation in the port sector, to subsequently address the issue of cybersecurity in the port sector in Section 3. In this third section, basic definitions related to cyberspace and cybersecurity will be presented followed by an overview of the current situation of cybersecurity in the port sector within the European Union discussing general aspects, legislative developments, and their main challenges, including the COVID-19 pandemic’s impact on the issue.

2 Brief comments about the digital transformation in the port sector

The phenomenon called digital transformation (DT or DX) alludes to the great changes caused by the use of digital technologies in society in general. In the economic sphere, this phenomenon refers to the process of adopting information, computing, communication, and connectivity technologies in order to improve an entity and solve problems, introducing significant changes in its performance and then improving its development. Thus, this phenomenon encompasses much more than technology itself; which is considered only one element of this complex process. To have competitive advantages in the digital world, companies must invest not only in the use of new technologies, but also in strategies and changes in their way of organizing (Vial 2019).

In the port sector, the efficiency introduced by the advent of containers in maritime transport required that the ports invest increasingly in the modernization and renewal of their infrastructure and port operations. Since then, digital transformation has proven to be a fundamental element for increasing the competitive advantage of ports. Investing in the capacity to track cargo and share information among the actors involved in cargo handling has become essential to reduce uncertainties in transport, improve the level of reliability in the services offered by the port, and improve the logistics of the integrated transport process (Heilig et al. 2019).

An effective digital transformation strategy involves not only the implementation of the technology itself, but also a specific management approach based on the port needs and particularities, the involvement of the stakeholders, and support through public policies. The benefits brought by automation and digitalization in this sector are manifold and include, inter alia, decline of accidents in ports and at sea, the reduction of pollution and polluting gas emissions, the optimization of port operations, and the improvement of the flow of incoming and outgoing ships (Babica et al. 2020).

Accordingly, the European Sea Ports Organisation (ESPO), an organization founded in 1993 that represents the interests of the port authorities, port associations, and port administrations of the EU Member States and Norway (Polemi 2018), addressed the digitalization process in the port sector in its recent Memorandum for the Commission and European Parliament entitled “Priorities of European Ports for 2019-2024.” In this...
document, the ESPO underlines that “digitalisation of the transport, logistics and supply chain will enhance efficiency, safety, security and environmental performance” (European Sea Ports Organisation 2019).

The 2020’s Review of Maritime Transport, published annually by the United Nations Conference on Trade and Development (UNCTAD), underlines that, as one of the COVID-19 pandemic’s legacy, digital transformation will further permeate supply chains, including the maritime transport sector, becoming a fundamental element instead of an option. Moreover, the digitalization has played a critical role in maintaining the maritime transport and port operations during the pandemic (United Nations Conference on Trade and Development 2020).

Nevertheless, an important aspect that must be considered with the increasing reliance on digital data and solutions is the risk of cyber incidents (European Sea Ports Organisation 2019). This issue has gained prominence in the maritime-port industry due to the materialization of some of these threats, as in the ransomware attack, in 2017, on the Danish logistics company MAERSK, which caused operational difficulties and large financial losses (United Nations Conference on Trade and Development 2018). Thus, with the inevitable progress of the digitalization and automation processes in the maritime-port sector, cybersecurity has become increasingly relevant and one of the main concerns of the sector.

3 Cybersecurity in the European Union port sector

The transportation sector, which comprises the ports, integrates a country’s critical infrastructure, which includes “any element of a system that is required to maintain societal function, maintain health and physical security, and ensure social and economic welfare” (Miron and Muita 2014). In the EU legislation, this concept can be found in article 2 (a) of the Directive 2008/14/EC, which defines critical infrastructure as “an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.” Thus, ensuring all aspects of the security of ports is paramount to maintain the functioning of the modern society, since disruptions on their activities can affect the economy, the safety, and the provision of basic services (Polemi 2018).

That said, the maritime-port sector has always demonstrated concern for the physical safety of its operations, proceedings, and activities (Jones et al. 2016), implementing safety management systems, and being legally supported by public institutions with the development of national and international rules and policies in this regard (Polemi 2018). However, technological dependence has introduced new types of risks and threats: the cybernetic kind (Jones et al. 2016). While digital transformation in ports can provide greater effectiveness in their operations and management, the pursuit of this competitive advantage can often result in the disregard of important security issues, namely cyber risks, which affects the balance between the benefits and risks of this process (Marques-Guedes 2018).

In this regard, at the current time, ports need not only to maintain the usual frequency of port operations, but also to continually invest in improving their efficiency
which, in many ports, is being done through this process of digital transformation. However, the proliferation of cyber-attacks carried out against ports and actors in the maritime-port sector around the world highlighted the degree of vulnerability of these sectors in face of this type of threat, as well as the lack of awareness and investment in cybersecurity.

To better comprehend the issue of cybersecurity in the port sector, basic definitions regarding cyberspace and cybersecurity will first be introduced. Subsequently, the main issue will be addressed by providing an overview of the current landscape of cybersecurity in the European Union’s port sector.

### 3.1 Basic definitions

Before delving into the issue of cybersecurity in the port sector, it is necessary to introduce general concepts specific to this subject. Firstly, an attempt must be made to delimit the definition of cyberspace. There seems to be no consensus among experts regarding the term cyberspace. A morphological analysis of the word reveals that its prefix “cyber-” refers to the virtual world and to the universe of information and communication systems and technologies (Marques-Guedes and Santos 2015).

Depending on the context, cyberspace is used to refer to different phenomena, such as telecommunications, computer technologies, hypertext, and hypermedia, among others, so that its concept is now vague and broad. Faced with this plurality of concepts, cyberspace is perceived as a collective concept, referring to the diversity of experiences that relate to computing and correlated technologies (Strate 1999). Hence, cyberspace can be broadly defined as “the collection of computing devices connected by networks in which electronic information is stored and utilized, and communication takes place” (Rantapelkonen and Kantola 2013).

