Ahokas, Jenna; Kiiski, Tuomas; Malmsten, Jarmo; Ojala, Lauri M.

**Conference Paper**

# Cybersecurity in ports: A conceptual approach



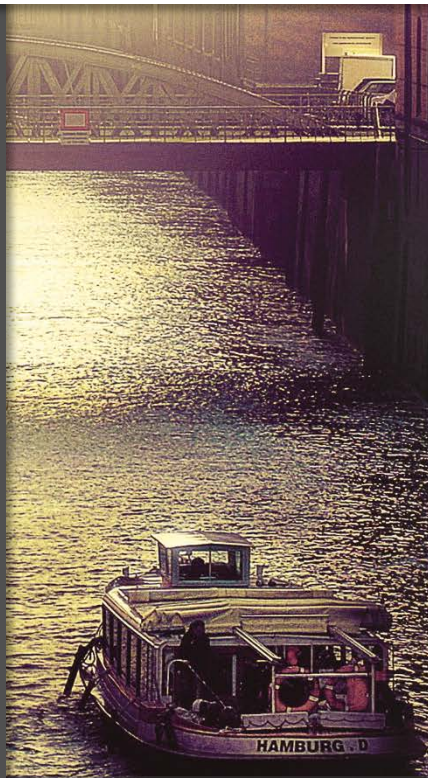
*Suggested Citation:* Ahokas, Jenna; Kiiski, Tuomas; Malmsten, Jarmo; Ojala, Lauri M. (2017) : Cybersecurity in ports: A conceptual approach, In: Kersten, Wolfgang Blecker, Thorsten Ringle, Christian M. (Ed.): Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg International Conference of Logistics (HICL), Vol. 23, ISBN 978-3-7450-4328-0, epubli GmbH, Berlin, pp. 343-359, https://doi.org/10.15480/882.1448

Proceedings of the Hamburg International Conference of Logistics (HICL) – 23

Jenna Ahokas, Tuomas Kiiski, Jarmo Malmsten, Lauri Ojala

# Cybersecurity in Ports: a Conceptual Approach

HICL






Published in: Digitalization in Supply Chain Management and Logistics
Wolfgang Kersten, Thorsten Blecker and Christian M. Ringle (Eds.)
ISBN 9783745043280, Oktober 2017, epubli

# Cybersecurity in Ports: a Conceptual Approach

Jenna Ahokas[1], Tuomas Kiiski[1], Jarmo Malmsten[1], Lauri Ojala[1]

1 – Turku School of Economics at the University of Turku

*As the world is becoming increasingly digitalized, the role of cybersecurity on society is mounting. Recent cyberattacks have showed the vulnerability of critical infrastructure, including ports. The objective is to describe how cybersecurity is perceived in ports, as preparedness and regulation for cyberthreats in ports appears inadequate. The study is a conceptual analysis built upon a comprehensive literature review. The results show that regardless of the growing awareness of the issue, much work needs to be done in order to mitigate the cyberthreats in ports. Situation calls for, among other things, adoption of industry standards and practical level coordination.*

*Cybersecurity in general has been a topical subject, while in the context of ports the theme has thus far been scantly studied. In addition, cybersecurity is currently not included in International Maritime Organization's safety and security Conventions relevant to port, such as ISPS or ISM. Hence this study is among the first openings in its field.*

**Keywords:** Cybersecurity; Maritime Security; Critical Infrastructure; Ports

# 1 Introduction

The world is rapidly becoming digitalized and dependent on efficient communication systems. The activities, which traditionally have relied on paper documentation or manual processing, are now increasingly converted into electronic format, where data is stored in a digital environment called cyberspace (Goldby, 2008; Fitzgerald, et al., 2013). For business, the implications of these changes are massive by any standards, including improved data integrity, processing capacity and emergence of new business models (Boyes, Isbell and Luck, 2016). Some have even visioned a dawn of the fourth industrial revolution (Lasi, et al., 2014).

Downside of this development is that reliance on technology makes society susceptible to the functionality of systems (Urcioli, 2015; Carrapico and Barrinha, 2017). Along with natural disasters and terrorism, malicious acts by individuals through cyberspace on essential systems have been underlined as a potential threat to the society (Kapto, 2013). The motive behind cyberattacks are diverse, including excitement, money and political agendas (Ahokas and Kiiski, 2017). Assuring the resiliency of society against cyberattacks requires focusing on cybersecurity of critical infrastructure. Cybersecurity indicates the security of cyberspace in terms of access to, and control and storaging of data (Boyes, Isbell and Luck, 2016).

