Available online at www.sciencedirect.com

ScienceDirect

Transportation Research Procedia 45 (2020) 547–554

Transportation Research Procedia

www.elsevier.com/locate/procedia

AIIT 2nd International Congress on Transport Infrastructure and Systems in a changing world (TIS ROMA 2019), 23rd-24th September 2019, Rome, Italy

Critical infrastructures cybersecurity and the maritime sector

Juan Ignacio Alcaide[a*], Ruth Garcia Llave[a]

[a]*University of Cadiz, Campus Rio San Pedro, Puerto Real 11510, Spain*

Abstract

The paper addresses cyber-security in the maritime field, a sector increasingly vulnerable to cyber-attacks due to advances that are already in the process of implementation. This paper explores the level of knowledge and training required on the subject and its interaction with marine ecosystem. For this reason, we will carry out a deep bibliographic review in which we will support our later study. We will analyze the results obtained in an online questionnaire answered by experienced maritime professionals. The results show a lack of general knowledge in the field of maritime cybersecurity. Therefore, it is necessary to increase training levels in the maritime sector and the port interface connection with the supply chain.

Keywords: Cybersecurity; Critical Infrastructures; Maritime Sector; Maritime Supply Chain

1. Introduction

The maritime industry represents 90% of the commercial trade exchanges carried out worldwide, where the supply chains of the main production sectors depend on it (UNCTAD, 2018). The maritime sector, as a vital part of the global economy must be protected from threats and cyber-attacks. A cybernetic incident can lead to a major environmental or economic disaster, even being able to cause the loss of human lives. The maritime sector is immersed now in a process of adaptation to new technological environment demanded by information technologies (creates, processes, stores, information, etc.), and integrates operational technology (monitors, control, etc.) with the aim of optimizing management processes. Technological changes are being implemented by shipping companies more slowly compared to other productive sectors. As a result, the maritime sector is suffering largely the risks of cyber-attacks associated to this way of conceiving and managing business,. The US Coast Guard recognized the emerging cyber-threats to its regulated community (USCG, 2017). In 2017, the MAERSK shipping company faced the attack of the Petya virus, temporarily limiting its commercial and logistic operation, not only damaging the company's reservation system and slowing container tracking, but also causing congestion in almost 76 ports around the world operated by its subsidiary, APM Terminals (Jensen, 2017).

There are more than 50,000 merchant ships operating internationally, transporting all types of cargo. These ships have to berth in Critical Infrastructures (CI) to carry out their usual operations (ports, platforms,

* Corresponding author. Tel.: +34-956-016-385; fax: +34-956-016-385.
E-mail address: juanignacio.alcaide@uca.es

10.1016/j.trpro.2020.03.058

refineries, pipelines, power stations, etc.). Ports are one of the most important links in the logistics chain, particularly in recent years, due to exceptional growth of container shipping. In the CI, the possible illicit activities of cybercrime or cyberterrorism can come to condition the economic and institutional activity of the countries, and always cause losses to multiple economic actors, as a consequence of the collapse of processes and services (enisa, 2011; IMO, 2017). Cyber-security in the maritime sector is the great obsession of shipping companies, since nowadays almost everything is managed through the internet, which is the vehicle of relationship and transition between a company, its suppliers and its customers, giving rise to hackers to pirate and access the data of a shipping company very easily. These attacks not only refer to economic damages but also affect the reputation and reliability when it affects the confidence that the environment has in the company. Since the plans are focused on reducing risks associated with safety, port disruption and environmental concerns, a traditional cyber-security assessment may not suffice (BIMCO, 2018).

A large part of security breaches is caused by human factor and poor processes which means that also crew aspects need to be considered when assessing the cyber risk. The best cyber-security practices need to be implemented, where risk management is essential for maritime transport to handle the safety of life at sea, property and the environment. In this sense ships and their crew should be able to detect and act in case of a cyber-attack, in addition to having sufficient training to enable them to comply with the standards of cybersecurity protection demanded by the maritime sector (BIMCO, 2018; USCG, 2017). The objective of this document is based on the need to implement and update the technological changes in the maritime environment, which is why an important base issue arises: the maritime industry is at the real risks of cyber-threats/attacks. Trying to shed light on the issue, we will carry out a study of cyber-security in the maritime field and the degree of knowledge of some of its actors.