Cybersecurity, then, refers to the capacity of cyberspace to resist intentional or unintentional threats and to recover from the materialization of such threats (Kapto 2013). Cybersecurity measures are actions taken to protect a device or a device’s system from attacks and unauthorized access, with the aim to maintain a stable condition in which cyberspace is in a state of security, i.e., protected and reliable (Ahokas et al. 2017).

A vulnerable cyberspace, that is, with insufficient cybersecurity measures, is exposed to different types of cyber threats (Ahokas et al. 2017). Associated with these threats, cyber risks estimate the probability of potential damage and losses from the materialization of these threats, such as damage to the company’s image, shutdown of its services, and financial losses (Biener et al. 2015).

Based on the motivations and objectives behind the cyber threats, they can be classified as hacktivism, cybercrime, cyberespionage, cyberterrorism, or cyberwarfare (Ahokas et al. 2017).

Hacktivism involves threats to cybersecurity that, through the use of hacking techniques, have the purpose of spreading or creating pressure for a certain cause or objective (Boyes et al. 2020). The term cybercrime, in turn, refers to the actions of anyone who, motivated by financial or personal gain, revenge, or bullying, interferes with information systems or technologies (Boyes et al. 2020). Such acts may infringe copyrights, involve forgery or identity theft, disseminate false information, and jeopardize the confidentiality, integrity, and availability of information and systems (Ahokas et al. 2017).
Cyberespionage refers to, whether for state or commercial reasons, the unauthorized access to sensitive and/or secret information, such as personal or commercial data and corporate strategies (Boyes et al. 2020). These sorts of attacks can result in damage to a company’s reputation, profits and efficiency, besides loss of important information (Ahokas et al. 2017). Cyberterrorism describes attempts to target, damage, or disrupt the operation of national critical infrastructures, through the use of computer networks, with the intention of intimidating or coercing a government or its people in support of specific political or social objectives (Weimann 2005). Finally, cyberwarfare is a cyber conflict between two States during which cyber-attacks against enemy State cyber structures are elements of a military operation (Kapto 2013).

Regardless of the motivations, cyber-attacks in general have a high degree of danger, since, unlike conventional physical attacks, they can be performed anonymously and from a safe distance. Moreover, not only can the vulnerabilities of the system be studied carefully before the attack, but it can also be implemented in the system and lie dormant for considerable time without being detected (Meyer-Larsen and Müller 2018).

These threats and risks are common to several sectors, including the maritime-port sector (Jensen 2015), in which they have materialized several times. They represent a real danger, both at a national and international level, to the stability and security of any entity, since “cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks,” since they “know no borders and no one is immune” (Juncker 2017). Such a scenario should be sufficient to galvanize investment in cybersecurity, regulation thereof, and the promotion and development of policies and strategies specifically aimed at this sector.

Following the introduction of some initial concepts on cybersecurity, the matter will be analyzed within the European port sector.

3.2 The current panorama of cybersecurity in the European Union port sector

Within the European Union, maritime transport is considered crucial to the economy. The more than 1200 ports located in the territories of its Member States enable the import and export of goods, trade within the EU, energy supply, and passenger transport. In order to efficiently perform these activities and improve their competitive advantage, ports are becoming increasingly dependent on technology. This scenario highlights the issue of cybersecurity in light of the new risks and threats arising from this digitization and digitalization of the sector (European Union Agency for Cybersecurity 2019).

3.2.1 General aspects of cybersecurity in the port sector

The port sector, in particular, has a set of features that are attractive to various types of cyber threats. First of all, ports provide essential services within the global trade logistics chain, supplying domestic markets with basic goods necessary for maintaining the functioning of modern society, making them part of countries’ critical infrastructures. In addition, ports store an enormous amount of essential information and data related to their functioning, which involves the entry and exit of ships and port operations, such as loading and unloading and storage of goods, besides being engaged in numerous high-value monetary transactions (Ahokas et al. 2017).
Cyber-attacks against ports can be carried out by different entities, ranging from individuals to the governments of enemy States. For instance, in the event of a cybercrime, criminal organizations seeking to gain some kind of financial advantage can identify vulnerabilities by illegally invading the port’s digital system. The illegal data thus harvested can facilitate the action of these organizations to execute theft or smuggling of goods that are arriving, leaving, or stored in the port area. In addition, criminals can also encrypt the system or information located in the port’s digital system, preventing any type of access until a ransom is paid (Meyer-Larsen and Müller 2018). When this is achieved by means of a malicious software, the program is called ransomware and the attack is referred to as a ransomware attack. Meanwhile, in the case of cyberwarfare, it is possible to disrupt a country’s port system in order to prevent it from functioning, thereby compromising military operations or domestic supplies in some way (Boyes et al. 2020).

The port sector is at highest risk from cybercrime such as ransomware and cyberespionage, followed by hacking and cyberterrorism which have a medium probability of materialization, with cyberwarfare having the lowest probability, although, should it occur, it has the potential to make a major impact (Moerel and Dezeure 2017).

Therefore, disruptions in the operation of ports can result in losses to the international trade logistics chain, to the economy of states, and to the public and private companies involved. Several cyber-attacks on ports have been reported around the world, in countries such as Iran, Australia, the United States of America, Canada, Spain, Belgium, and Brazil, among many others. The number of cyber-attacks on ports may be even higher than has been reported, given that, due to the industry’s lack of cybersecurity awareness, many companies refrain from reporting such attacks (Meyer-Larsen and Müller 2018).

In the European Union, cyber-attacks on the Port of Antwerp in Belgium between 2011 and 2013 and on the Port of Barcelona in Spain in 2018 are of particular note. In the case of the Port of Antwerp, it was uncovered in 2013 that hackers, hired by a criminal organization trafficking drugs, had invaded the port’s information system, i.e., its Port Community System (PCS). The hacking of PCS gave that criminal organization access to important data related to the security measures of the port and the position of each container that arrived at the port. This information enabled them to steal the containers before the arrival of the owners or the supervisors of the cargo at the port. These containers carried illegal drugs from other countries that were hidden within legitimate goods. This tactic was used surreptitiously by the criminal organization for 2 years before it was discovered (Jones et al. 2016).