The concerns relating to cybersecurity have already materialized as the number of cyberattacks have shown a year-by-year increase, causing substantial financial losses to society in general and business in particular (Colesniuc, 2013). Hence cybersecurity has been identified as a top-level priority among policymakers, businesses, scholars and individual persons (Lewis, 2002). As a result, adoption of specific cybersecurity strategies have been initiated (ICC, 2015).

Ports are key nodes of global trade — approximately 80 per cent of world trade is transported by sea — and thus comprise an integral part of critical infrastructure (UNCTAD, 2016). In addition, ports hold substantial amounts of data, are involved in a large number of monetary transactions and stakeholders making them attractive objects for cyberattacks (CyberKeel, 2014; Jensen, 2015).

European Network and Information Security Agency (ENISA 2011) was one of the first to identify a lack of awareness of cybersecurity in maritime transport and ports. Despite substantial academic interest shown towards cybersecurity in general (Hult and Sivanesan, 2013) as well as maritime security (Germond, 2015), cybersecurity in ports seems far more uncharted an area (Ahokas and Kiiski, 2017).

Fresh empirical evidence from the Baltic Sea Region indicates that preparedness and regulation for cyberthreats in seaports appears inadequate (Ahokas and Laakso, 2017).

Concerns about cybersecurity have risen relatively recently, which is evidenced by the fact that cybersecurity is currently not mentioned in the International Maritime Organization IMO's safety and security Conventions relevant to ports, such as International Ship and Port Facility Security Code (ISPS) or International Safety Management Code (ISM). Apart from IMO's Interim guidelines on cybersecurity published in 2016 in Maritime Safety Committee's (MSC) Circular MSC.1/Circ.1526, there are no supranational guidelines how to tackle the issue.

However, IMO is making cyber risk management onboard ships mandatory as of 1 January 2021, as cited in Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems adopted in June 2017. The resolution states that an approved safety management system should take cyber risk management into account in accordance with the objectives and requirements of the ISM Code. Based on the recommendations in MSC.1/Circ.1526 Guidelines on maritime cyber risk management, the resolution confirms that existing risk management practices should be used to address the operational risks arising from the increased dependence on cyber enabled systems.

Thus, the gap of knowledge on cybersecurity in ports identified above merits further investigation on the topic. For this purpose, this paper reviews the key elements and aspects of cybersecurity with the focus on ports. A conceptual analysis is conducted through a comprehensive literature review aiming to address the following research question: "How is cybersecurity perceived in ports?"

The paper is divided as follows: Section 2 contains a discussion regarding security from the perspective of ports. Section 3 elaborates the key concepts and issues related to cybersecurity. Section 4 provides insights on cybersecurity in ports. Section 5 sums up the results and draws conclusions.

## 2 Security Aspects in Ports

Risk, threat and security are essential concepts when scanning any business environment. By definition, a risk is a likelihood of an event with potentially either positive or negative consequences (Prezelj and Ziberna, 2013). According to Merriam-Webster dictionary a threat is "an expression of intention to inflict evil,

injury, or damage" (Merriam-Webster, 2017). Security is a concept with multidimensional meanings (Brooks, 2010), which is often addressing intentional threats in contrast to ones with accidental or natural origin (Craigen, Diakun-Thibault, and Purse, 2014). A difference between risk and security is that the latter involves also uncertainty (Marlow, 2010).

Maritime community, with its operating field encompassing around the globe, is susceptible to various types of threats. This turns the focus on maritime security, a concept of which has recently gained buzzword status among the policymakers (Bueger, 2015). Maritime security can be seen either as a state of security within the maritime domain or as a vehicle to mitigate risk of threats, for example, terrorism, piracy or smuggling, taking place not only on traditional sea or port locations, but also along the entire supply chain (Helmick, 2008; Germond, 2015).

Characteristics of a port make it challenging object from the security perspective. A port is a complex and multipart organization with institutions and functions crossing multiple layers (Baltazar and Brooks, 2007). A port usually consists of a port authority, port superstructure, for example cranes and conveyors, and infrastructure, loading and unloading operations, storage facilities, and intra-port operations (Brooks and Cullinane, 2007; Meersman and Van de Voorde, 2010).

From the national security perspective, ports, together with energy systems, transport infrastructure, health industry, and water supply facilities, comprise critical infrastructure (Ho and Ho, 2006; Prezelj and Ziberna, 2013). Critical infrastructure refers to facilities, networks, and assets, which are essential in terms of citizens' health, safety, security, and economic well-being as well as effective functioning of society (Carrapico and Barrinha, 2017).

