PUBLICATIONS OF THE HAZARD PROJECT
3:2017

CYBERSECURITY IN PORTS

Jenna Ahokas
Tuomas Kiiski

PUBLICATIONS OF THE HAZARD PROJECT
3:2017

CYBERSECURITY IN PORTS

Jenna Ahokas Jenna
Kiiski Tuomas

Turku 2017

ISBN 978-951-29-7071-1

PUBLISHED BY:
HAZARD Project
Turku School of Economics
University of Turku
Rehtorinpellonkatu 3, FI- 20014 University of Turku, Finland
http://blogit.utu.fi/hazard/

Published 26.6.2017

TABLE OF CONTENTS

ACRONYMS

CPS	Cyber-physical System
ECN	Electronic Communication Network
ENISA	European Union Agency for Network and Information Security
EU	European Union
HTML	HyperText Markup Language
ICT	Information and Communication Technology
IET	Institute of Engineering and Technology
IMO	International Maritime Organization
ISPS	International Ship and Port Facility Security
ITS	Intelligent Transport System
NHS	National Health Service of the United Kingdom
NIST	National Institute of Standards and Technology, United States Department of Commerce

1 INTRODUCTION

1.1 Background

The National Institute of Standards and Technology (NIST) of the United States has identified that national and economic security depends on reliability and functionality of critical infrastructure (NIST 2014). Also, the European Union (EU) has highlighted the importance of the critical infrastructure sector to its Member States and their economic security. Critical infrastructure sectors include industries such as transport, energy and telecommunication networks. The negative impact from natural disasters, terrorism, criminal activity, or malicious behaviour towards the critical infrastructure sector influences the security of the Member States of the EU and its citizens. (European Commission 2017.) One infrastructure, considered the backbone of an economy, is logistical infrastructure because it supplies and operates as a link between nations, organizations, and individuals (Düerkop & Huth 2016). The functionality of critical infrastructure is continuously enhanced by creating new innovations, opportunities, and threats (Limnéll et al. 2014).

In 2015, the volume of world seaborne trade was 10 billion tons (UNCTAD 2016). Ports and terminals handle more than 70% of the value of seaborne trade and are the main link between landside and international trade. Ports are classified as critical infrastructure, affecting the economic and social well-being of a country. (Kurapati et al. 2015.)

Cybersecurity refers narrowly to the maintenance of integrity and availability of information and systems, confirmation of business continuance and the continuous usefulness of cyberassets (Boyes et al. 2016). Cybersecurity has increased its importance in the maritime sector, especially in port operations. The World Economic Forum raised cyberattacks as the fourth top global risk in January 2012. A year later, cyberattacks were seen to pose an even higher risk to the global economy. (Hult & Sivanesan 2013.) The maritime sector is very important for the EU and its Member States. In the EU region, 52% of the goods traffic in 2010 was by maritime transport. Maritime regions account for more than 40% of Europe’s GDP. In the EU, 22 Member States have a maritime border and manage more than 1,200 seaports in support of maritime sector activity. (ENISA 2011.)

Computer and communication networks form the core of intelligent transport systems (ITS). ITS are technologies, applications or platforms that improve the quality of transport or achieve other outcomes based on applications that monitor, manage or enhance transport systems. They have enhanced the effectiveness, coherence and efficiency of the transport network. Three common objectives of transport system dictate the cybersecurity approach: 1) safe operation for all transport modes; 2) operating and efficiently moving people, goods and services; and 3) communication with the public for public interest and safety. (Fok 2013.)

The issue of maritime security has become a greater concern on the international maritime agenda. Historically, the earliest issues of maritime security referred to piracy and cargo theft;

this has expanded to includes stowaways and people- and drug trafficking. On 1 July 2004, the International Maritime Organization (IMO) accepted the International Ship and Port Facility Security (ISPS) Code linking ships and ports together, enabling them to cooperate in preventing and uncovering threats to security in the maritime transport sector. (Cited in Thai & Grewal 2007.)

1.2 Purpose and structure of the report

This report aims to clarify the main points and definitions of the cyberspace and cybersecurity for ports and port operators. It is important to point out possible threats that ports need to identify for the future. The objective of the report is to describe cybersecurity in ports. More specifically, the question to be addressed is:

- What effects does cybersecurity have on ports?

Chapter 2 inspects the concepts of cyberspace and cybersecurity. It also surveys the threats, risks, vulnerabilities, and known aspects of cyberthreats. Chapter 3 outlines the concepts of ports and port environments, and the security risks studied in the literature. It gives a broad view of port functions and how they rely on Information and Communication Technologies (ICT).

Chapter 4 examines the concept of critical infrastructure and presents three cybersecurity frameworks. It is vitally important to look more closely at critical infrastructure, of which ports are a significant part. The researched frameworks are:

1) Cyberrisk Management Strategy for Ports by the International Maritime Organization (IMO),
2) Code of Practice by the Institute of Engineering and Technology (IET), and
3) Framework for Improving Critical Infrastructure Cybersecurity by the National Institute of Standards and Technology of the United States (NIST).

The framework for critical infrastructure can be connected to ports and port operations. Chapter 5 summarises the results of this report and proposes what should be researched and how cybersecurity is seen to evolve in the future.

2 CYBERSPACE AND CYBERSECURITY

2.1 Definitions of cyberspace

Cyber is a prefix of cyberspace which refers to electronical communication networks (ECN)[1] and virtual reality. It evolved from the word cybernetics. The roots of cybernetics date back to 1948 when Norbert Wiener published his book "Cybernetics: Or Control and Communication in the Animal and the Machine". In the book, Wiener researched the connection between control and monitoring. He emphasized communication as a key factor in the context of effective operations, and monitoring of organic and mechanical systems. (Cited in Benedikt 1991.) Ashby (1956, 9) has defined that the main themes of cybernetics are i) collaboration, ii) regulation, and iii) occupancy. Even though cybernetics has its connection with the physical world, it does not depend on the laws of physics. The basic idea of cybernetics is the concept of difference. Here, the concept of difference is that two things are either significantly different, or one of the things has changed over time. The concept of cybernetics offers a single vocabulary and a single set of concepts suitable for representing the most diverse types of system.

The term cyberspace became popular in 1984 when William Gibson published the novel "Neuromancer". In it, he describes cyberspace as a three-dimensional space where pure information is moved between computer and computer clusters. Gibson also saw people as generators and users of information. (Cited in Craigen et al. 2014, 14; Limnéll et al. 2014, 29.)

Cyber is a broadly defined term; its definitions can include different aspects, such as cyberattacks, cyberwarfare, cybercrime, cyberterrorism, and cyberspace. Cyberspace can be understood as an electronic world, where information, software, and people are shared and it is seamlessly woven into the physical world. In linkage to critical infrastructure, cyberspace is increasingly involved in global discussions alongside global water shortages and climate change. Cyberspace has evolved to become the nervous system of society, because cyberspace connects individuals and organizations around the world. If problems occur in cyberspace, for example a cyberattack on a nation's energy sector, the citizens of the nation become very vulnerable and disconnected. (Hult & Sivanesan 2013.)

A report by FireEye and Marsh & McLennan (2017) highlighted cyberincidents that occurred in late 2015 whereby hackers succeeded in shutting off power to hundreds of thousands of residents in Ukraine. According to public reports, these attacks were accompanied by parallel cyberintrusions into Ukraine's train system and TV stations.

[1] A computer-based order matching system that provides investors with direct access to the market, bypassing the middleman (bank) for order placement (Electronical Communication Networks).