On September 20, 2018, the Port Authority of the Port of Barcelona reported through social media, using its official Twitter profile, that a cyber-attack had affected several of their servers (Port de Barcelona 2018c) and cautioned that delays might occur in their operations while officers tried to remedy the situation (Port de Barcelona 2018b). The following day, they announced that, despite the attack on their system, the port was operating as normal and that the attack had not jeopardized their sea and land operations (Port de Barcelona 2018a). Not many details of the attack are known beyond those that have been made public.

Besides these two incidents, the attack on the Danish company MAERSK in June 2017, which was one of the largest cyber-attacks carried out to date in the maritime-port sector, should also be highlighted. The ransomware attack sustained by
the company, in addition to demanding the payment of a ransom, compromised its operations around the world, causing several days of disruption in seventeen terminals operated by the company, including two terminals in the Port of Rotterdam, in the Netherlands (United Nations Conference on Trade and Development 2017). Although there was no disclosure of data concerning their business and customers, the company estimated that the attack resulted in a financial loss of between 200 and 300 million dollars (Moerel and Dezeure 2017).

These attacks may have been facilitated due to the lack of awareness in the maritime-port sector regarding investment in cybersecurity. In 2014, CyberKeel, a company specialized in maritime cybersecurity, undertook a study on the issue involving several maritime-port stakeholders. It was observed that the maritime sector’s approach to cybersecurity is characterized by a lack of awareness of the incidence of cyber-attacks, a perception of these risks as being unrealistic, and a view of cybersecurity as being primarily a technical concern (Cyberkeel 2014). The lack of awareness regarding the actual danger of such threats has resulted in a lack of investment and resources allocated to cybersecurity by the companies. The episode involving MAERSK and the publicity given to other cyber-attacks have increased the visibility of the problem but is not nearly enough.

In view of the increasing pressure to develop policies to deal with cybersecurity in general, strategies have been developed both within the European Union and at the national level by some Member States. State action to provide the necessary support to ports and raise awareness of the vulnerabilities of digital systems to cyber-attacks is fundamental (Jensen 2015). In a similar way, some maritime authorities and international organizations have also been working towards creating cybersecurity strategies and standards to be adopted by the maritime-port industry. However, the very international nature of this sector and the large number of stakeholders involved render policy development and implementation of cybersecurity measures challenging (Ahokas et al. 2017).

One way in which the situation could potentially be improved is through the development of an international framework that establishes global cybersecurity standards, to avoid, for example, the adoption of conflicting national legislation by individual States, which can make implementation difficult given the international nature of the sector. However, this may take years to achieve and would most likely require the involvement of international organizations such as the International Maritime Organization (IMO). And since such a framework has not yet been developed, a more practical approach would be to develop a good practices guide on maritime-port cybersecurity to be adopted on a voluntary basis at a regional and/or international level (Jensen 2015).

Accordingly, in November 2019, the ENISA published a guide of good practices entitled Port Cybersecurity - Good Practices for Cybersecurity in the Maritime Sector, which aims to indicate good practices for cybersecurity in the maritime and port environment (European Union Agency for Cybersecurity 2019). This and other important international and European Union documents on cybersecurity in the maritime-port sector will be addressed in the following section.

### 3.2.2 International framework related to port cybersecurity

Port security measures have usually been reactions to major global shocks or disasters, such as the adoption of the IMO ISPS Code in response to threats to ships and ports...
following the September 11, 2001, terrorist attacks in the USA (Ahokas et al. 2017). The International Ship and Port Security Code (ISPS), which entered into force in 2004 under Chapter XI-2 of the International Convention for the Safety of Life at Sea (SOLAS Convention), acknowledges the importance of ports in maritime security and outlines a set of mandatory measures and recommendations to be followed by ships and port facilities in order to improve their security (International Maritime Organization 2020).

This Code assumes that ensuring the safety of ships and ports is a risk management activity. Therefore, in order to ensure that the measures adopted are the most appropriate, an analysis of the individual risks in each case must be carried out (Moerel and Dezeure 2017).

Although this code is designed to address the physical security of ports, it can be linked to cybersecurity at certain points, such as its measures concerning access control and authentication requirements. Among the ISPS Code’s measures, it is noteworthy that ports are required to prepare a risk analysis, called Port Facility Security Assessment (PFSA), and a security plan, called the Port Facility Security Plan (PFSP). In the scope of the PFSA, an analysis of all aspects and security risks regarding the port and its facilities should be carried out, in particular, identifying its vulnerabilities and the possible security measures that should be taken in view of each risk. This analysis will be used as the basis for the PFSP, which must identify all measures, procedures, and actions that should be taken for each of the different security levels (Nordfeld and Dimitrios 2018).

Another key international document for the maritime-port sector, which, like the SOLAS Convention, has been elaborated within the IMO, is the Convention on Facilitation of International Maritime Traffic (FAL Convention). This convention, in force since 1967, has as its main purpose to increase the efficiency of maritime transport, with norms and recommendations to standardize and simplify formalities, procedures, and typical documents of the maritime-port sector. To this end, it established standard forms to be used in the interchange of information in the maritime-port sector, in particular, with regard to communication between ports and ships (International Maritime Organization 1965).

In order to ensure the FAL Convention remains current and relevant, it is regularly amended and updated within the IMO Facilitation Committee (FAL Committee), which meets annually. In this regard, as of April 2019, the FAL Convention requires that public authorities introduce systems that enable the electronic exchange of information between ships and ports (International Maritime Organization 2019). This mandatory requirement was introduced in 2016 through a set of amendments under the revised Annex of the convention. Considering the advantages provided by the new information technologies and systems, this convention also encourages the use of single window systems to facilitate the storage, access, and exchange of information. On the other hand, this requirement for implementation and standardization of electronic information exchange ultimately increases the cyber risks and cyber threats to the industry (European Union Agency for Cybersecurity 2019).