Typical threats of ports include, but are not limited to, financial losses, theft of cargo or information, and strikes or system malfunctions that can compromise the operations of a port (Ho and Ho, 2006; Loh and Thai, 2015). Moreover, in light of the recent surge of activity, threat of terrorism should not be neglected. One scenario suggests that terrorist may target or use ships at sea or in ports as weapon to attack passengers and personnel of ports (Eski, 2011). Owing to technological development, a new kind of threats have emerged as digitalization has enabled threats coming through cyberspace to become reality (Rittinghouse and Hancock, 2003; Geers, 2009; Miron and Muita, 2014).

Port security related policymaking is traditionally driven by global shocks. For example, repercussions of 9/11 terror attacks led to global adoption of IMO's ISPS Code. The ISPS aims to enhance maritime security both on ships and in

ports (Pinto and Talley, 2006; Thai and Grewal, 2007). Adoption of such initiatives comes with a price, of which are usually put on shipper's account (Dekker and Stevens, 2007). However, policies pursued by the major players persists fragmented (Papa, 2013). For example, the USA adopted national policies such as Container Security Initiative, which differs from global standards (Marlow, 2010).

# 3 Key Concepts and Issues Related to Cybersecurity

The literature behind cyber-related issues is arguably embedded with various cyber-prefixed concepts, of which are often used interchangeably (Bayuk, et al., 2012). In order to make clarity in this complex field, the first part the Section provides a conceptual image of the process involving concepts related to cybersecurity. The remainder of the Section contains elaborate definitions of the concepts in question.

## 3.1 Conceptual Illustration

Figure 1 provides a simplified process description of the relevant concepts and their mutual relationships. In a nutshell, conceptual description of the role of cybersecurity (C) is as follows. All action is taking place in cyberspace (A), where system (B; here e.g. the IT systems of a port community) is located. It is protected by cybersecurity (C). System vulnerabilities (D) together with existing cyberthreats (F) and the level of cybersecurity (C) comprise the level of cyberrisk (E) at any given time. In case cybersecurity (C) is not at an adequate level, cyberrisk (E) may materialize through a cyberattack (G), which targets the system (B) through an identified vulnerability (D). In practice, a cyberattack (G) can be considered as a materialized cyberthreat (F), which contains also specific technical methods to inflict damage.

## 3.2 Definitions

According to Rantapelkonen and Kantola (2013, p.25) cyberspace is "the collection of computing devices connected by networks, in which electronic information is stored and utilized, and communication takes place".

Merriam-Webster dictionary defines cybersecurity as ”measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack” (Merriam-Webster, 2017). In other words, the objective of cybersecurity is a stable condition, where cyberspace is trusted and protected. At this point, there is also sufficient capacity to proactively control and sustain cyberthreats (Ministry of Defence of Finland, 2013; Limnéll, Majewski and Salminen, 2015).

Vulnerability refers to a feature or weakness of a computer or data system's design, integration, and maintenance (Maurushat, 2013). Vulnerability can either be direct such as weak passwords that lead to unauthorized access, or indirect such as the absence of network segregation (IMO, 2016a). Spotting the vulnerabilities requires great precision as it is estimated that over 90 per cent of attackers are familiar with the vulnerabilities of their targets (Afful-Dadzie and Allen, 2014; Loukas, 2015). According to Maurushat (2013) vulnerabilities can be divided into three categories: 1) known vulnerability, 2) zero-day attack, and 3) future threat.

A known vulnerability is noticed in public through some form of communication such as publication, and refers to failure of existing paradigms for recognizing, reacting to or mitigating vulnerabilities. A zero-day attack refers to utilization of a security vulnerability on the same day, when it becomes generally known. A future threat means a condition that could end in harm as a consequence of a formerly unknown security vulnerability. Vulnerabilities are increasing e.g. due to i) shift of society towards on ubiquitous and automated computing environment; and ii) increased utilization of the Internet (Lewis, 2002).

Cyberrisk refers to a variety of different sources of risk affecting the information and technology assets of a firm (Biener, Eling and Wirfs, 2015). In more detail, realized risks may result financial losses, disruption or damage to the reputation of an organization from some sort of failure of its information technology systems (IRM, 2014).

The growth of digitalization has entailed increase in frequency, sophistication and scope of cyberthreats (Chertoff, 2008). A cyberthreat refers to a malicious attempt in cyberspace, which aims to damage or interrupt a computer network or system (Boyes, Isbell and Luck, 2016). Five basic types of cyberthreats are hacktivism, cybercriminality, cyberespionage, cyberterrorism and cyberwar (table 1). Each of them has their individual features relating to actors involved, as well as motivations and objectives behind actions.