Cyberspace is made up of combined networks through information and cyber-physical systems (CPS)[2]. These information systems and CPS use electronic, computer-based and wireless connections including information, services, and social and commercial operations that exist only in cyberspace. (Boyes et al. 2016, 11.) In the early 1940s in the United States, cyberspace and cyberpower were seen as a means of exerting broad order and control across warring domains. Cyberspace is based on communication, and its operational success is dependent on maintaining lines of communication. (Lee 2013.)

2.2 Driving forces of cyberspace

The driving forces of cyberspace are Time, Space, Anonymity, Asymmetry, and Efficiency. These factors create the "TSAAE" formula that influences reality and the understanding of security. (Hanska & Limnéll 2013, 2.)

If an individual or organization does not understand these key factors of the TSAAE, there will be a greater probability of failure and loss of strategic advantage. The formula highlights a new approach to understanding security. Because cyberspace is a flexible environment, these driving forces manifest themselves differently in the physical world. (Limnéll et al. 2014, 63.)

Time is a vital and irreplaceable part of human life. Every action, its preparation and realization, takes time. In the physical world, physical threats do not generally occur instantly. For example, it takes time to marshal troops or forces for battle. In cyberspace, however, actions can occur in the blink of an eye and without warning, or over a longer period of time. In terms of time, it matter little whether a cyberattack is launched from the house next door or from the other side of the world. (Benedikt 1991, 3; Hanska & Limnéll 2013, 2.)

Space is interwoven with time into a complex tapestry. In cyberspace, no one is safe from a cyberattack, and anyone can start a cyberattack in the digital battle space. In the worst case, a cyberattack needs only on person to press "enter" on a keyboard. In cyberspace, any destination can be attacked instantly. Cyberspace is unestablished and constantly changing through technology updates and networks changes. In the long term, cyberspace can be changed in the desired direction by international contracts and instructions. The challenge in cyberspace is the difficulty of defining what the effects of a cyberattack will be and where it was launched from. (Hanska & Limnéll 2013, 5; Limnéll et al. 2014, 65.)

The key challenge in **Anonymity** is the identification of cyberspace and its operations. Identification refers to the operators' identity and denotation of their location, which is difficult in cyberspace. The certainty level of identification depends on three factors: the target level of identification, the nature of the actions, and the intended aim of identification. Sometimes,

[2] A system designed as an entity, or set of entities, with a specific purpose, or to meet a capability objective. A CPS should include a computational aspect (cyber) and a physical aspect working together to accomplish a task or function. (Boyes et al. 2016.)

politically operated groups will claim responsibility of for a cyberattack. For example, the government of the United States was, informally, involved in the creation and implementation of the Stuxnet malware that disrupted Iran's nuclear program in 2011. By admitting to its involvement, the United State showed the world that it had both the power and the resources to use advanced cyberweapons on demand. (Limnéll et al. 2014, 67–68.)

The term **Asymmetry** is quite old, but became part of the public debate after the attacks of 9/11[3], in which Al-Qaida waged symmetrical warfare (Limnéll et al. 2014, 68). Asymmetrical warfare exploits the weak point of an opponent and attempts to use competitive advantage in the most optimal way. Cyberspace creates new opportunities for asymmetrical warfare. Each cyberoperation, including information warfare, is asymmetrical by nature, even though the distribution and implementation of operations is symmetrical. (Hanska & Limnéll 2013, 10.) Asymmetry characterises cyberthreats. It also contains limited possibilities to identify the generators of cyberattacks and offers the opportunity to use these means by non-state actors, which are individuals or organizations that have significant political influence but are not allied to any particular country or state. (Colesniuc 2013.) Asymmetry allows cyberattackers to take advantage of changes faster and more easily (Babcock 2015).

Efficiency of a cyberattack does not mean that the Internet crashes. The aim of a cyberattack is usually to weaken the reliability with which organizations and nations perform without interruptions. The key element of efficiency in cyberspace is that the operator can perform multiple actions at the same time in different dimensions. The wider the network of operation that organizations and nations use, the more networks and information systems need to be protected. (Hanska & Limnéll 2013, 13.) With regard to efficiency, non-governmental operators have two ways to exert strategic influences. First, they can commercialize their own cyberskills and cooperate with national or other non-governmental operators. Second, they can form different alliances, for instance with national authorities that can offer them cyberskills. Even though cyberspace can be used for malicious operations, it has established a platform for new innovations, such as digitalization, virtualization and automation. Thanks to these innovations, organizations have been able to cute various intermediaries from their production and service chains. (Limnéll et al. 2014, 70–71.)

2.3 Definitions of cybersecurity

Cybersecurity is a broadly used term whose definitions differ greatly and often subjectively. According to Lewis (2006), cybersecurity entails the safeguarding of computer networks and the information they include from penetration and from malicious damage or disruption. Craigen et al. (2014) define cybersecurity as an organization and collection of resources, processes and

[3] On September 11, 2011, terrorists hijacked four aeroplanes in the US and deliberately flew them into the towers of the World Trade Centre in New York, the Pentagon in Washington D.C, and a field in Pennsylvania (History.com 2017).

structures, which are used to protect cyberspace and cyber-related systems that misalign legal ownerships from actual property rights.

Cybersecurity can be seen also as a collection of tools, methods, security concepts, security safeguards, guidelines, risk management methods, processes, educations, insurances, and technologies. This collection can be used to protect the assets of cyberspace, organizations, and users. (Boyes et al. 2016.)

Colesniuc (2013) has defined cybersecurity as a method that helps to ensure the safety of cyberspace from threats which can take different forms, such as espionage or stealing secret information from national or international companies and government institutions. Chertoff (2008) has highlighted that not only governments are responsible for cybersecurity issues; individuals, organizations and institutions are also responsible, in the way they use the Internet and operate systems based on information and communication technology.

Different measures and procedures help organizations in multiple ways. Organizations can verify whether their security managements meet the necessary principles, processes and methods, and they can identify their own security strengths and weaknesses. Additionally, they can identify security trends both within and without their management setup. Based on the identified trends, they can then make changes to their own security position. (Boyes et al. 2016.)

2.4 Main objects of cybersecurity

To identify threat levels to cybersecurity, it is necessary to fully understand what the process entails. Individuals, nations, and companies face the same challenges posed by cybersecurity threats, and must recognize that these threats are increasing in frequency, sophistication, and scope. (Chertoff 2008.) Sophisticated cyberattackers are not afraid to use all necessary means to gain access to sensitive data (Shackleford 2015). A recent example is the worldwide WannaCry ransomware attack, which targeted computers running the Microsoft Windows operating system. The attack started on May 12, 2017 and infected more than 300,000 computers in 150 countries. Among those affected were the National Health Service (NHS) of Britain, international shipper FedEx, the Telefonica telecommunications company in Spain and the Deutsche Bahn railroad operator in Germany. (Graham 2017.)

Cybersecurity threats are exploiting the growing complexity and connectivity of critical infrastructure, placing the security, economy, public safety, and health of entire countries in danger. The risks to cybersecurity can affect an organization’s bottom line, raising costs and affecting revenue. They can also damage an organization’s ability to develop, complicating the maintenance and procurement of customers. (NIST 2014.)

As organizations evaluate the security of their operations and the likelihood of threats, risks and vulnerabilities, they need to address three questions:

- From what we are protecting ourselves?

- What are we protecting?
- How we are protecting it?

The main factor is the subject of the first question. Organizations need to decide what or whom they will primarily protect, and how strongly they can operate if the security fails. To address the second question, organizations need to identify possible threats through threat analysis. The third question refers to the measures and procedures that organizations will implement to ensure an object's security from the factor that threaten it. (Limnéll et al. 2014, 37.)

In a study what organizations see as the biggest cyberthreats, the CyberEdge group (2014) found these to be phishing[4], malwares[5], such as viruses and worms, and zero-day-attacks[6]. From the organizations' perspective, less attention is paid to cyberattacks on Internet software, focused attacks, viruses targeting mobile devices, inactivity of services and downloaded malwares.