Specifically on cybersecurity in the maritime sector, it is worth mentioning the IMO document entitled Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3), approved at the 41st session of the FAL Committee and the 98th session of the Maritime Security Committee (MSC) (International Maritime Organization 2017). This
document recognizes the urgency of raising the industry’s awareness of cybersecurity and presents recommendations on cyber risk management in the maritime sector (Rana 2019).

In addition, these guidelines acknowledge that each institution in the maritime industry is different. Therefore, to obtain details and guidance related to the development and implementation of suitable risk management processes, each institution should refer to the most relevant requirements stipulated by the flag state administrations for their particular needs. They can also employ industry standards such as ISO/IEC 27001 (International Organization for Standardization 2013), which sets out requirements for an information security management system, and good practice guides such as Guidelines on Cybersecurity Onboard Ships (International Chamber of Shipping 2018), developed by a group of institutions and organizations (International Maritime Organization 2017).

However, the IMO Guidelines on Maritime Cyber Risk Management focus on offering recommendations to safekeep ships from current cyber risks and threats. It does not offer guidelines to port authorities and stakeholders on the management of their physical and digital interconnected infrastructure and systems (Polemi 2018).

It is thus noted that none of the aforementioned international conventions or documents specifically addresses cybersecurity in the port sector. Although good practice guides on the subject have been developed at both national and international levels, such as the Good Practice Guide - Cyber Security for Ports and Port Systems, published in 2016 and revised in 2020 by the UK Institute of Engineering and Technology (Boyes et al. 2020), and the good practices guide on port cybersecurity published in November 2019 by the ENISA within the EU, no binding international norms and standards exist on the subject.

3.2.3 European Union’s framework related to port cybersecurity

As mentioned above, in 2011, the ENISA published a report analyzing aspects of cybersecurity in the maritime sector. This was the first and only report published by the agency until the good practices guide on port cybersecurity was published in November 2019. In the 2011 report, the ENISA highlighted two important points (ENISA 2011):

- The low to non-existent awareness of the need and challenges of cybersecurity in the maritime sector; and
- The lack of specific regulations on cybersecurity, particularly with regard to the maritime-port sector and on how to proceed legally in the event of a cyber-attack.

Since 2011, digital transformation in society as a whole has intensified and in an effort to be aligned with this process, notwithstanding the lack of specific legislative documents on cybersecurity in the maritime-port sector, the EU was compelled to develop its cybersecurity legislation and framework, in general.

Before addressing the European legislation on cybersecurity, a number of European documents on security in the maritime-port sector, such as Regulation (EC) 725/2004, Directive 2005/65/EC, and Regulation (EC) 336/2006, should be highlighted. These documents correspond to chapters of the SOLAS Convention which have been transposed into European legislation.
Regulation (EC) 725/2004 seeks to enhance the security of ships and port facilities (European Union 2004). It is responsible for implementing the ISPS Code, while Directive 2005/65/EC focuses specifically on enhancing port security (European Union 2005). These two documents were responsible for introducing the ISPS Code measures such as the risk analysis and the port security plans (PFSA and PFSP) into European legislation. As for Regulation (EC) 336/2006, it concerns the implementation of the International Safety Management (ISM) Code in the European maritime sector (European Union 2006); however, it should be noted that this Code is not applicable to ports (European Union Agency for Cybersecurity).

Another important European Union document is Directive 2008/14/EC, aforementioned, which “establishes a procedure for the identification and designation of European critical infrastructures (‘ECIs’), and a common approach to the assessment of the need to improve the protection of such infrastructures in order to contribute to the protection of people” (Article 1) (European Union 2008). The energy and transport sectors, including the ports, are the sectors “to be used for the purposes of implementing this Directive” (Article 3, n° 3). This document recognized the vital societal importance of these sectors and the need of special and specific security measures to avoid any interruption of their services.

In 2010, the use of the FAL Convention standard forms was implemented in the territories of European Union Member States by Directive 2010/65/EU (European Union 2010). This Directive also introduced the maritime information exchange system at both the national and the European Union levels which simplifies the electronic information exchange between the maritime authorities of the Member States.

However, in June 2019, the Regulation (EU) 2019/1239 repealed and replaced Directive 2010/65/EU, with effect from 15 August 2025 establishing its application instead (European Union 2019b). The new Regulation addresses the multiple and non-harmonized reporting processes by ships still existent in the EU ports. When a ship arrives at, stays in, and departs from a port, it is obliged to transmit to a range of entities an array of information regarding its arrival at, stay in, or departure from the port. The non-harmonized reporting processes create an excessive administrative burden.

The framework established by Regulation (EU) 2019/1239 aims “to facilitate the electronic transmission of information in relation to reporting obligations for ships arriving at, staying in and departing from a Union port,” with the creation of a “technologically neutral and interoperable European Maritime Single Window environment (‘EMSWe’) with harmonised interfaces” (Article 1).

In June 2014, the European Union presented its Maritime Security Strategy, publishing its action plan in December of the same year, which was revised in 2018 (Marques-Guedes 2019). This strategy was developed as an instrument of cooperation across borders and sectors to promote overall compliance with legislation and security in the European maritime domain, including the maritime infrastructure which comprises ports and port facilities (Council of the European Union 2014). It was observed, in item V, that “maritime security threats are multifaceted, pose a potential risk to European citizens and can be detrimental to the EU’s and its Member States’ strategic interests,” and went on to enumerate the risks and threats that had been identified which included “(…) d) Terrorism and other intentional unlawful acts at sea and in ports against ships, cargo, crew and passengers, ports and port facilities and critical maritime and energy infrastructure, including cyber-attacks [emphasis added]; (…) .”
European Union’s Maritime Security Strategy is thus one of the first documents within the European Union, besides the ENISA’s 2011 and 2019 reports, to formally acknowledge cyber-attacks as risks and threats to the European maritime-port industry.