Hacktivism refers to operations in cyberspace that make use of various hacking techniques to invade into web pages and on computers, and create pressure

Table 1: Types and elements of cyberthreats

| Cyberthreats | Actors | Motivations | Objectives |
|---|---|---|---|
| Hacktivism | Hacktivists<br>Hackers<br>Individuals | Egoism<br>Political<br>Reputation | Attention<br>Disruptions<br>Knowledge |
| Cybercriminality | Individuals<br>Industrial spies<br>Organized crime | Economical<br>Informational | Cargo<br>Digital assets<br>Organizational data |
| Cyberespionage | Industrial spies<br>Governments<br>Organized crime | Ideological<br>Informational<br>Political | Digital assets<br>Knowledge<br>Organizational data |
| Cyberterrorism | Governments<br><br>Terrorists | Ideological<br>Political<br>Religious<br>Social | Disruptions<br>National institutions<br>Critical Infrastructure |
| Cyberwar | Governments<br><br>Terrorists | Egoism<br>Political<br>Religious<br>Social | Military<br>National<br>Critical |

on a certain object (Limnéll, Majewski and Salminen, 2015; Boyes, Isbell and Luck, 2016). A hacker uses own quick programming skills for invading into a computer network file and seeks recognition for his/her technological capabilities (Christou, 2016). Hackers can be divided into three different groups (Rittinghouse and Hancock, 2003; Kapto, 2013):

1. White-hat hacker aims to promote security with his/her actions
2. Grey-hat hacker, often with criminal background, seeks gaps and vulnerabilities
3. Black-hat hackers, i.e. a hacktivist, has criminal intentions

Cybercriminality refers to criminal activities that involve computer and information systems either as a primary tool or as a primary target (Christou, 2016; Carrapico and Barrinha, 2017). The aim is to gain financial benefits or to inflict personally motivated harm such as revenge or bullying (Gross, Canetti and Vashdi, 2017). The economic benefit of cybercriminality can include criminal damage, robbery of cargo, or identity thefts (European Commission, 2013; Boyes, Isbell and Luck, 2016). Cybercriminality can be divided into four categories (Limnéll, Majewski and Salminen, 2015; Luppicini, 2014):

1. Actions endangering confidentiality, integrity and availability of data and systems
2. Forgery or identity thefts
3. Illicit gambling or spreading false information
4. Copyright or brand violations

Cyberespionage refers to illegal access to secret and delicate information such as company strategy, private information, or intellectual capital, and it aims for getting competitive advantage (Rittinghouse and Hancock, 2003; Boyes, Isbell and Luck, 2016). Five different losses can be seen as a consequences of cyberespionage (Platt, 2011; Fitzpatrick and Dilullo, 2015):

1. Loss of intellectual property, business and customer information
2. Extra costs due to interrupted business plans and competitive exercises
3. Loss of profits and efficiency
4. Damage to company reputation

5. Increased IT related security costs

Cyberterrorism is defined by Limnéll, Majewski and Salminen (2015, p.131) as ”a deliberate politically motivated attack against information, computer systems, computer software, and databases in the form of a violent invasion by international groups or secret agents”. Cyberterrorist is an individual, who is specialized in hacking into computer systems and is competent in organizing individual cyberattacks on global networks (Kapto, 2013).

Cyberwar is a part of modern information war between nations, during which cyberattacks are made against opponents computer networks, which are relevant from the military perspective (Lewis, 2002; Ministry of Defence of Finland, 2011; Kapto, 2013). Cyberwar employs malicious software and viruses to disable military targets (Gross, Canetti and Vashdi, 2017).

In case cyberrisks are realized, a cyberattack will take place, which has the basic elements of cyberthreats in relation to actors, motivations and objectives. The exact methods used by cyberattackers vary, while the most common ones are phishing, malicious software and Denial-of-Service attack. (Colesniuc, 2013; CyberEdge Group, 2016). Phishing is an attempt to gain discrete information by imitating a reputable enterprise or person in e-mail or other communication channel. Malicious software or malware is a harmful program to steal, encrypt, delete or change data, hijack or monitor users of target computer (Kendrick, 2010). A Denial-of-Service (DoS) attack is an attempt to overtake a network by blocking it with huge amount of communication (Fok, 2015).