The European Network and Information Agency (ENISA) has identified as cyberthreats attacks that focus on web pages or web applications, identity thefts, attacks exploit information leaks, and programs that damage or disrupt operations. Drive-by-malware[7] performs by injecting a damaging code into the HTML-code[8] of a web page. It is focuses on the user of the computer system, infecting the computer even if all the user does is visit the web page. (ENISA 2011.)

2.5 Threat levels

A threat can be seen as any act bringing danger, harm or uncertainty to the cyberenvironment[9]. By defining the threats, it becomes easier to identify the level of security needed, evaluate different threatening actors, and increase comprehension of what kind of method is needed to produce security. A threat can be an act that causes damage, disruption or difficulty to operations. (Limnéll et al. 2014, 110.) Threats are caused by malicious actions or the unintended results of benign actions. Malicious actions can, for example, involve hacking or the introduction

[4] Phishing is a form of fraud in which the attacker tries to gain information such as personal (security) details by masquerading as a reputable entity or person in e-mail or other communication channels (Rupert 2010, 51).

[5] Malware, or malicious software, is a program or file that is harmful to a computer user. Malicious programs can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission. (Rupert 2010, 52.)

[6] A zero-day-attack exploits a security vulnerability on the same day the vulnerability becomes generally known. There are zero days between the time the vulnerability is discovered and the first attack. (CyberEdge Group 2014.)

[7] Drive-by-malware is a program that involves the user downloading material from the Internet which contains some aspects of malicious malware (Rupert 2010, 51).

[8] HTML-code is the set of markup symbols or codes inserted in a file intended for display on a World Wide Web browser page (Rupert 2010, 15).

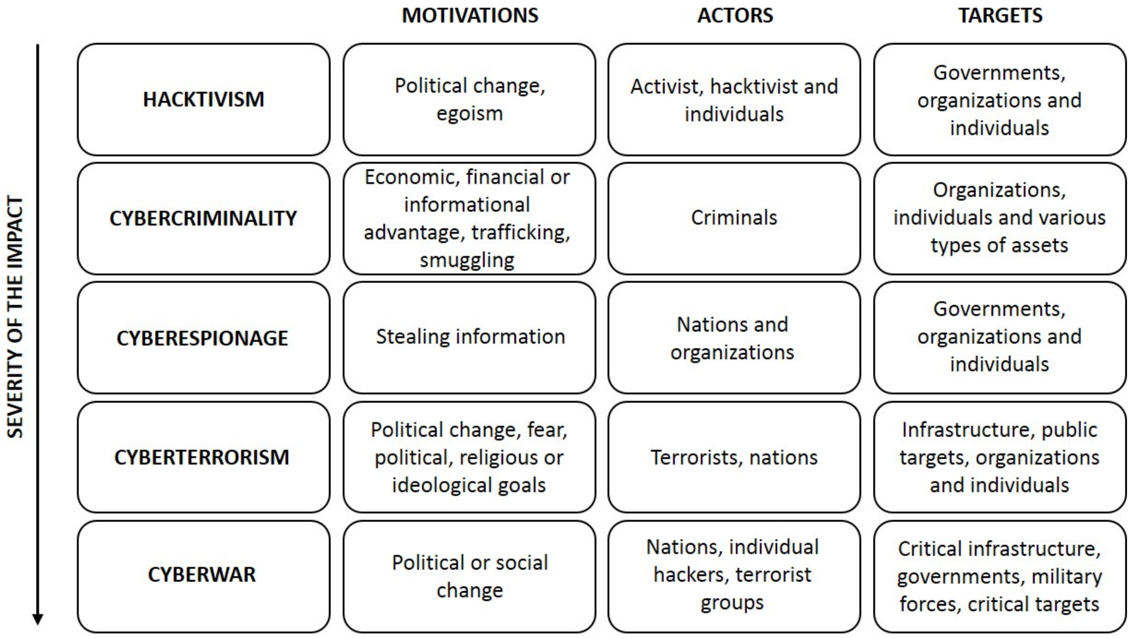
[9] Cyberenvironment comprises the interconnected networks of both information and cyber physical systems that use electronic, computer-based and wireless systems, including information, services, and social and business functions that exist only in cyberspace (Boyes et al. 2016).

of malware. Benign actions and their unintended results can include software maintenance or user permissions. (IMO 2016.)

Cyberattacks are considered dangerous because there are so many aspects that influence their results, consequences and nature. For example, a cyberattack can harm employees physically through death or injury, damage equipment, or lead to widespread economic disruption. (Colesniuc 2013; Sanger et al. 2014.)

Performing cyberattacks does not require extensive knowledge or experience. Attackers with even a minimum of equipment can possess enough skills to do serious damage in cyberspace and the physical world. The results or consequences of cyberattacks can be difficult to define, precisely because the damage can be greater than expected or known. The aspect of anonymity is a very difficult concept in cyberspace because it creates gaps and complexity between individuals and government legislations. (Sanger et al. 2014.)

Lewis (2002) has identified four elements of the reassessment of cyberthreat. 1) A historical context for cyberattacks towards critical infrastructure needs to be identified. 2) Cyberattacks should be examined by the number of failures, such as power outages, transport delays and communication interruptions. 3) The reliance of critical infrastructure on computer networks and redundancy that is present in these systems need examination. 4) The usage of cyberweapons and political goals and targets of terrorists, and the possibility that cyberweapons can accomplish these goals, need to be considered in cases of cyberterrorism. Figure 1 illustrates different threat levels of cybersecurity. They are termed levels, because each of them contains different political and social features.



SEVERITY OF THE IMPACT

	MOTIVATIONS	ACTORS	TARGETS
HACKTIVISM	Political change, egoism	Activist, hacktivist and individuals	Governments, organizations and individuals
CYBERCRIMINALITY	Economic, financial or informational advantage, trafficking, smuggling	Criminals	Organizations, individuals and various types of assets
CYBERESPIONAGE	Stealing information	Nations and organizations	Governments, organizations and individuals
CYBERTERRORISM	Political change, fear, political, religious or ideological goals	Terrorists, nations	Infrastructure, public targets, organizations and individuals
CYBERWAR	Political or social change	Nations, individual hackers, terrorist groups	Critical infrastructure, governments, military forces, critical targets

Figure 1 Motivations, actors, and targets of cyberthreats (modified from Boyes 2015)

Figure 1 shows examples of motivations, actors, and targets of cyberthreats. A cyberattack can be one of the following: hacktivism, criminality, espionage, terrorism or warfare. Cyberattackers may aim to gain political or social control and power, instigate political changes, steal information, and gain economic advantage or some other aspects of egoism.

The attackers can be individuals, activist groups, competitors, cybercriminals, terrorists, proxy terror threat actors[10] and nation states. The targets are usually critical infrastructure, various types of assets, nations, governments, organizations, or individuals. (Boyes et al. 2016, 12.)

The motivations of cyberthreats can be separated into strategic threat levels, the creators of threats, and the motives of these actions. Decision making on cybersecurity contributes to the threat catalogue, which highlights the threats that an organization considers harmful to its operations and needs to be protected from. (Limnéll et al. 2014, 111.)

2.5.1 Hacktivism

The term hacktivism is a blend of the words hacker and activism, but refers to very different actions and actors from those involved in cyberattacks. Hacktivism usually means undisturbed utilization of cyberspace that helps to advance specific actions. The utilization of cyberspace is seen as searching information through the Internet, setting up and maintaining web pages, passing information, and using digital tools to coordinate operations. Hacktivism is the act of hacking or breaking into a computer system. The operations of hacktivism use different kinds of hacking techniques to invade web pages and computers. The aim of hacktivism is to disrupt or interrupt a certain web page or its usage without any severe damage occurring. (Limnéll et al. 2014, 114.)