On the subject of cybersecurity in general, the European Union’s effort to legislate on this issue is evident. In this context, three important documents are noteworthy: Regulation (EU) 2016/679, Directive (EU) 2016/1148, and Regulation (EU) 2019/881. The purpose of Regulation (EU) 2016/679, called the General Regulation on Data Protection (RGPD), is to protect individuals with regard to the processing of personal data and the unrestricted movement of such data, stressing that this is a fundamental right (European Union 2016a). The requirements for the personal data protection established by this regulation apply to all sectors, including the maritime-port sector (European Union Agency for Cybersecurity 2019).

The Directive (EU) 2016/1148 also known as the NIS Directive was created with the aim of increasing the degree of security of networks, services, and information systems (European Union 2016b). To this end, it introduces measures related to cybersecurity and obliges Member States to adopt a national strategy for the security of networks and information systems. With regard to the maritime-port sector in particular, this directive takes into account two points. The first concerns the security requirements applicable to the sector under EU legal acts which cover all operations, including networks and information systems, of which “part of the mandatory procedures to be followed includes the reporting of all incidents and should therefore be considered as lex specialis, in so far as those requirements are at least equivalent to the corresponding provisions of this Directive.”

And the second point, that Member States, when identifying key operators in this sector, should take into account existing and future international codes and guidelines developed by the IMO, in order to enable a coherent approach to the various maritime operators. Under the aegis of this Directive, the port sector can be qualified as operators of essential services. As operators of essential services, it is required that appropriate measures are taken to manage security risks and reduce any impact in the event of an incident. In addition, in case of any incident that significantly affects the continuity of the services, it must be reported to the competent national authorities for cybersecurity (Moerel and Dezeure 2017).

The Regulation (EU) 2019/881 of April 2019, referred to as the EU Cybersecurity Act, introduces a cybersecurity certification framework for products, services, and processes related to information and communication technologies, applicable within the European Union (European Union 2019a). In addition, it strengthens ENISA’s role with regard to the security of EU Member States’ cyberspace by giving it a permanent mandate, more resources, and new functions. The ENISA assumes a key role in the development and implementation of this certification framework, which will provide a set of technical requirements, standards, and procedures that will define the level of reliability of these technologies (European Commission 2020).

In November 2019, the ENISA, already acting under the EU Cybersecurity Act, published a good practices guide on cybersecurity in the port sector aimed at the maritime-port industry. This document aims to introduce a set of good practices to the industry by analyzing relevant challenges, risks, and threats to cybersecurity and presenting possible scenarios. It also intends to raise awareness in the sector and promote cooperation in the maritime-port environment in the EU. Therefore, this guide,
which has been developed in collaboration with several ports in the European Union, seeks to continue the 2011 ENISA report by addressing the evolving challenges of cybersecurity in the maritime-port sector (European Union Agency for Cybersecurity 2019).

In March 2021, the European Commission presented the document entitled “2030 Digital Compass: the European way for the Digital Decade” a communication to the European Parliament, the Council and the European Economic and Social Committee, and The Committee of the Regions Empty. This document aims to present an initial plan to enhance EU’s digital transformation, improving their digital sovereign and digital policies and also addressing vulnerabilities and threats. For that, the European Commission proposes what they call a Digital Compass that is based on four points that demonstrates the EU’s main digital goals, which are the following: (1) the digital empowerment of the population; (2) the enhancement of digital infrastructures connectivity and performance; (3) the digital transformation of businesses; and (4) the digitalization of public services (European Union 2021). This clearly demonstrates the EU’s ambitions on the deepening of their digital dependency, a scenario that requires even more consideration to cybersecurity policies and strategies.

In addition to these documents drawn up within the European Union, some EU Member States have also taken the initiative to develop their own national strategies on the subject of cybersecurity, such as the French Critical Infrastructures Information Protection (CIIP) law, developed with the aim of strengthening the cybersecurity of their critical infrastructure (Agence Nationale de la Sécurité des Systèmes d’Information 2020).

3.2.4 The European port sector’s current challenges regarding cybersecurity

2019 ENISA’s good practice guide underlined several current challenges that the port sector, in particular, faces regarding the risks and threats arising from the sector’s digital transformation and the implementation of cybersecurity measures to avoid them or, at least, minimize their effects should they occur.

According to this document, the main challenges of the sector at the time were (European Union Agency for Cybersecurity 2019):

- The lack of digital culture in the port sector due to its conservative nature;
- The lack of awareness and training on cybersecurity;
- The lack of time and budget devoted to cybersecurity;
- The lack of human resources and people qualified to deal with specific cybersecurity issues;
- The complexity of the port sector due to the wide variety of actors and interdependence among them;
- The importance of striking a balance between the efficiency of services provided and cybersecurity;
- The existence of outdated systems and practices;
- The absence of legal requirements related to cybersecurity;
- The difficulty of keeping up to date with recent threats;
- The technical complexity of the port’s IT (use of data as information) and OT (use of data to control or monitor physical processes) systems;
The tendency of convergence and connectivity of IT and OT systems;
Challenges in the logistics chain;
The great interdependence between the port’s systems and other external systems; and
The new cyber risks arising from the intensification of the digital transformation of ports.

These challenges are each of a different nature, involving technical, policy, legal, and business issues. Many of them are not novel, having been repeatedly pointed out by scholars and operators working in the area and by reports from public and private institutions. The ENISA’s reports of 2011 and 2019 reached similar conclusions regarding the continuous lack of cybersecurity awareness in the maritime-port sector, even after the materialization of cyber-attacks that caused security breaches, affecting credibility and causing damage and loss to the stakeholders involved.