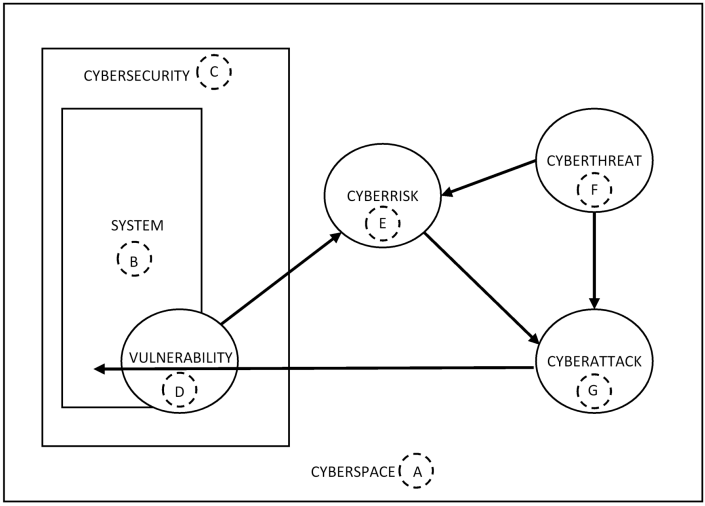



Figure 1: Simplified process chart of concepts related to cybersecurity

# 4 Cybersecurity in Ports

ENISA's study in 2011 on cybersecurity in maritime transport and ports identified a clear lack of awareness on cybersecurity issues (ENISA, 2011). However, this has not resulted in any European-wide strategy or coordinated action on the topic. As mentioned in Section 2, critical infrastructure, including ports, constitutes a likely target for cyberattacks given its significance on the functionality of societies. In addition, what makes ports particularly vulnerable to cyberthreats relates to their basic characteristics: dependency of data systems, handling massive volumes of cargo or passengers , high monetary values, immense number of transactions, numerous stakeholders involved, as well as non-transparent ownership of goods end equipment (see e.g. Jensen, 2015). The geographical location may also be influential as cyberattackers have been noted to target operators inside ports, where the level of preparation tends to be low (Miron and Muita, 2014).

Potential consequences of cyberattacks against ports can be harmful in many ways. The most common ones are scenarios, where cyberattackers gain access to one or more of the following: i) overtake control of a ship, ii) shut down the entire port, iii) delete or alter operational data, or iv) access to delicate information (CyberKeel, 2014).

In response to a growing pressure for countermeasures against cyberthreats, policymakers throughout the world have started the adoption of multilevel general cybersecurity strategies. Examples of these is the United Kingdom's National Cyber Security Strategy 2016–2021 (UK, 2016) at a national level, and the Cyber security strategy of European Union: an Open, Safe and Secure Cyberspace (European Commission, 2013) at a supranational level.

Similarly, work has begun among maritime authorities and international organizations to develop strategies and standards for port facilities and ships against cyberthreats. However, there are some challenges in this process. When designing maritime specific guidelines, the globalized nature of the business and large number of stakeholders set requirements for policy development. For example, operations of a large container shipping company can easily involve over 100 countries, and its fleet size be measured in several hundreds of vessels (Jensen, 2015). Global coordination and standardization of practices are essential elements in this regard. So far none of the maritime specific guidelines are not mandatory by nature, which may hinder the adoption process.

In 2015, the United States Coast Guard (2015) introduced its Cyber strategy (for critical maritime infrastructure). The Institution of Engineering and Technology (IET) introduced in 2016 the Code of Practice (Boyes, Isbell and Luck, 2016).

In 2016, the Baltic and International Maritime Council (BIMCO), the International Chamber of Shipping (ICS), INTERCARGO, INTERTANKO and the Cruise Lines International Association (CLIA) published "Guidelines on Cyber Security Onboard Ships" (BIMCO, et al., 2016). The guidelines introduced a six-step approach, which is dedicated to cybersecurity and cyberthreats:

1. Identification of external and internal cyberthreats
2. Identification of vulnerabilities
3. Assessment of risk exposure
4. Development of protection and detection measure
5. Establishment of contingency plan
6. Response to cybersecurity incidents

In 2016, IMO published the "Interim Guidelines on Maritime Cyber Risk Management", which underlines that cyberrisk management should be complementary to existing security and safety risk management requirements, like ISM and ISPS Codes (IMO, 2016a). The objective of IMO's guidelines is to keep cyberrisks at a reasonable level by using multilevel approach that involves all relevant port actors (IMO, 2016a).

By and large, the number of reported cyberattacks against ports has remained on a very low level thus far. The only case, which has received wider attention, was the attack against port of Antwerp in late-2013 (Boyes, Isbell and Luck, 2016). The exact reasons behind absence of attacks can only be speculated. Similarly, the number of attempts is fairly uncertain given that they may not be reported or noticed. It should be remembered that the security situation is constantly evolving — what was adequate yesterday may not hold today.

There is very limited amount of publicly available information about contemporary cybersecurity related practices in ports, which is presumably due to discretionary nature of the subject. However, initial empirical evidence from the Baltic Sea Region indicate that neither ports nor regulation seem to be well prepared to cyberthreats (Ahokas and Laakso, 2017).