Hacktivism groups sometimes seek publicity, try to convey a special meaning or create pressure on a certain objective. For example, drug dealers bought cyberattack services from a hacker group aimed at the port of Antwerp in Belgium. The hacker group succeeded in injecting a virus into the port's data system, giving them control over container movements and schedules. They were able to do this without the knowledge of the port owners or employees. Hacktivist groups can target either a port itself, the port operator, or a third party such as suppliers or recipients of cargo. (Boyes et al. 2016.)

[10] Proxy terror threat actors have the capacity and sophisticated technical support available to a nation state made available by the sponsoring nation. These actors include cyberfighters, such as groups of nationally motivated individuals who threaten or attack other groups, businesses and the infrastructure of the other nation states. These cyberfighters can be seen as a type of hacktivist whose interest is the support of a nation state and they may enjoy significant sophisticated technical support from that nation state. (Boyes et al. 2016.)

2.5.2 Cybercriminality

Cybercriminality narrowly refers to any illegal activity that focuses on computers, digital information, data systems or information networks. In a broader view, cybercriminality is any illegal activity that somehow focuses on information technology. (Limnéll et al. 2014, 120.) Cybercriminality can also aim for economic benefit that contains criminal damage, such as robbery of cargo, smuggling of humans or cargo, or avoiding taxes (Boyes et al. 2016). Cybercrime can be also referred to as computer crime, where a computer is used as a tool to carry out illegal activities, such as identity thefts, privacy violations, trafficking intellectual property or child pornography. (Luppicini 2014.)

There are four types of cybercriminality. Type 1) involves actions that endanger confidentiality, completeness and availability of information and data systems. Type 2) involves crimes that take advantage of computers, such as forgery and identity thefts. Type 3) refers to criminal actions such as illicit gambling or spreading false information. Type 4) includes crimes involving copyright and trademark infringement. (Limnéll et al. 2014, 125.)

In the 21st century, more highly sophisticated criminal groups have emerged that utilize cybercriminality for cyberattacks. These groups can spot vulnerabilities in business networks, and their aim is to steal or collect economical valuable information. Even though cybercriminality is a growing threat, it does not possess the same level of risk and damage as cyberterrorism. (Lewis 2002.)

2.5.3 Cyberespionage

Definitions of cyberespionage differ widely. Boyes et al. (2016) define it as illegal access to secret and delicate information such as company strategy, private information, or intellectual capital. Limnéll et al. (2014, 130) see cyberespionage as one of the severe cyberthreats that is aimed at getting competitive advantage by spying on an opponent's product development information. Fitzpatrick and Dilullo (2015) refer to cyberespionage as an activity which has the potential of costing the world economy billions of dollars and massive employment losses.

The target of cyberespionage is typically the information infrastructure of organizations. One survey from PriceWatershouseCoopers (PwC) highlighted that almost 120,000 cyberattacks take place daily, the target of which proprietary information. Cyberespionage has grown rapidly, from 3.4 million incidents in 2009 to 42.8 million in 2014. (see Fitzpatrick & Dilullo 2015.)

Five types of financial loss can occur from cyberespionage: 1) The theft of intellectual property, private business and/or customer information; 2) possible costs resulting from interrupted business plans or competitive exercises; 3) short-term profit losses and ineffectiveness combined with service disruptions and employee distractions; 4) damage to an organization's credibility due to loss of faith by customers and/or business partners in viability of its business or IT security programs; and 5) increased security costs to protect from future mischievous cyberactivity. (Platt 2011; Fitzpatrick & Dilullo 2015.)

2.5.4 Cyberterrorism

Cyberterrorism was first mentioned in 1980 by Barry Collin. He referred to changes to traditional terrorism brought about by a union of the physical and digital worlds. In Collin's perspective, terrorists can achieve similar effects with cyberattack as with physical power. Nowadays, cyberterrorism is mostly seen as having political, social, religious and ideological aims and is generally performed by small groups. Cyberterrorists often attempt to create specific factors and spread fear among or influence a population or its decision makers. (see Limnéll et al. 2014, 131.)

Cyberterrorism can be identified as the usage of computer network instruments to close down parts of critical infrastructure or to press or oblige a government or civilian population. Cyberterrorism is becoming an increasingly important threat nations and critical infrastructure, because the operations of both are increasingly dependent on computer networks. New vulnerabilities are being generated that threaten to become the electronic Achilles' heel of both nations and critical infrastructure. (Lewis 2002; Platt 2011.)

The characteristics of cyberterrorism include political or ideological targets, digitality of targets or measures, damage to humans or property, criminality or illegality, and fear as a result. Cyberterrorism strives to cause direct or indirect damage to the operation of its target. It uses methods such as dissemination of propaganda, vandalism, espionage programs, changing system commands, and cyberattacks on civil or military infrastructure. (Limnéll et al. 2014, 134–135; Luppicini 2014.)

2.5.5 Cyberwar

Cyberwar usually refers to furious attacks on the computer networks of an unsuspecting opponent (Lewis 2002). Cyberwar affects societies, organizations, and individuals. It can be defined in many ways; some experts compare cyberwar to concepts of drug war and war against poverty. Others think that espionage and hacktivism are not a cyberwar without severe physical damage. Realistically, serious security breaches and cyberespionage can speed up developments that could lead to physical confrontation between nations. (Limnéll et al. 2014, 139.) Warfare can also mean different types of conflicts between nations. The purpose of warfare is to disrupt, for example, transport systems so that e.g. ports are unable to run operative functions such as bulk cargo terminals. (Boyes et al. 2016, 14.)

Traditional warfare includes the four dimensions of land, sea, space, and air. Limnéll et al. (2014, 140) propose that cyberspace should be a fifth dimension. Their suggestion is supported by official knowledge that, for example, Russia and the United States have established their own headquarters and military forces for cyberwarfare. The main mission for these troops is to develop military cyber capability and doctrine.

Lee (2013, 67) has defined that cyberweapons can overpower even carefully crafted defences. It has been shown that by combining the experience and knowledge of military and civilian professionals, advanced cyberthreats can be better protected against. Cyberwar is a part of information warfare that is a fixed part of modern military capacity because telecommunications and network services have societal significance and are vital elements in political and military crises. (Ministry of Defence of Finland 2011).

2.6 Risks

Risk can be understood as an action or the likelihood of an intensification of a certain threat or other event that would cause hazardous results. Other definitions see risk as a measure of the likelihood and strictness of unfavourable consequences. In the 1990s risk was defined as a trinity of scenario, probability, and results. Later the aspect of vulnerability was added to the definition. (Prezelj & Ziberna 2013.) Risk has two main components. The first sees risk as a future outcome and it can take several forms. The second is the probability of a certain outcome occurring. (Khan & Burnes 2007.)

Risks are a part of every operation, and therefore they cannot be inhibited. Risks are usually seen as an operation’s condition existence. Risks can be seen as either a positive or negative occasion in the future, and they change continuously. They can be avoided, adopted, defined, moderated and transferred, and they come with certain terms. Responsible management is needed to identify and control risks. Risk management means that individuals, organizations, and societies aim to forecast consistent changes. The aim of forecasting is to define and evaluate the risks clearly and develop different methods of handling them within an organization. Risk management consists of planning, identifying and analysing risks, development of risk follow-up and reassessment of risks. (Ho & Ho 2006; Limnéll et al. 2014, 108–110.)

For all processes, risks are unavoidable. Risk management provides businesses with an efficient framework for managing and mitigating the risks. It identifies, assesses, and prioritizes risks by using economical resources to minimize, observe and control the possibility of regrettable events. (Khan & Burnes 2007; Düerkop & Huth 2016.)