1.1. State of the art

Considerable changes have taken place in cybersecurity in recent decades. Many cybersecurity experts believe that malware is the key choice of weapon to carry out malicious intends to breach cybersecurity efforts in the cyberspace (Donaldson et al., 2015; Jang-Jaccard and Nepal, 2014). Internet of Things (IoT) is characterized by heterogeneous technologies, which concur to the provisioning of innovative services in various application domains (Vermesan and Friess, 2013). Moreover, the high number of interconnected devices arises scalability issues; therefore a flexible infrastructure is needed able to deal with security threats in such a dynamic environment (Sicari et al., 2015). Nation-state attacks and attacks against industrial controls and SCADA will become a more frequent and serious threat to both public and private-sector companies. A data breach from an unsecured IoT device in the workplace is predicted to be very likely over the next years, such a breach could be catastrophic (Ponemon, 2018).

There are many studies focused on physical-security aspects and do not adequately consider security processes associated with international supply chains and maritime sector (Acciaro and Serra, 2013; Bichou et al., 2013; Chang et al., 2014). In the maritime supply chain management, it is necessary to perform risk assessments at regular intervals to identify the possibility of cyberattacks that might occur in the future. Polatidis et al., (2018) present a cyberattack path discovery method that is used as a component of a maritime risk management system (Polatidis et al., 2018). Cyber oversight of suppliers is also a challenge, such as when a company uses a third-party data hosting company that works with a fourth-party systems integrator.

2. Methodology

The research was carried out by mailing a questionnaire to maritime professionals from which we will get their degree of knowledge about cybersecurity. This questionnaire was realized in the period of September to December 2018. The questionnaire was structured in 14 closed questions, where the knowledge in cybersecurity and the habitual practices of the respondents were deepened, it is likely to become increasingly difficult to obtain satisfactory results from a voluntary data collection. Finally, we obtained 124 responses to the questionnaire, from which we used 102. One of the main limitations of our study was the lack of participation of the respondents, a situation that did not allow us to get the degree of reliability desired by the survey. The reason has to do with the actors of the maritime sector, which covers a wide range of respondents, so that the survey could have covered a significant sample size that would allow us to obtain reliable results on the knowledge on this matter at a general level. On the other hand, the maritime professionals when receiving the questionnaire via email showed a lack of knowledge or insecurity about the possibility of their computers being infected by a virus (spam), which means that they were reluctant to answer the questionnaire. However one of the most relevant aspects is the lack of connection to the internet of the personnel on board.

3. Cyber-Security

In our days, cyber risk is a subject of such volume that it has an effect on any of the usual activities. Undoubtedly, the speed and weaknesses and risks generated by technological developments, which are of critical importance in the economy, information, etc., expand. The path marked by technology implies breaking with cyber risk and, in general, developing management practices and solutions at all levels (Fig 1). In 2018, 59% of companies in US and the UK said they had experienced a data breach via a third party, but only 35% rated their third-party risk management program as highly effective (Ponemon, 2018).

According to the International Telecommunications Union (ITU), cybersecurity is the set of tools, policies, security concepts, security safeguards, guidelines, risk management methods, actions, training, best practices, insurance and technologies that can be used to protect the assets of the organization and users in the cyber-environment. These assets and users are the connected computing devices, the users, the services or applications, the communication systems, the multimedia communications and the information in its entirety transmitted or stored in the cyber-environment (ITU, 2018).

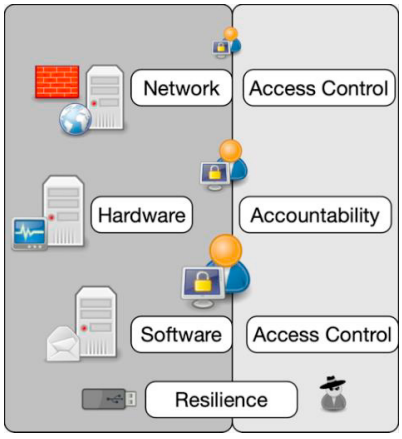

Fig. 1. Cyber threats.