Moreover, it appears that other maritime industry sectors are not neither that well prepared against cyberthreats. In mid-2017, there was a cyberattack against the world's largest shipping line, Maersk, which temporarily crippled the entire company (Knowsler, 2017). The episode has explicitly showed that there is still room for improvement in this sector as well.

The notion of ports lesser role in terms of cybersecurity considerations receives support when looking at academic literature, as the number of articles concerning cybersecurity in ports is scarce. In addition, the topic appears recent, i.e. published after 2011. Apart from two peer-reviewed journal articles by Kouwenhoven (2014) and Jones (2015), other dedicated reports are predominantly industry, policy or consultancy papers (Ahokas and Kiiski, 2017). The topic's novelty is convergent with the body of literature, while the scarcity observation is contrasting given the reported influx of studies covering cybersecurity and maritime security in general (Germond, 2008; Jensen, 2015).

# 5 Results and Conclusions

The recent growth of cyberattacks and subsequent increased awareness of cybersecurity, in which ports appeared to be somewhat neglected, provided the ultimate inspirations for this paper. A conceptual analysis, which was based on comprehensive literature review, was conducted. Objective of the paper was to describe cybersecurity in ports by answering to specific research question: "How is cybersecurity perceived in ports?" This was approached by first establishing port's dual role in security as being part of both maritime and national security considerations. After this, the relevant terminology and concepts related to cybersecurity were scrutinized. Finally, state-of-the-art situations about cybersecurity in ports were mapped.

The results show that regardless of the growing awareness of the issues, much work needs to be done in order to mitigate the cyberthreats in ports. The matter is both novel and of great urgency as cyberattacks are becoming more common with pervasive impacts on society. Maritime sector and ports in particular are no exception in this regard as recent attacks against Maersk and port of Antwerp have showed.

There is limited amount of information available about the contemporary cybersecurity related practices in ports, which presumably is due to discretionary

nature of the subject. However, there are indications suggesting that the ports current level of preparation and regulations are not adequate.

Over the past five years, policymakers and other stakeholders have become actively engaged in cyberthreats by adopting cybersecurity strategies and guidelines, for example, IMO (2016a) and BIMCO, et al. (2016). However, mandatory global standards are yet to be introduced, which, among other things, could expedite the adoption process. Owing to the global scale and large number of parties involved, coordinated efforts are needed to ensure adoption of adequate practices and regulations throughout the industry. This supports Helmick's (2008) call for extensive cybersecurity framework. Here, IMO's Resolution adopted in June 2017 to make cyber risk management onboard ships mandatory as of 1 January 2021 is a significant, yet belated step ahead. Similar steps for seaports are still pending.

Unlike popular research streams of maritime security and cybersecurity in general, the port environment in a cyber context appears to have received scant exposure. Only few journal papers appear to have dealt with the topic, while the majority of publications consist of consultancy or policy related papers.

The terminology behind cybersecurity appears far from being harmonized as the use of various concepts with different meanings is common (see also IMO, 2016b). This finding supports previous arguments by Craigen, Diakun-Thibault and Purse (2014) and Hult and Sivanesan (2013). Especially the relationship between cyberthreat and cyberattack is a cumbersome (Kadivar, 2014; Loukas, 2015). In order to provide input to this issue, a conceptual map was introduced that delineates the relationships between different concepts.

This paper contains limitations that needs to be taken into consideration. The major limitation compounds from the novelty of the topic as there is only limited amount of publications and empirical data available. Future research should study port cybersecurity strategies in more detail, for example, by establishing a suitable typology and/or a taxonomy on these preparation plans. In addition, more information is needed about how these strategies have been implemented empirically and how effective they are in terms of mitigating cyberthreats.

## References

Afful-Dadzie, A. and T. T. Allen (2014). "Data-Driven Cyber-Vulnerability Maintenance Policies". In: *Journal of Quality Technology* 46.3, pp. 234–250.