The urgency of the problem is evident considering the importance of the sector and the number and nature of the challenges still faced by it. In the context of the European Union, the recently established Regulation (EU) 2019/1239 implementing an European Maritime Single Window Environment demonstrates EU’s intent on increasingly investing in the sector’s standardization through digitalization, which also demands an even more attentive and careful approach to cybersecurity, since a cyber-attack could cause innumerable damages and losses in a European level, besides undermining the credibility and effectiveness of initiatives such as this.

There is no denying that since the publication of the 2011 ENISA report there has been a remarkable evolution in the awareness and legislation on the issue of cybersecurity, in general, in the European context. However, there is still a long way to go, especially on regulation of cybersecurity for the maritime-port sector. Given the long list of existing challenges, efforts from different institutions are fundamental, ranging from the maritime-port sector stakeholders, from national governments and regional and international institutions and organizations interested in the topic, so that they can collaboratively work towards finding possible solutions or answers to these challenges.

Since the outbreak of the COVID-19 pandemic, digital solutions are proving to be important instruments in the maintenance of many economic and social activities. While the digital transformation has been impacting and changing the port sector environment and its functioning in the last few decades, it is hard to pinpoint precisely the intensification level of the digitalization process directly related to the COVID-19 pandemic. Nevertheless, some examples illustrate this impact, such as the use of drones in ports to guarantee the observance to social distancing rules and the installation of thermal cameras to assist in the measurement of body temperature, with the latter being used by the Port of Coronel in Chile since the early days of the pandemic (WBG, IAPH, WPSP 2021). Another example is the COVID-19 contact tracing system launched in September of 2020 by the Philippine Ports Authority (PPA) to be used by all the port community with the aim of facilitating the movement inside the ports while maintaining the necessary health protocols (Philippine Ports Authority 2020).

Although it is still early to estimate the full extent of the damage and losses caused by the COVID-19 pandemic, it is evident that the pandemic caused disruptions to economies all around the world, affecting countries in different levels. In regard to the volumes of global container trade, there was a decline by 8.6% in February 2020 when
compared to the same period of 2019 (ITF 2021). This affected directly the activities of container ports, suffering a reduction by 6% in February and March in the volumes handled in the main global container ports (ITF 2021).

In June of 2020, a variety of maritime trade and logistics stakeholders launched a call for action to accelerate digitalization in the sector in light of the COVID-19 pandemic, listing a series of priorities, including the need to review the IMO’s Guidelines on Maritime Cyber Risk Management in order to also address cyber risks in the port environment1. According to this statement, the pandemic also highlighted the current heterogenous landscape in the sector when it comes to the different levels of digitalization, which is illustrated by the fact that only 49 out of 174 Member States of the IMO having functioning Port Community Systems (PCS) to date (IAPH, BIMCO, FONASBA, ICHCA, ICS, IHMA, IMPA, IPCSA, ISSA 2020).

With the digital transformation playing a fundamental role in the COVID-19 pandemic (United Nations Conference on Trade and Development 2020), cybersecurity needs to become a topic of discussion within the port communities to facilitate the development and implementation of collaborative measures through the cooperation of public and private sector stakeholders. In this sense, Port Authorities should leverage on their central role in port operations in order to facilitate this dialogue and cooperation among stakeholders (IAPH, ICHCA, TT CLUB, WPSP 2020).

Since the outbreak of the COVID-19 pandemic, an increase in cyber threats and attacks has been observed. A study published by the UK-based risk management firm Astaara in partnership with the British Port Association reported that since February 2020 cyber-attacks in the global maritime sector have quadrupled. While cybercrimes cost the global economy around 2 trillion dollars per year, only 150 billion dollars are spent yearly on cybersecurity measures (Astaara, British Ports Association 2020). Accordingly, the Port of Los Angeles’ executive director revealed in December 2020 that unauthorized cyber intrusions attempts have doubled since the start of the pandemic (IAPH, BIMCO, FONASBA, ICHCA, ICS, IHMA, IMPA, IPCSA, ISSA 2020).

The maritime and port stakeholders have started to understand the value of information security and to invest in improving their cybersecurity culture in order to support their whole operations and services. This culture can continue to be developed with the implementation of concrete actions towards raising awareness and training on cybersecurity directed towards the personnel working in the maritime and logistics supply chains at national, regional, and international levels. Furthermore, maritime and cybersecurity organizations and institutions, such as the IMO and ENISA, can also act on cybersecurity training and development by organizing events and offering courses and seminars on the subject (Polemi 2018).

The white paper on Port Community Cybersecurity published by International Association of Ports and Harbors (IAPH) with the support of other institutions underlines the importance of creating a common global language regarding cybersecurity

---

1 This call for action was launched by the following institutions: the International Association of Ports and Harbors (IAPH), BIMCO, the International Cargo Handling Coordination Association (ICHCA), the International Chamber of Shipping (ICS), the International Harbour Masters’ Association (IHMA), the International Maritime Pilots Association (IMPA), the International Port Community Systems Association (IPCSA), the International Ship Supplier’s Association (ISSA), the Federation of National Associations of Ship Brokers and Agents (FONASBA), and the PROTECT Group.
within the port communities. This revolves around the implementation of three elements. The first one concerns the need to define a common glossary of cyber terms for their specific environment to avoid any inaccuracy or ambiguity in the dialogue. Making the language more accessible to professionals of different backgrounds will improve communication and the understanding that digitalization and cybersecurity are also business issues not limited to the IT sector (IAPH, ICHCA, TT CLUB, WPSP 2020).

The second one, with the acceptation of its business aspect, regards the importance of allocated financial support to effectively manage cybersecurity within the port community ecosystem. Port stakeholders need to start taking cybersecurity into consideration when making investments decisions. The third element is establishing who is responsible for managing each of the aspects present in an organization’s cybersecurity efforts and understanding that it is a shared responsibility (IAPH, ICHCA, TT CLUB, WPSP 2020).