2.7 Vulnerabilities

Vulnerability is seen as a weakness of cyberspace. With vulnerability, actors can weaken the data of a system or reliability of an operation. Vulnerability occurs when there is a fault or a weakness in the system that allows the attacker unwanted access. Management of vulnerabilities consists of their systematic identification, classification, correction and easing.

Outside of cyberspace, vulnerability is a weakness that is connected to technological, material or know-how matters. (Limnéll et al. 2014, 110–111.)

Over 90% of cyberattackers are familiar with the vulnerabilities of their targets, and have easy access to the technologies that were supposed to prevent attacks in the first place (Afful-Dadzie & Allen 2014). Vulnerabilities often result from insufficiency in a system's design, integration and maintenance, and from mistakes in cybercontrol (IMO 2016). The vulnerabilities of operational or information technology can be either direct, such as weak passwords that lead to unauthorized access, or indirect, such as the absence of network segregation. There can be consequences for security and the confidentiality, honesty, and availability of information. (IMO 2016.)

Lewis (2002) has identified that even though there is much discussion of the vulnerability of computer networks and critical infrastructure, it results from the rapid development of the technology. Computer networks may be more vulnerable than a single critical infrastructure, and different parts of the infrastructure have similar vulnerabilities.

IMO (2016) has highlighted the vulnerabilities that can lead in to cyberrisks in certain systems, such as bridge systems, cargo handling and management systems, access control and communication systems and administrative and crew welfare systems. For ports, the possible vulnerabilities include, for example, limited training and readiness for cybersecurity, software errors and coincidence, and connection and interdependence of networks (Homeland Security 2016).

Given that private industry owns and operates many crucial economic assets, including economic infrastructure, this poses a problem for governments, as it means a lack of control and cooperative mechanism with which to deal with attacks. An example of a cyberattack against critical infrastructure took place in Estonia on April 26, 2007. The idea behind the cyberattack was to put pressure on the Estonian government to move a Soviet statue from the Second World War from the military cemetery to its original spot in the centre of Tallinn. The Estonian government, law enforcement, banking, media and Internet infrastructure all had to cope with three weeks of cyberattacks. A hacker defaced the website of the Estonian Prime Minister's political party, inserting an apology for having moved the statue along with a promise to move it back to its original location. (Geers 2009; Platt 2011.)

3 PORTS AND PORT SECURITY

3.1 Definitions of ports

Ports are one of the important aspects of a country's transport infrastructure. To many trading nations, they are the main transport link between trading partners and the centres of motorways and railroads. Ports are the biggest economic factor for a nation's welfare and are usually seen as a gateway to trade. Most ports also attract commercial infrastructures, such as banks, offices, and industrial activities. (Alderton 2008, 2; Song & Panayides 2008.) Overall, some 90% of global trade is transported by ship, highlighting the huge significance of ports in the world of transport (Bancroft 2014).

Ports can be seen as complex and multipart organizations with institutions and functions crossing multiple levels. The strategic role of ports is very important given that they are the sole link between international shipping and the logistics community, and the only one that can combine all these institutions, functions, assets, processes and other elements. (Bichou 2004.) With a port and port facilities, goods and raw materials, such as oil and grain, have access to national industries and local supermarkets and other stores (Jensen 2015).

Traditionally, a port is an area where ships are loaded with cargo and/or unloaded of cargo. A port contains a common territory at sea where ships await their turn. Ports can be roughly divided into two types: 1) bigger main ports that handle international trade or 2) smaller ports that service the needs of the hinterland mainly with coastal transport or short marine transport. A port can also refer to a town that has its own harbour and facilities for a ship or shore interface and customs facilities. (Alderton 2008, 7.)

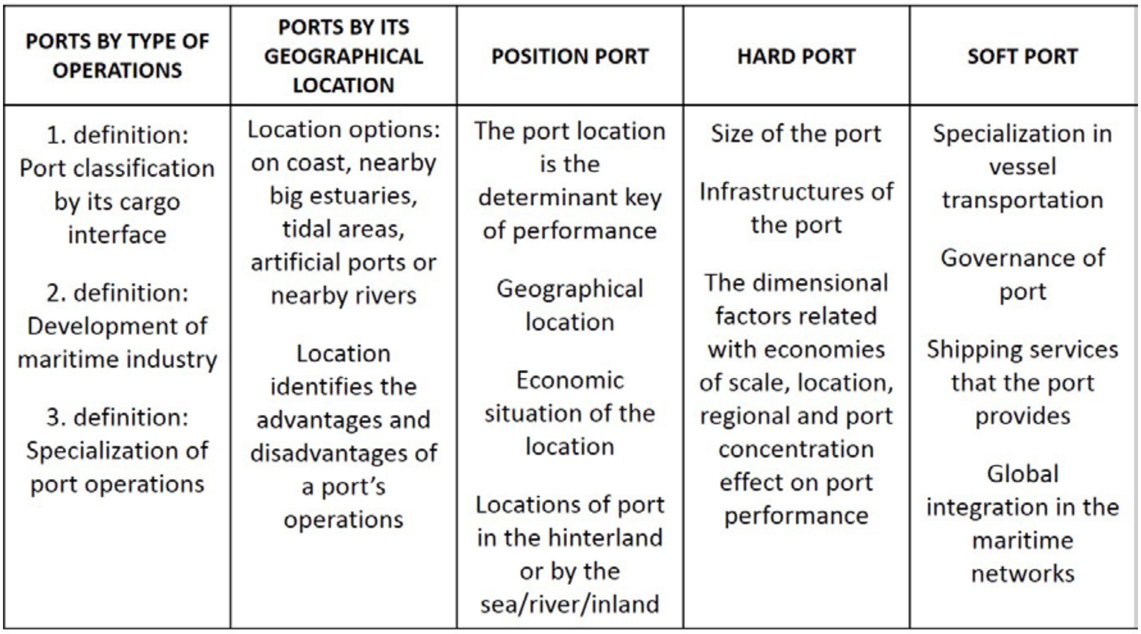
A port is a complex cyberenvironment[11] that consists of operations and systems on land and sea. The four main types of assets are buildings, vertical infrastructure, factory and machinery, and information and data systems. With these assets, variety in operational services can be assured, and technology has an important role in it. Reduction or endangerment of one or several assets has a potential to affect the speed and efficiency of a port's operation and observation of operations. This affects security and the reliable distribution of duties. (Boyes et al. 2016, 15.)

According to Bichou and Gray (2004), complexity of ports means that they usually include multiple different institutions and functions that cross through every level of the ports. They have identified three channels that help identify the functions of a port. The first one is the logistics channel, which deals with cargo processes through supply chains such as shipping lines and freight forwarders. The second channel is trade and the third one is supply. These both interlink with ownership of goods through the whole system of influenced organizations. The

[11] Cyberenvironment comprises the interconnected networks of both information and cyber physical systems that use electronic, computer-based and wireless systems, including information, services, and social and business functions that exist only in cyberspace (Boyes et al. 2016).

only difference between the trade and supply channels is that the former refers to the level of the sector or industry, such as the oil trade. The supply channel refers to the level of the firm.

A port’s main functions usually include civil engineering features, administrative functions, and operational functions. Civil engineering features deal with access to sea and land, berth infrastructure, network with road and rail and industrial area management. Administrative functions operate all the paperwork that needs to be done when ships arrive at port, such as control of dangerous cargo and immigration, health, customs and commercial documentary control. Operational functions include pilotage, tugging and mooring activities, use of berths and sheds, and loading, discharging, storage and cargo distribution. (Alderton 2008, 4–5.)