3.1. Cyber-attacks

Cyber-attacks are illegal actions that are carried out through computer channels or that aim to destroy and damage computers, electronic media and internet networks, as well as management and organization systems. Premeditated and politically motivated attacks against information, computer systems, computer programs and data that may result in violence against non-combatant targets by subnational groups or clandestine agents.

There are three basic types of cyber-attack, from which all others derive: confidentiality, integrity and availability. A cyber-attack is not an end in itself, but an extraordinary means to a wide variety of purposes, limited primarily by the imagination, adaptation and interest of the attacker, which can be the espionage, propaganda, denial-of-service, data modification and infrastructure manipulation. Internal threat is related, among others, to crew members, provider, service, etc. The following Table is applied for two different types of attacks. Firstly, for a relevant attack in the present or the past. Secondly, for a potential attack in the future (CyberRoad, 2015).

Table 1. Cyber-threats in shipping industry. Source: Adapted from (CyberRoad, 2015).

Attack Name	
Attacker	Organized group; Espionage group or Industrial competitors; Insider; Phisher; Spyware/malware attacker; Terrorist; Activist; Others.
Resources / Knowledge	Depending on the attacker and target
Source Sectors	Commercial source; local or national government; individual user; Others.
Type of Attack	Spam; phishing scheme; spyware; malware; exploit; botnet; backdoor; ransomware; social engineering; clumsy behavior; misinformation; physical; damaging; insider attacks; Others.
Fundamental Motivation of Attack And Objectives	The challenge; political; industrial; espionage; financial drivers; governmental reasons; vengeance; reputation; stalking; verification of systems to improve them; unintentional; religious and ideological; Others. Data/Information (selling, publication, staling, destruction, etc.); interruption/disruption CI or economies; shipment/cargo (fraudulent, traffic, etc.)
Target	Industry; finance; government / national; military; private/individuals; Others.

The variety and complexity of cyber-attacks depends on the motivation and the time necessary for its execution, among which stand out: Malware, Virus, Worm, Trojans, Spyware, Spoofing, Phishing, Ransomware, etc. Malware refers to a broad class of attacks that is loaded on a system, typically without the knowledge of the legitimate owner, to compromise the system to the benefit of an adversary.

The continued increase in cyber-attacks, along with the security breaches caused by them, is motivating a significant investment in cybersecurity. Cyber-attacks are derived from several partial costs: direct economic, service, reputation and image, penalties, etc. The financial cost of cybercrime for companies has increased by 27.4% in 2017 compared to 2016. Cybersecurity Ventures predicts cybercrime will cost the world in excess of $6 trillion annually by 2021 (Cybersecurity Ventures, 2019). This cost varied according to the modality, but the main affectations suffered by large companies by cybercrime are caused by malware, attacks on web pages, denial of services, leakage of information through active or former employees, malicious codes that open access to corporate platforms, phishing, physical theft of electronic devices and a network of infected computers remotely controlled by a hacker known as botnets.

4. Maritime Cyber-Security

One of the effects of globalization is the high dependence shown by nations to the use of complex computer systems and global information networks. These systems create the possibility of increasing vulnerabilities and threats that may affect the safety of the maritime sector. The states with interests in the world maritime trade and with the intention of improving the regulation of the critical infrastructures and the dependence at the time of developing a security plan that manage the risks and threats from the port system have shown their recognition to the weaknesses or cybernetic vulnerabilities.

A part of shipping cybersecurity is the policies of exchange of information and collaboration between the actors and governments. Collaboration is vital to identify potentially dangerous risks that could cause critical infrastructure damage and a significant negative effect on the environment, economy or safety. The sectoral structure of freight and passenger transport by sea needs dynamic supply chains. However, in the field of cybersecurity the sectoral interdependencies and massive interconnectivity make risk. In particular, a global image of the possible threats and the spectrum of threats and their various cascading effects that are associated with security incidents, see Fig. 2.

Fig. 2. Maritime critical information infrastructure. Source: (CyberRoad, 2015).