In parallel, insurance companies and auditors could also cooperate on raising awareness and promote the adoption of cybersecurity measures by requiring that stakeholders comply with cybersecurity standards, guidelines, and legislation (Polemi 2018).

Since maritime security issues such as these are not uncommon and since it is very important that the EU and international rules regarding them are harmoniously implemented, the issue of cybersecurity in the maritime-port sector would be best addressed through the drafting of an European and/or international document covering the issue of cybersecurity in the maritime-port sector. During the elaboration of such document within the setting of an organization such as the European Union or even the International Maritime Organization, all or most of these challenges could be exhaustively analyzed and debated by the most varied stakeholders and national representatives from different regions of Europe and the world, presenting different perspectives, with the purpose of finding appropriate solutions and responses to these problems. However, when developing any policy, strategy, or legislation on the subject, it is vital that it protects against the cyber risks and threats while enabling the evolution of digital transformation in the sector (European Sea Port Organisation 2019).

4 Final remarks

The process of digital transformation has altered society in the most varied aspects, influencing its ways of consumption, operation, and interaction. This process also affects critical services and infrastructures, which are fundamental to the maintenance of the functioning of current society. These services are increasingly required to be more efficient in order to accomplish their purpose in maintaining such a lifestyle.

In the port sector in particular, this efficiency is also essential to improve the ports’ competitive advantage within the complex market in which they operate. Notwithstanding the hesitation of the maritime-port sector to fully embrace digital transformation, this process has been a key element in the development of international trade and maritime transport, especially after the introduction of containers in the 1960s.

However, the digital age has also brought cyber risks and threats that are not being properly considered by stakeholders in this sector. These risks and threats, in the event
that they occur, can have major impacts both financially and in terms of service continuity, as observed in the case of MAERSK in 2017. Moreover, they can jeopardize the security, economies, maritime operations, societies, and environment of the EU Member States, both at national and European levels.

The new digital era introduced new challenges for port operators with regard to the security of their physical and digital assets and operations. However, for several reasons, especially the lack of awareness, the complexity, and the interdependence of the sector’s stakeholders, it led to cybersecurity measures not being properly considered or implemented.

With the COVID-19 pandemic, the increase of digital dependence, and the quadrupling of cyber-attacks in the global shipping industry, the European port sector will be digitally vulnerable if the cyber risks are not considered and the cybersecurity measures are not appropriately adopted. It is important to take advantage of the opportunities offered by this process, while ensuring the security of the port’s operations, personnel, and infrastructure.

On this note, investing in cybersecurity in the port sector should be understood as a tool that will securely enable the intensification of digital transformation in the sector. Since security is a collective responsibility, especially in such an interdependent and complex industry, it is crucial that the stakeholders in the maritime-port sector and all others interested in the continuity of their services, whether public or private, national or international, act in cooperation to improve their digital resilience.

Within the European Union, legislation has evolved considerably with regard to cybersecurity. However, there is still no regulation addressing the maritime-port sector specifically. Although the good practices guide on port cybersecurity published by the ENISA in November 2019 is an important development, the relevance of the maritime-port sector for society and for the States’ economies makes it urgent to invest in cybersecurity and to find solutions to the various current challenges to cybersecurity in order to reduce the degree of vulnerability of this sector to cyber risks and threats.

**Code availability**  Not applicable

**Author contribution**  Not applicable

**Funding**  Not applicable

**Data Availability**  Not applicable

**Declarations**

**Conflict of interest**  Not applicable

**References**

Aastara Company, British Ports Association (2020) Managing Port’s Cyber Risks: white paper. https://www.britishports.org.uk/system/files/documents/bpa_a斯塔拉_白色_论文_0.pdf. Accessed 4 May 2021
Agence Nationale de la Sécurité des Systèmes d'Information (2020) The French CIIP Framework. https://www.ssi.gouv.fr/en/cybersecurity-in-france/ciip-in-france/. Accessed 15 Nov 2020

Ahokas J, Kiiski T, Malmsten J, Ojala L (2017) Cybersecurity in ports: a conceptual approach. In: Kersten W, Blecker T, Ringle CM (eds) Digitalization in Supply Chain Management and Logistics, 1st edn. Epubli GmbH, Berlin, pp 343–359

Babica V, Sceulovs D, Rustenova E (2020) Digitalization in maritime industry: prospects and pitfalls. In: Ginters E, Estrada MAR, Eroles MAP (eds) ICTE in Transportation and Logistics 2019, 1st edn. Springer, Cham, pp 20–27

Biener C, Eling M, Wirfs JH (2015) Insurability of cyber risk: an empirical analysis. Geneva Pap Risk Insur Issues Pract 40:131–158. https://doi.org/10.1057/gpp.2014.19

Boyes H, Isbell R, Luck, A (2020) Good Practice Guide Cyber Security for Ports and Port Systems. The Institution of Engineering and Technology. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/859925/cyber-security-for-ports-and-port-systems-code-of-practice.pdf. Accessed 30 Oct 2020

Council of the European Union (2014) European Union maritime security strategy: responding together to global challenges. http://register.consilium.europa.eu/doc/srv/?l=EN&f=ST%201205%202014%20INIT. Accessed 17 Oct 2020

Cyberkeel (2014) Maritime cyber-risks. https://docs.wixstatic.com/ugd/2d153e_46bd931729324d4b81723567d9e7d288.pdf. Accessed 2 Oct 2020

European Commission (2020) The EU Cybersecurity Act. https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act. Accessed 15 Nov 2020

European Sea Ports Organisation (2019) Priorities of European Ports for 2019-2024: what ports do for Europe, what Europe can do for ports. https://www.espo.be/media/Memorandum%20ESPO%20FINAL%20Digital%20version.pdf. Accessed 2 Oct 2020

European Union (2004) Regulation (EC) n° 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security. Eur-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32004R0725&from=En. Accessed 17 Oct 2020