PORTS BY TYPE OF OPERATIONS	PORTS BY ITS GEOGRAPHICAL LOCATION	POSITION PORT	HARD PORT	SOFT PORT
1. definition: Port classification by its cargo interface 2. definition: Development of maritime industry 3. definition: Specialization of port operations	Location options: on coast, nearby big estuaries, tidal areas, artificial ports or nearby rivers Location identifies the advantages and disadvantages of a port’s operations	The port location is the determinant key of performance Geographical location Economic situation of the location Locations of port in the hinterland or by the sea/river/inland	Size of the port Infrastructures of the port The dimensional factors related with economies of scale, location, regional and port concentration effect on port performance	Specialization in vessel transportation Governance of port Shipping services that the port provides Global integration in the maritime networks

Figure 2 Different definitions of port (modified from Alderton 2008; Caldeirinha & Felício 2014)

Figure 2 explains the different definitions of port by Alderton (2008) and Caldeirinha and Felício (2014). Ports can be divided into two groups based on their operations or geographical location. They can be defined in three categories based on their operations. The first definition relates to the cargo interface that can be referred to as a centre port or mega-port. The second relates to the development of the maritime industry and was created in the mid-1960 to illustrate development after the Second World War. This development is seen in bigger industrial areas with their own maritime terminal, customs port, or oil port. The third definition refers to specialized ports, such as a naval port, fishing port, or a port specialized in the transport of certain commodity. (Alderton 2008, 10.)

By geographical definition, ports can be located on coasts, near large estuaries, in tidal areas, near rivers, or they can be artificial. Geographical location can be used to identify the advantages and disadvantages of a port’s operations. For example, a tidal port requires more expensive land surveying operations and dredging than a traditional port. (Alderton 2008, 10.)

Ports can also be characterized by their quality of existent installations, infrastructure and degree of services specified by their features. There are three classification categories: position port, hard port and soft port. For a position port, geographical location and the economic performance of the location are the determining features. A position port can be located in the hinterland, by the sea, inland or by a river. For a position port, location is the most important factor for performance. (Caldeirinha & Felício 2014.)

Infrastructure, size of port, size of terminal, water depth of the pier area and amount of existent equipment are the determining features for a hard port. The important factors and performance influencers relate to economic scale, location, region, and port concentration. Bigger ports not only have better performance through learning, the port sector has better economies of scale. The features of a soft port include degree of specialization in cargo handling, governance model, shipping services provided by the port, and degree of integration with global maritime networks. These features also provide a wider selection for ship owners, greater flexibility, and smaller transit times leading to improved port performance. (Caldeirinha & Felício 2014.)

3.2 Development of ports

Port structures change constantly and grow in complexity, making them dependent on information and communication technologies throughout their life cycle. Some of embedded technologies are in fixed or mobile assets needed for port operations; others can be run remotely, such as systems used to schedule ships and move cargo. (Boyes et al. 2016.) Alderton (2008, 10) notes that cargo management technology has developed radically in recent decades.

Ports can change and develop, or even die if changes occur in the inland transport infrastructure and/or trade models. The life cycle of port is usually very long, which drives ports to adapt and transform over time. Ports were first developed to meet the demand of sea trade and transport. They brought new competition and changes to trading patterns. (Alderton 2008, 14.) Figure 3 summarizes the development of ports and how these development concepts have evolved. This figure combines the concepts from Alderton’s book and an article by Pettit and Beresford.

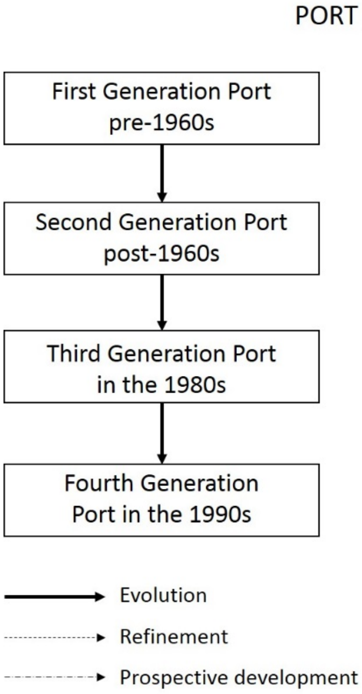

PORT DEVELOPMENT
First Generation Port pre-1960s
Second Generation Port post-1960s
Third Generation Port in the 1980s
Fourth Generation Port in the 1990s
WORKPORT Model
Identified changes through 1960s to 1990s:
- Changes in cargo forms and improved support services
- Increasing diversity of port-related activities
- Development of logistics and value addition
Ports of Rotterdam
Dubai Ports World (formerly P&O)
Distripark
Roadways
- ICDs
- Non value-added
Nedlloyd
- Districenter
- Value-added
Evolution
Refinement
Prospective development

Figure 3 Stages of port development (modified from Alderton 2008; Pettit & Beresford 2009)

First generation port refers to ports that were operated before 1960, as shown in Figure 3. These ports were the only cargo interface between land and sea transport. They were usually separate from the activities of transport and trade and were seen as independent operators with little or no cooperation with local authorities. Furthermore, the activities of a port itself were also separate from each other. These ports handled either breakbulk or bulk. (Alderton 2008, 79.)

Second generation ports operated after 1960 and were developed as transport, industrial and commercial service centres. They offered industrial and commercial services that were not directly linked to their loading or unloading activities. The policies and strategies of these ports were based on larger concepts, and management approaches were more sophisticated. Second generation ports developed relationships with local authorities and with transport and trade partners. (Alderton 2008, 80.)

The 1980s saw the emergence of third generation ports, which operated with global containerization and intermodalism linked to the growing requirements of international trade. These ports were considered hubs of an international production and distribution network. Their organizational structures were integrated and management was more proactive. Environmental approaches were integrated into their strategies. They were more modernised than first and second generation ports. (Alderton 2008, 80.) Third generation ports offer value-added services, such as warehousing and packaging apart from cargo handling (Bichou & Gray 2004). They also provide traditional activities such as ship services and cargo handling (Pettit & Beresford 2009).

Fourth generation ports emerged in the 1990s alongside expanding globalization and the development of major international companies. Their strategies and approaches were more sophisticated and included the use of automation. Accompanying this development were the standardization of information and globalization of port communities. Ports now had better control over their environmental activities and acquisition of knowledge. The decisive factor was information technology. (Alderton 2008, 81.) The sophistication of fourth generation ports is seen in their range of logistics and value-added services (Song & Panayides 2008; Pettit & Beresford 2009). These ports have common operators or administration but are located separately around the world, and can be considered global multiport companies (Bichou & Gray 2004; Notteboom & Rodrigue 2005).

Figure 3 presents the WORKPORT model illustrates that the stages of development can not be fixed in time and ports do not clearly go through certain stages in order. The model sees that in the 1960s and 1970s the ports were mainly discrete in terms of transport modes. In the 1980s ports started to diversify into the logistics field and they offered some value-added services. In the 1990s in the context of globalization ports were seen as mergers, acquisitions and joint venture operations which led to more complex and common operations. In terms of globalization ports became a greater part of global supply chains. (Pettit & Beresford 2009.)

The WORKPORT model in Figure 3 lists stages of development that cannot be fixed in time or any specific order. According to the model, in the 1960s and 1970s ports were mainly discrete in terms of transport modes. In the 1980s, they began diversifying into the logistics field and offered some value-added services. In the 1990s, in the context of globalization, they were seen as mergers, acquisitions and joint venture operations which led to more complex and common operations. In terms of globalization, ports became a greater part of global supply chains. (Pettit & Beresford 2009.)

An example of the WORKPORT model is Dubai Ports World, formerly known as P&O. It developed two different ports to operate in the global maritime markets. One, the port of Nedlloyd, offered custom-tailored value-added services in the early 1980s prior to its fusion with P&O. The other is P&O Roadways, which offers integrated transport services without adding value through its road, rail, and Inland Container Deports (ICDs) networks. ICDs can been seen as the earliest version of the international logistics rostrum for unitized cargo. (Pettit & Beresford 2009.)