4.1. Critical Infrastructures

The European Commission defines the Critical Infrastructure (CI) as an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters or other threats (terrorism, criminal activity, etc.), may have a significant negative impact on the security of the EU and the well-being of its citizens. The sectors to be used for the purposes of implementing of Directive are the energy and transport sectors, for instance, energy, transport (Road transport, Ocean and short-sea shipping and ports, etc.), etc. (EU, 2008). In 2012, the European Programme for Critical Infrastructure Protection (EPCIP) started.The EPCIP has proposed a list of European critical infrastructures based upon inputs by its Member States (EU, 2012). Nowadays, the main goal of the EU is to reduce the vulnerabilities of critical infrastructure and to increase their resilience.

Thus, the European Commission Directive on the Security of Network and Information Systems, which requires critical infrastructure operators, and specifically information technology providers, to take adequate measures to manage risk, report security incidents to national authorities and provide early warnings of threats (EU, 2016). Infrastructures are interconnected not only across national and continental boundaries. There exist the interconnections and interdependencies between infrastructure sectors, and the supply chain (Fig. 3). Interconnections between infrastructures add a challenge to risk treatment in case of the infrastructure's vulnerability and complexity (Rinaldi S., Peerenboom J., 2001).

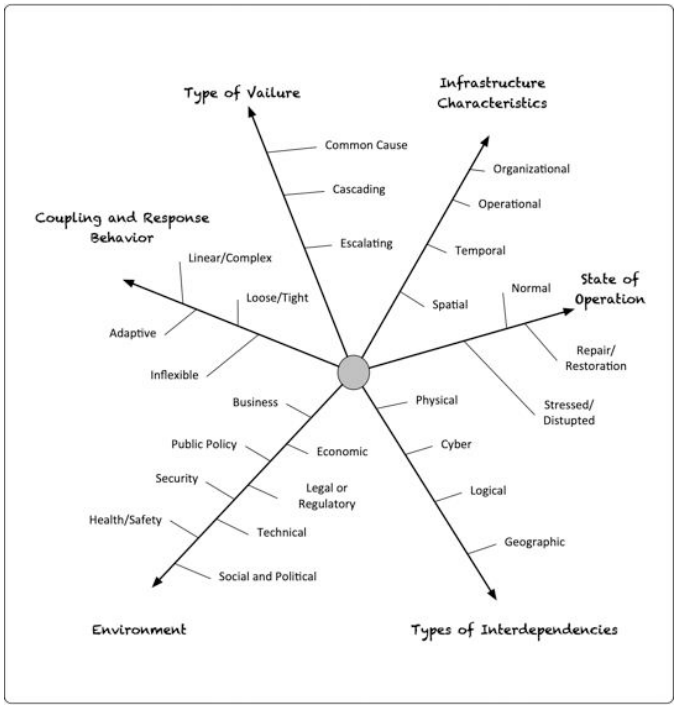

Fig. 3. Understanding and Analyzing Critical Infrastructure Interdependencies. Source: Adaptation from (Rinaldi et al., 2001).

4.2. The role of IMO

The International Ship and Port Facility Security (ISPS) code regulates the ship security analysis that must be performed by ship owners and operators. The code was developed in the aftermath of the terrorist attacks on the United States on September 11th, 2001 (IMO, 2002). The concern regarding cybersecurity in the maritime sector has been increasing in recent years, which is why the International Maritime Organization (IMO) has decided to act in this area, implementing regulations and providing guidelines for industry professionals to have knowledge on how to prevent and act in a cyber-attack.

The IMO, understands the cyber risk in the maritime sector as the degree to which a technological asset can be potentially threatened, suffer failures related to transport operations and cargo handling in terminals or failures in security, because of which the systems have been damaged by some type of virus. Risk management is fundamental for the safe operation of maritime transport and this has been focused mainly on the physical security regulated by the ISPS Code. To carry out cybersecurity risk management, the IMO proposes an approach based on five functional elements: identify, protect, detect, respond and recover.