European Union (2005) Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security. Eur-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32005L0065&from=EN. Accessed 12 Oct 2020

European Union (2006) Regulation (EC) n° 336/2006 of the European Parliament and of the Council of 15 February 2006 on the implementation of the International Safety Management Code within the Community and repealing Council Regulation (EC) n° 3051/95. Eur-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32006R0336&from=GA. Accessed 17 Nov 2020

European Union (2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Eur-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32008L0114&from=EN. Accessed 17 Oct 2020

European Union (2010) Directive 2010/65/EU of the European Parliament and of the Council of 20 October 2010 on reporting formalities for ships arriving in and/or departing from ports of the Member States and repealing Directive 2002/6/EC. Eur-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010L0065&from=EN. Accessed 24 Oct 2020

European Union (2016a) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Eur-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN. Accessed 4 Nov 2020

European Union (2016b) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Eur-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN. Accessed 5 Oct 2020

European Union (2019a) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) n° 526/2013 (Cybersecurity Act). Eur-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN. Accessed 5 Oct 2020

European Union (2019b) Regulation (EU) 2019/1239 of the European Parliament and of the Council of 20 June 2019 establishing a European Maritime Single Window environment and repealing Directive...
Marques-Guedes A (2019) A Segurança do ciberespaço em Portugal e no setor marítimo. Edições Culturais da Marinha, Lisboa

Marques-Guedes A, Santos L (2015) Breves reflexões sobre poder e ciberespaço. Revista de Direito e Segurança 6:189–209 http://hdl.handle.net/10400.26/14329

Meyer-Larsen N, Müller R (2018) Enhancing the cybersecurity of port community systems. In: Freitag M, Kotzab H, Pannek J (eds) Dynamics in Logistics: Proceedings of the 6th International Conference LDIC 2018, Bremen, Germany. Springer, Berlin, pp 318–323

Miron W, Muita K (2014) Cybersecurity capability maturity models for providers of critical infrastructure. Technology Innovation. Manag Rev 4(10):33–39. https://doi.org/10.22215/timreview/837

Moerel L, Dezeure F (2017) Cyber security in ports: business as usual? Vlaams Nederlandse Delta. http://www.vndelta.eu/files/3215/1125/0649/Cyber_Security_in_Ports_Whitepaper_VND_vonference_november_2017.pdf. Accessed 30 Apr 2020

Nordfeld A, Dimitrios D (2018) Assessing the need of implementing ISPS Code instruments to maritime customs units. In: Il Diritto Maritimo – Quaderni 5: Port, Maritime and Transport Law, between legacies of the past and modernization. Bonomo Editore, Bologne pp 243-260

Philippine Ports Authority (2020) PPA launches COVID-19 contact tracing system for all port users, community. https://www.ppa.com.ph/content/ssa-launches-covid-19-contact-tracing-system-all-port-users-community. Accessed 4 May 2020

Polemi N (2018) Port cybersecurity: securing critical information infrastructures and supply chains. Elsevier, Amsterdam

Port de Barcelona (2018a) “[ACTUALIZACIÓN] El #PortdeBarcelona ha respondido activamente al #ciberataque recibido ayer, operando con total normalidad y sin verse alterada en ningún momento su operativa marítima y terrestre.”. Twitter. https://twitter.com/portdebarcelona/status/10431455773379456. Accessed 30 Apr 2020

Port de Barcelona (2018b) “Delivery and reception of goods may be somewhat delayed today. We will continue to provide status updates on this matter”. Twitter. https://twitter.com/portofbarcelona/status/1042701904726421504. Accessed 30 Apr 2020

Port de Barcelona (2018c) “Early this morning the #PortofBarcelona suffered a cyberattack affecting a number of its servers. Our Information Systems department is gauging the extent of the attack and implementing its contingency plans for this type of situation”. Twitter. https://twitter.com/portofbarcelona/status/1042701903270961152. Accessed 30 Apr 2020

Rana A (2019) Commercial maritime and cyber risk management. Safety and Defense 5(1):46–48. https://doi.org/10.37105/sd.42

Rantapakelkonen J, Kantola H (2013) Insights into cyberspace, cyber security, and cyberwar in the Nordic countries. The Fog of Cyber Defence. National Defence University, Helsinki, pp 24–36

Sanchez-Gonzalez P, Díaz-Gutiérrez D, Leo TJ, Núñez-Rivas LR (2019) Toward digitalization of maritime transport? Journal Sensors 19(4):1–22. https://doi.org/10.3390/s19040926

Strate L (1999) The varieties of cyberspace: problems in definition and delimitation. West J Commun 63(3):382–412. https://doi.org/10.1080/10570319909374648

United Nations Conference on Trade and Development (2017) Review of Maritime Transport 2017. https://unctad.org/en/PublicationsLibrary/rmt2017_en.pdf. Accessed 30 Apr 2020

United Nations Conference on Trade and Development (2018) Review of Maritime Transport 2018. https://unctad.org/system/files/official-document/rmt2018_en.pdf. Accessed 24 Nov 2020

United Nations Conference on Trade and Development (2020) Review of Maritime Transport 2020. https://unctad.org/system/files/official-document/rmt2020_en.pdf. Accessed 16 Nov 2020

Vial G (2019) Understanding digital transformation: a review and a research agenda. J Strateg Inf Syst 28:118–144. https://doi.org/10.1016/j.jsis.2019.01.003

WBG, IAPH, WPSP (2021) Accelerating Digitalization: critical actions to strengthen the resilience of the maritime-supply chain. http://pubdocs.worldbank.org/en/773471610730436879/Accelerating-Digitalization-Across-the-Maritime-Supply-Chain.pdf. Accessed in 4 May 2021

Weimann G (2005) Cyberterrorism: the sum of all fears? Studies in conflict and terrorism 28(2):129–149. https://doi.org/10.1080/10576100590905110

Publisher’s note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.