A Distripark is an area of land that is efficiently set up for distribution operations located close to ports or terminals with good connections to the hinterland. Over 20 years ago, Rotterdam in the Netherlands developed a concept for a port that would be highly coordinated and based on value-added logistics services. The Rotterdam Municipal Port Management (RMPM) has developed its concept of the Distripark to respond to international trade and logistics developments. Rotterdam’s three Distriparks – Botlek, Eemshaven and Maasvlakte – offer warehousing space, product forwarding and processing. (Pettit & Beresford 2009.)

The increasing competition between ports and the growing amount of vessel transport have forced ports towards better performance. This performance relies mostly on port characteristics such as infrastructure, cargo handling specifics, shipping services and integration level in maritime networks. (Caldeirinha & Felício 2014.) Ports are usually seen as a fundamental part of the supply chain and as an understandable focus for areal advance and employment initiatives. The specific distribution channel of the port varies mainly depending on what kind of cargo the port handles, the requirements of the customers, and other factors. (Song & Panayides 2008; Pettit & Beresford 2009.)

3.3 Maritime and port security

Port security regulations have not existed for as long as ports themselves. The United States determined to invest in the International Maritime Organization in 1948. This was followed in 1974 by the first functions of Safety of Life at Sea (SOLAS). Since then, multitude of other international regulations have been developed and established. The way ports are stereotyped can range anywhere from ‘cultural wastelands’ to hubs for extensive international drug smuggling. They are in fact a remarkable assets, facilitating flows of people and goods between countries all over the world. The existence of uncertainties at sea has led to ports concentrating themselves at docks. (Eski 2011.)

Over the years, ports have become the growing focus of international and national security groups trying to instigate better control and prevention of possible threats. The main common security interest of ports globally is to provide safe passage and anchorage. In the last decade, attention has focused on insecurities related to transport mechanisms such as containers. It is known that containers are excellent way of transporting illegal drugs and immigrants and that they are not often checked for irregularities. In the United States, roughly 10 million containers pass through ports annually and only 2 % of them are examined. (Eski 2011.)

In 2004, the IMO adopted the International Ship and Port Facility Security (ISPS) Code. To begin with, the ISPS Code basically covers the traditional confluence between ships and port facilities. Also, it covers ports that serve ships engaged in international travel, leaving security gaps for ships on domestic voyages. Some security threats can also arise from shore-based operations. Onshore operations link stevedoring companies, road and rail transport companies and freight forwarders. These operations can have direct effects on maritime transport and port facilities. (see Pinto & Talley 2006; Thai & Grewal 2007; Alderton 2008.)

The ISPS Code has three security levels, ranging from low to high in proportion to the nature and scope of the incident or perceived security threat. The Code requires that ports and port authorities develop and implement improved facility security plans (PFSP) for each operational level. PFSP is based on the port facility security assessment and a risk-analysis scheme that is undertaken by governments and authorized security organizations. Ports need to provide proper financial, human and information resources that include the nomination of a port facility security officer(s) (PFSO). (see Bichou 2004.)

The standard framework for security and environmental protection of maritime traffic and ports includes legal tools, such as UNCLOS, SOLAS, MARPOL, the ISM and ISPS codes, and management measures, such as formal safety assessment and integrated coastal zone management (Bichou 2004). Maritime safety regulations are implemented at national and international levels. Individual nations set their own rules and norms regarding the differing technical perspectives of ships and navigation in order to increase safety. A flag state is a country that regulates ships under its registrations. It exercises its own jurisdiction and control over administrative, technical and social matters relating to ships that operate under its flag in order to ensure safety at sea. (Ma 2002.)

Due to the increase of cyberattacks and cyberthreats, many international organizations and agencies have developed new frameworks, standards and guidelines for port facilities and ships to protect themselves from these threats. The target of the ISPS Code is to enhance maritime security both on board ships and in ports. The traditional approach to maritime security was container security, which meant keeping the cargo inside the container safe. Nowadays, container security also includes keeping goods that do not belong inside the container out of it, such as weapons of mass destruction. (Pinto & Talley 2006; Thai & Grewal 2007.)

Cyberattackers usually target port operators inside the port area because operators tend to have fewer security controls than the port itself and are therefore easier to attack (Shackleford 2015). For ports, cyberthreats include, for example, an action to delete operational data containing time schedules and information for container shipments (Jensen 2015).

3.4 Risks in port facilities

Ports have long been considered an invisible industry, having always operated almost by themselves with scant attention and awareness from society (CyberKeel 2014). For port facilities, many different risks arise during their life cycle. Risks can appear at the start of the life cycle in the form of poor investigation of documents or insufficient time or budget allocation. For example, the implementation of more specific port security in safety planning has increased the emphasis of site designs. (Marsh & McLennan Companies 2014.) Risks to ports affect not only the ports themselves, but also their customers and other stakeholders. The risks can include, for example, financial losses, theft of cargo or information, and strikes or malfunctions in security, which can lead to the shutdown of a port. Port-related risks can affect the whole supply chain. (Ho & Ho 2006; Loh & Thai 2015.)

Usually, port incidents are unintentional events such as environmental harm, transport system interruption, or damage to employees and personnel. Accidents at ports can be classified by type, origin, and cause. Roughly 50% of accidents relate to loss of the cargo, 29% to fires, and 17% to explosions. It has also been observed that almost 40% of port incidents happen at sea, 21% on land concerning warehousing, processes and transport, and 39% at a sea-land interface. (Pinto & Talley 2006.)

Most of the insecurities that happen at sea and in ports can be categorised under the term maritime terrorism. Maritime terrorism suggests that there are terrorists groups targeting or using ships at sea or in ports' as weapons to attack passengers and personnel. Both the literature and legislation consider human casualties, economic losses, environmental damage and other negative effects as insecurities. (Eski 2011.) Ports can be used in cyberterrorism to indoctrinate fear and create both physical and economical disturbance (Boyes et al. 2016).

The planning phase is the most complex stage in the life cycle of a port, because it demands cooperation between different stakeholders. The risks there are inadequate information defining the risks and calculating the rewards. The risks also contain the use of undemonstrated technology or suppliers. (Marsh & McLennan Companies 2014.)

Design exposures or natural dangers can affect the construction phase. Design exposure refers to the loss of, or damage to uncompleted work. Crucial geological or poor soil condition findings can also affect marine construction. General natural dangers include earthquake, volcanic activity, windstorm, flooding and tidal wave, any of which can cause destructive damage to projects and processes during construction. Usually, natural dangers are unexpected and very difficult to detect in time. (Ministry of Defence of Finland 2011; Marsh & McLennan Companies 2014.)

Operations during a port's life cycle have three types of risk: assets and handling equipment risks, turnover stream risks and liability risks. Assets and handling equipment risks include the loss of or damage to assets, damage to sea walls, piers and wharves caused by natural dangers or terrorism. Turnover stream risks include actions such as strikes, denial of access or transport accidents or damage that affects critical cargo handling equipment. Liability risks include injuries towards third-party operators, loss of or damage to vessels or cargo, fines and duty and pollution risks. (Marsh & McLennan Companies 2014.)

The amount of information that a port holds itself, large monetary transfers and the number of stakeholders attract cyberattackers to target ports and port facilities. Usually, the computer systems and databases of ports contains information pertaining to 5-10 different stakeholders. (CyberKeel 2014.) For example, cyberattackers may gain access to commandeer a ship, close a port or its terminal, access delicate information such as pricing documents or time schedules, and change manifests or container numbers. Even the smallest cyberattacks can lead to business losses of millions of dollars. (Caponi & Belmont 2014.)