Ahokas, I. and K. Laakso (2017). *Deplhi study on safety and security in the Baltic Sea Region ports*. URL: https://blogit.utu.fi/hazard/.
Ahokas, J. and T. Kiiski (2017). *Cybersecurity in ports*.
Baltazar, R. and M. R. Brooks (2007). "Port Governance, Devolution and the Matching Framework: a Configuration Theory Approach". In: *Devolution, Port Governance and Port Performance*. Ed. by M. R. Brooks and K. Cullinane. London: Elsevier, pp. 379–403.
Baltic and International Maritime Council (BIMCO), International Chamber of Shipping (ICS), INTERCARGO, INTERTANKO, and Cruise Lines International Association (CLIA) (2016). *The Guidelines on Cyber Security Onboard Ships. Version 1.1.* Bagsvaerd.
Bayuk, J. L., J. Healey, P. Rohmeyer, M. H. Sachs, J. Schmidt, and J. Weiss (2012). *Cyber Security Policy Guidebook*. New Jersey: Wiley.
Biener, C., M. Eling, and J. H. Wirfs (2015). "Insurability of Cyber Risk: an Empirical Analysis". In: *The Geneva Papers* 40, pp. 131–158.
Boyes, H., R. Isbell, and A. Luck (2016). *Code of Practice: Cyber Security for Ports and Port Systems*. Stevenage.
Brooks, D. J. (2010). "What is Security: Definition through knowledge categorization". In: *Security Journal* 23.3, pp. 225–239.
Brooks, M. R. and K. Cullinane (2007). "Governance Models Defined". In: *Devolution, Port Governance and Port Performance*. Ed. by M. R. Brooks and K. Cullinane. London: Elsevier, pp. 405–435.
Bueger, C. (2015). "What is maritime security?" In: *Marine Policy* 53, pp. 159–164.
Carrapico, H. and A. Barrinha (2017). "The EU as a Coherent (Cyber)Security Actor?" In: *Journal of Common Market Studies*, pp. 1–19.
Chertoff, M. (2008). "The cybersecurity challenge". In: *Regulation and Governance* 2.4, pp. 480–484.
Colesniuc, D. (2013). "Cyberspace and Critical Information Infrastructure". In: *Informatica Economica* 17.4, pp. 123–132.
Commerce (ICC), I. C. of (2015). *Cyber Security Guide for Business*. Paris.
Craigen, D., N. Diakun-Thibault, and R. Purse (2014). "Defining Cybersecurity". In: *Technology Innovation Management Review* 4.10, pp. 13–21.
CyberKeel (2014). *Maritime Cyber-Risks*. Copenhagen.
*Cybersecurity in the European Union: Resielience and Adaptability in Governance Policy* (2016). Hampshire: Palgrave Macmillan.
*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* (2013). URL: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security.
Defense, M. of (2011). *Security Strategy for Society - Government Resolution 16.12.2010*. Helsinki: Ministry of Defense of Finland.
Defense, M. of (2013). *Finland's Cyber Security Strategy - Government Resolution 24.1.2013*. Helsinki: Ministry of Defense of Finland.
Dekker, S. and H. Stevens (2007). "Maritime security in the European Union — empirical findings on financial implications for port facilities". In: *Maritime Policy & Management* 34.5, pp. 485–499.
Eski, Y. (2011). ""Port of Call": Towards a criminology of port security". In: *Criminology & Criminal Justice* 11.5, pp. 415–431.
Fitzgerald, M., N. Kruschwitz, D. Bonnet, and M. Welch (2013). *Embracing Digital Technology: A New Strategic Imperative*. 2, pp. 1–12.

Fitzpatrick, W. M. and S. A. Dilullo (2015). "Cyber Espionage and the S.P.I.E.S. Taxonomy". In: *Competition Forum* 13.2, pp. 307–336.
Fok, E. (2015). "Cyber Security Challenges: Protecting Your Transportation Management Center". In: *Institution of Transportation Engineers Journal* 85.2, pp. 32–36.
Geers, K. (2009). "The Cyber Threat to National Critical Infrastructures: Beyond Theory". In: *Information Security Journal: A Global Perspective* 18.1, pp. 1–7.
Germond, B. (2015). "The geopolitical dimension of maritime security". In: *Marine Policy* 54, pp. 137–142.
Goldby, M. (2008). "Electronic bills of lading and central registeries: what is holding back progress?" In: *Information & Communications Technology Law* 17.2, pp. 125–149.
Gross, M. L., D. Canetti, and D. R. Vashdi (2017). "Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes". In: *Journal Of Cybersecurity* 3.1, pp. 49–58.
Group, C. (2016). *2016 Cyberthreat Defense Report - North America, Europe, Asia Pacific, and Latin America*. Annapolis.
Helmick, J. S. (2008). "Port and maritime security: A research perspective". In: *Journal of Transportation Security* 1.1, pp. 15–28.
Ho, M. W. and K. H. ( Ho (2006). "Risk Management in Large Physical Infrastructure Investments: The Context of Seaport Infrastructure Development and Investment". In: *Maritime Economics & Logistics* 8.2, pp. 140–168.
Hult, F. and G. Sivanesan (2013). "Introducing cyber". In: *Journal of Business Continuity & Emergency Planning* 7.2, pp. 97–102.
International Maritime Organization (IMO) (2016a). *IMO Multilingual Glossary on Cyberterms*. London.
International Maritime Organization (IMO) (2016b). *Interim Guidelines on Maritime Cyber Risk Management*. London.
Jensen, L. (2015). "Challenges in Maritime Cyber-Resilience". In: *Technology Innovation Management Review* 5.4, pp. 35–39.
Jones, S. (2015). "Addressing cyber security risks at ports and terminals". In: *Port Technology International Journal* 62.
Kadivar, M. (2014). "Cyber-Attack Attributes". In: *Technology Innovation Management Review* 4.11, pp. 22–27.
Kapto, A. S. (2013). "Cyberwarfare: Genesis and Doctrinal Outlines". In: *Herald of the Russian Academy of Science* 83.4, pp. 357–364.
Kendrick, R. (2010). *Cyber Risks for Business Professionals: A Management Guide*. Cambridgeshire: IT Governance Publishing.
Knowsler, G. (2017). *Maersk cyber attack forces carrier to put cargo bookings on hold*. URL: http://fairplay.ihs.com/article/4288541/maersk-cyber-attack-forces-carrier-to-put-cargo-bookings-on-hold.
Kouwenhoven, N. (2014). "The implications and threats of cyber security for ports". In: *Port Technology International Journal* 61.
Lasi, H., P. Fettke, H.-G. Kemper, T. Feld, and M. Hoffmann (2014). "Industry 4.0". In: *Business & Information Systems Engineering* 6.4, pp. 239–242.
Lewis, J. A. (2002). "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats". In:
Limnéll, J., K. Majewski, and M. Salminen (2015). *Cyber Security for Decision Makers*. Docendo.