In 2016, in accordance with ship owners and operators (BIMCO) published in collaboration with CLIA, ICS, Intercargo and Intertanko a guide, which highlights both the dimension of cyber risk in the maritime sector and the need to carry out an assessment of these risks with the milestones recommended by the National Institute of Standards and Technology of the Department of Commerce of the United States (NIST) (BIMCO, 2018). The aforementioned guide makes use of the ISO27001 standard for cybersecurity management. This standard belongs to the group on cybersecurity ISO27000 which is applicable to all types of organizations and they are recognized guides in the cybersecurity sector. It is the best-known standard in the ISO 27000 family that provides the requirements for an information security management system (ISMS) and code of practice for information security controls (ISO, 2009).

4.3. Cyber-threats

Cyber criminals have economic objectives and cause economic damages to state, installations, companies and individuals. Stealing data or modification information for their own benefit. Not all institutions or companies disclose these incidents, since this damages their image. However, Hacktivist activities usually block institutions to highlight some adverse phenomena to society. They usually do not cause serious economic damages.

The cyber criminal's threat in the twenty-first century is testing the maritime sector. The maritime industry and the CI should be aware of the catastrophic result that the ship's systems were controlled by cybercriminals, which could result in collisions, pollution, grounding, the interruption of port operations or an incendiary device. At present, the authorities and the industry itself is not prepared to give an effective response to any of the threats posed. Ships in port represent another component of port infrastructures that must be protected. All coastal States must have the ability to monitor all the ships that enter its CI in order to validate whether they are cyber clean, in convergence with supply chains, port operations and information technology (Fig. 4).

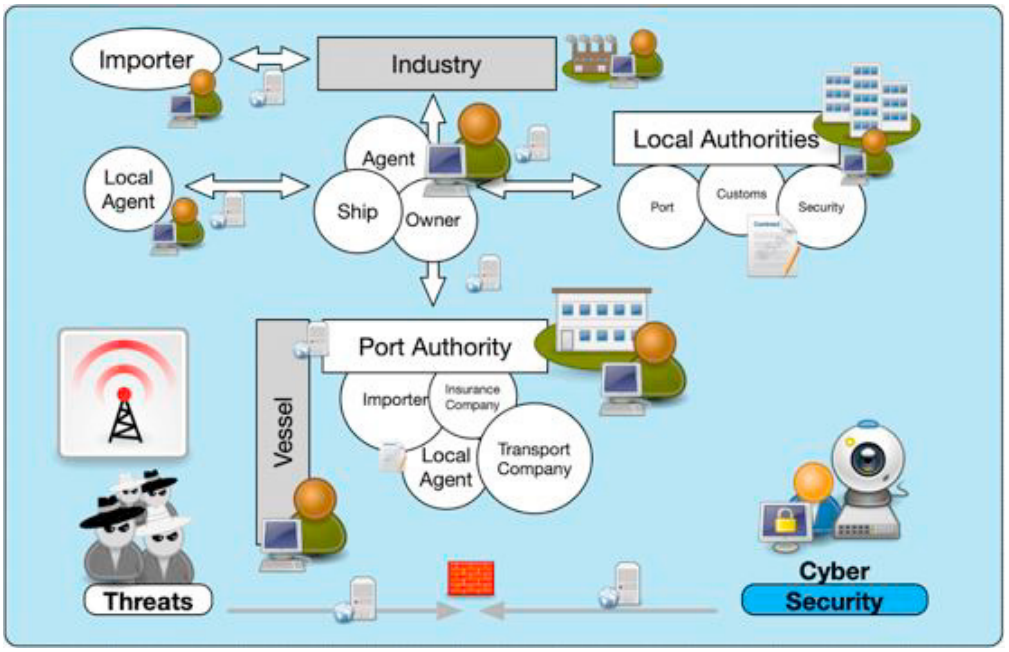

Fig. 4. Understanding and Analyzing Critical Infrastructure Interdependencies.

4.4. Cyber-attacks on board

In the maritime sector and more specifically in maritime navigation, the vulnerability of certain navigation systems has been revealed, where cyber-attacks introducing false signals that overlap with the actual location of ships or represent nonexistent emergencies. These circumstances are aggravated by the increase in the use of technology to control navigation, engines, cargoes, etc., as well as by the use of dynamic positioning, ship-to-shore interfaces, control of propulsion systems or opening and closing of cargo valves, passenger boarding systems, etc. It is necessary to consider that the human factor plays a fundamental role in the effectiveness of the cyber-attacks as a significant vulnerability element for companies. Therefore, the primary barrier of any critical installation and of the vessel itself is its personnel/crew and their readiness and preparation against cyber-attacks

According to the IMO, 2017), the most vulnerable systems to suffer attacks through the network are: cargo and element handling systems; the propulsion systems and the power management and control machinery; access control systems; passenger administration and management systems and communication systems. The handling systems of loading and unloading of cargo that belong to the supply chain of ports and ships is one of the targets of attack for hackers, since these are the key of the good functioning and coordination of the loading and unloading of the ships and compliance of their respective lines in time -. The forms of attack to these systems are manifested as: manipulation and sabotage; falsification; piracy and robbery; destruction; alteration and deviation.

The AIS (Automatic Identification System) used in the tracking and location of ships worldwide is one of the electronic devices vulnerable to potential cyber-attacks. This device operates using coordinates given by a GPS and exchanges data on the position of a ship, its course as well as exchanges information with the ships and installations of other ships that are sailing in the area either in the high seas or off the coast.

In 2010, a marine drilling platform changed its location from South Korea to South America on monitoring systems due to the attack of a computer virus. In August 2011, a group of hackers infiltrated the servers of IRISL (Iranian Shipping Line) and damaged hundreds of data about cargoes, dates and places of delivery. In June 2011, cybercriminals had taken control of their systems in the port of Antwerp by seriously violating them. Europol (European Cybercrime Centre EC3) reported on June of 2013, that they had been victims of an attack directed by a drug cartel to introduce drugs in Europe for two years. The criminal group used cyber-experts and took control of the computer systems of harbor logistic companies and container terminals (Europol, 2013). In 2017, the MAERSK shipping company and which is still affected as we discussed earlier in which the "PETYA" virus massively affected the global navigation. There are two categories of cyber-attacks that may affect either land companies or ships. On the one hand, unmanaged attacks when a company or the systems and data of a ship are one of the many potential targets. On the other hand, directed attacks where a company or the systems and data of a ship are the objective that is intended to be achieved.

4.5. Maritime cybersecurity survey

This study was aimed to design a survey about the impact that knowledge and training of different parties of maritime industry would have on cybersecurity, the results of which being weighed against research results. We started with an initial survey followed by further questionnaires where participants of the first round were invited to complete at least one. Answers from the first survey were used to generate more specific questions in the following rounds. The main area of the survey focusses on maritime industry attacks. The professional profile of the participants is the following: Terminals and ports (40.5%), Ships (43.8%) and other sectors (15.7%). 33% of the respondents show that they had suffered some type of cyber-incident in the last year, this figure in accordance with the growth of cyber threats in the sector. Besides 40% of users share passwords between them and does not make any type of preventive measures (email, USB, web, etc.). On the other hand, it is very common to work on personal devices.

The lack of knowledge of maritime experts consulted exceeds 75%, where it is essential to highlight, among other topics: procedures (detect, act, communicate, recover, etc.); simulacra; cyber security/threats. It is revealing that respondents in a high percentage see in the implementation of technological systems the solution to cyber-threats in the sector. Position that eludes the responsibility of the operator or responsible for the management.

5. Conclusion

The analysis of critical infrastructures and cyber-security in this study shows that the dynamics of maritime sector exhibit vulnerabilities and critical components. However, to understand the cyber-attacks in the maritime field presents greater challenges when the dimension of the problem remains highly unidentified. In this internet age and post-globalization of maritime transport, with the digital transformation of the logistics chain and its different components, we must strengthen the resilience of its fundamental elements. Being vaccinated against a certain disease does not prevent the growth or spread of other possible threats. In others words, having an antivirus does not make you magically immune to threats. The key is usage. Nowadays, there is a gap between the practices of actors in maritime industry and the vulnerability of systems. It becomes essential to improve training and the implementation of innovative solutions.