Loh, H. S. and V. V. Thai (2015). "Management of disruptions by seaports: preliminary findings". In: *Asia Pacific Journal of Marketing and Logistics* 27.1, pp. 146–162.
Loukas, G. (2015). *Cyber-Physical Attacks: A Growing Invisible Threat*. Oxford: Elsevier Science.
Luppicini, R. (2014). "Illuminating the Dark Side of the Internet with Actor-Network Theory: An Integrative Review of Current Cybercrime Research". In: *Global Media Journal - Canadian Edition* 7.1, pp. 35–49.
Marlow, P. B. (2010). "Maritime security and update of key issues". In: *Maritime Policy & Management* 37.7.
Maurushat, A. (2013). *Disclosure of Security Vulnerabilities: Legal and Ethical Issues*. London: Springer.
Meersman, H. and E. Van de Voorde (2010). "Port Management, Operation and Competition: a Focus on North Europe". In: *The handbook of Maritime Economics and Business*. Ed. by C. T. Grammenos. London: Lloyd's List, pp. 891–906.
*Merriam-Webster Dictionary* (2017). URL: https://www.merriam-webster.com/.
Miron, W. and K. Muita (2014). "Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure". In: *Technology Innovation Management Review* 4.10, pp. 33–39.
Papa, P. (2013). "US and EU strategies for maritime transport security: A comparative perspective". In: *Transport Policy* 28, pp. 75–85.
Pinto, C. A. and W. K. Talley (2006). "The Security Incident Cycle of Ports". In: *Maritime Economics & Logistics* 8.3, pp. 267–286.
Platt, V. (2011). "Still the fire-proof house? An analysis of Canada's cyber security strategy". In: *International Journal: Canada's Journal of Global Policy* 67.1, pp. 155–167.
Prezelj, I. and A. Ziberna (2013). "Consequence-, time- and interdependency-based risk assessment in the field of critical infrastructure". In: *Risk management* 15.2, pp. 100–131.
Rantapelkonen, J. and H. Kantola (2013). "Insights into Cyberspace, Cyber Security, and Cyberwar in the Nordic Countries". In: *The Fog of Cyber Defense*. Ed. by J. Rantapelkonen and M. Salminen. Helsinki: National Defense University, pp. 24–36.
Risk Management (IRM)I, I. of (2014). *Cyber Risk: Executive Summary*. London.
Rittinghouse, J. and W. M. Hancock (2003). *Cybersecurity Operations Handbook*. London: Elsevier Digital Press.
Thai, V. v. and D. Grewal (2007). "The Maritime Security Management System: Perceptions of the International Shipping Community". In: *Maritime Economics & Logistics* 9.2, pp. 119–137.
Trade, U. N. C. on and Development (2016). *Review of Maritime Transport 2016*. New York: United Nations Publication.
United Kingdom, H. G. (2016). *National Cyber Security Strategy 2016-2021*. London.
Urcioli, L. (2015). "Cyber-Resilience: A Strategic Approach for Supply Chain Management". In: *Technology Innovation Management Review* 5.4, pp. 13–18.