Therefore, it is necessary to strengthen training levels in the maritime sector and the port interface connection with the supply chain. The implementation of cybersecurity training system and the development of cyber resilience agendas shows possible application of the system in marine environment. In current cyber-world reality is infiltrated by different and mostly not yet detected advanced security threats. This could bring shipping companies, their supply chains actors and users the advantage of solving crisis caused by possible cyber-attack.

Acknowledgements

The authors gratefully acknowledge the valuable input from experts in the maritime sector. The authors also wish to thank the editor and anonymous reviewers for their helpful feedback on this paper.

References

Acciaro, M., Serra, P., 2013. Maritime supply chain security: a critical review. IFSPA 2013, Trade Supply Chain Act. Transp. Contemp. Logist. Marit. Issues 636.

Bichou, K., Bell, M., Evans, A., 2013. Risk management in port operations, logistics and supply chain security. CRC Press.

BIMCO, 2018. Guidelines on Cyber Security Onboard Ships. Bagsværd, BIMCO.

Chang, C.-H., Xu, J., Song, D.-P., 2014. An analysis of safety and security risks in container shipping operations: A case study of Taiwan. Saf. Sci. 63, 168–178.

CyberRoad, 2015. Development of the CYBER crime and CYBER terrorism research ROADmap, D4.4.

Cybersecurity Ventures, 2019. 2019 CyberVentures Cybercrime Report, Herjavec Group.

Donaldson, S.E., Siegel, S.G., Williams, C.K., Aslam, A., 2015. Defining the cybersecurity challenge. Springer, pp. 3–25.

enisa, 2011. Analysis of cyber security aspects in the maritime sector, European Network and Information Security Agency (enisa). Brussels.

EU, 2016. 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. (OJ L 194, 19.7.2016, p. 1–30). Brussels, Belgium.

EU, 2012. European Commission: Commission staff working document on the review of the European Programme for Critical Infrastructure Protection (EPCIP), 22.6.2012 SWD (2012) 190. Brussels, Belgium.

EU, 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 (OJ L 345, 23.12.2008, p. 75). Brussels, Belgium.

Europol, 2013. Cyber Bits - Hackers Deployed to Facilitate Drugs Smuggling, 30 June 2013. Hague.

IMO, 2017. Circular MSC-FAL.1/Circ.3, Guidelines on Maritime Cyber Risk Management, issued 05 July 2017. London (UK).

IMO, 2002. The international ship and port facility security code. In: SOLAS (Chapter XI-2). London (UK).

ISO, 2009. Information Technology, Security Techniques, Information Security Management Systems, Overview and Vocabulary, International Organization for Standardization (ISO). Geneva, CH.

ITU, 2018. Global Cybersecurity Index 2017. International Telecommunications Union (ITU),. Geneva, CH.

Jang-Jaccard, J., Nepal, S., 2014. A survey of emerging threats in cybersecurity, in: Journal of Computer and System Sciences. pp. 973–993.

Jensen, T., 2017. Cyber attack hits shipper Maersk, causes cargo delays - Reuters [WWW Document]. URL https://www.reuters.com/article/us-cyber-attack-maersk/cyber-attack-hits-shipper-maersk-causes-cargo-delays-idUSKBN19J0QB (accessed 4.19.19).

Polatidis, N., Pavlidis, M., Mouratidis, H., 2018. Cyber-attack path discovery in a dynamic supply chain maritime risk management system. Comput. Stand. Interfaces 56, 74–82.

Ponemon, 2018. Study on Global Megatrends in Cybersecurity, Ponemon Institute: Research Report. Michigan.

Rinaldi S., Peerenboom J., K.T., 2001. Identifying Understanding and Analyzing C I Interdependencies. EEE Control Syst. Mag. 11–25.

Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A., 2015. Security, privacy and trust in Internet of Things: The road ahead. Comput. Networks 76, 146–164.

UNCTAD, 2018. Review of Maritime Transport 2018, The United Nations Conference on Trade and Development. United Nations Pub, Geneva.

USCG, 2017. Guidelines for Addressing Cyber Risks at Maritime TS Act (MTSA). Regulated Facilities by NVIC 05-17. Washington, DC.

Vermesan, O., Friess, P., 2013. Internet of things: converging technologies for smart environments and integrated ecosystems. River Publishers.