Port accidents, port equipment failures, hazardous goods mishandling, breaches of security, and labour strikes are the main categories of disruptions. These disruptions also have direct and indirect consequences on the operations and functions of the entire transport and supply network. The consequences also affect the economic and social well-being of the environment that surrounds the port and its operations. For example, in 2011 an earthquake seriously disrupted the operations of north-eastern Japanese ports. It also affected activities of warehouses and production facilities serving the port areas. (Kurapati et al. 2015; Loh & Thai 2015.) Potential vulnerabilities of ports include, for example, limited training and readiness for cybersecurity, software errors and coincidence, and connection and interdependence of networks (Homeland Security 2016).

4 CYBERSECURITY SCHEMES OF PORTS AND CRITICAL INFRASTRUCTURE

Because ports form a significant part of the critical infrastructure, the definitions of critical infrastructure are examined below. Chapter 4.2 presents the cybersecurity framework for critical infrastructure by the National Institute of Standards and Technology (NIST). Chapter 4.3 and 4.4 present a cybersecurity code for ports developed by the Institute of Engineering and Technology (IET), and a cyberrisk management guidelines by the International Maritime Organization (IMO).

4.1 Critical infrastructure

The history of critical infrastructure dates back to the 1980s, when several projects were carried out to define important infrastructure in the public sector. Then, important infrastructure was defined to include highways, roads, bridges, airports, public transit, water supply and wastewater facilities, and solid-waste and hazardous-waste services. As international terrorism grew in the 1990s, the term was reworked within the concept of national security. Critical infrastructure was expanded to contain, amongst other things, energy systems, nuclear power systems, shipping services and transport systems. (Ho & Ho 2006; O'Rourke 2007; Prezelj & Ziberna 2013.)

NIST defines critical infrastructure as virtual or physical systems and assets that are fundamental to the nations. The incapability and demolishment of these systems and assets has a remarkable impact on security, national economic security, public health, and safety. The European Commission has identified the critical infrastructure as facilities, networks, services, and assets of physical and information technology. (see Colesniuc 2013; Muegge & Craigen 2015.)

Critical infrastructure is seen as a very complex association, so there is demand to develop a consistent concept that could be used in times of terror. The concept is called a "lifeline system" and it measures the performance of large, geographically spread out networks when there are, for example, earthquakes, hurricanes, and other malicious natural events. These lifelines are classified into six main systems: electric power, gas and liquid fuels, telecommunications, transport, waste disposal and water supply. This concept assists to clarify characteristics that are mutual to necessary support systems. It also arranges perceptions into engineering challenges to enhance the performance of large networks. (Rinaldi et al. 2001; O'Rourke 2007; Muegge & Craigen 2015.)

Nowadays the technology of computer networks is increasing rapidly and the critical infrastructure is ever more dependent on them. There are multiple aspects to the protection of the critical infrastructure, such as protection of civilian and commercial systems and services, and military forces and systems. The civilian aspect sets a high standard whereby nations will not accept a single attack on their critical infrastructure. The military aspect considers attacks less remarkable if they do not damage national capabilities. (Lewis 2002.)

For the future, it is important to create flexible and overall methods for nations and communities to understand the importance of these infrastructures. Resilient communities need to enhance awareness through education and risk communication. Communities need also to have strong and innovative leadership, effective planning and the long-term commitment of resources that will help to place complex systems. These systems and infrastructure require accurate information on time, updated science, technology, and information that is provided by partnerships and networks between communities, governments, scientist and engineers. (Rinaldi et al. 2001; O'Rourke 2007.)

Logistical infrastructure is one of the most important infrastructure types that nations, organizations, and individuals need in order to interact. It refers to all operations and functions that are necessary to fulfil the logistical mission. There are two ways to classify basic logistical processes: 1) logistical nodes that are included in the logistical infrastructure and include warehousing and handling of goods, and 2) logistical edges that operate as links between logistical nodes. Good infrastructure exists only when the operations are quick and efficient and there are only low-level barriers to performance. (Düerkop & Huth 2016.)

Because critical infrastructure is important for every nation in the world and cybersecurity is a global matter, there needs to be developed strategies and policies for both (Miron & Muita 2014). There are three problems concerning cyberthreats and critical infrastructure: 1) Reliable information concerning these is not available to the public; 2) so called "cyber gurus" tend to over-dramatize and oversimplify risks to critical infrastructure; and 3) the information is also limited by institutional culture, competition, and public image to simple vulnerabilities of critical infrastructure. (Muegge & Craigen 2015.)

4.2 Cybersecurity framework for Critical Infrastructure

In 2014, NIST published its first framework for critical infrastructure cybersecurity. The process began on February 12, 2013 when the President of the United States signed Executive Order 13636 on Improving Critical Infrastructure Cybersecurity. The main target of the framework is to structure several approaches which help to assemble standards, guidelines, and practices for cybersecurity. It also depends on already existing global guidelines, standards, and practices. It contains three different parts which are the Framework Core, the Framework Implementation Tiers and the Framework Profile. (NIST 2014, 2017.) This framework can be implemented also in ports because they are an important part of transport critical infrastructure.

The Core includes a set of cybersecurity activities, results, and informatory references that occur in all critical infrastructure sectors. The Core also provides an elaborate guide for how critical infrastructure can develop individual organizational Profiles. When organizations have though through this in the context of cybersecurity, it provides a high-level, strategic point of view of the lifecycle of their management of cybersecurity risks. The core contains five continuous functions:

- Identify – management of possible risks to systems, assets, and capabilities.
- Protect – execution of proper safeguards that ensure delivery of critical infrastructure services.
- Detect – actions that identify the incident of a cybersecurity event.
- Respond – actions that help to detect and fight against a cybersecurity event.
- Recover – actions to maintain strategies and to restore capacities during a cybersecurity event. (NIST 2014.)

The Framework Tiers include a mechanism for critical infrastructure to explore and understand the features of their own approach to control risks of cybersecurity. When thinking about these Tiers, organizations think through their current practices for risk management, threat environment, and all requirements, objectives for business and mission and organizational constrictions. There are four Tiers. In the first Tier (Partial) the practices are informal and there is limited awareness. The second Tier (Risk Informed) contains more awareness at organizational level but it is not implemented through the whole organization. In the third Tier (Repeatable) the practices are formally approved and included in policies. In the fourth Tier (Adaptive) the practices are agile and fully aware of cybersecurity risks. (NIST 2014, 2017.)

The Framework Profiles helps organizations align their cybersecurity actions with their business requirements, risk tolerances, and resources. These Profiles give organizations the chance to identify opportunities for enhancement of their cybersecurity posture. The Current Profile refers to the outcomes of cybersecurity risks that are already being identified. The Target Profile refers to the needed outcomes which help organizations to achieve the wanted goals for cybersecurity risk management. (NIST 2014.)

4.3 Cyberrisk management strategy for ports

Because port and port operators are scattered around the globe, it is very difficult to develop an overall strategy for all members of ports and port networks. For example, the offices of a big container shipping line can be spread across 150 countries and the shipping line may operate 300 vessels. (Jensen 2015.) When cyberrisk management is effective, it considers safety and security effects consequent to the revelation or exploitation of vulnerabilities in information technology systems. Cyberrisk management should be durable and evolve as a natural extension of already existing practices and strategies of safety and security management. (IMO 2016.)

Cyberrisk management consists of the process of identifying, analysing, assessing, and communicating a cyberrisk. It also includes accepting, avoiding, transferring, or mitigating cyberrisk to a desired level. It takes into consideration the costs and advantages of actions taken by stakeholders. It aims to support safe and secure shipping that is operationally resilient to cyberrisks, and it extends from senior management level to all operators in the port facilities. (IMO 2016.)

There are five functional elements in cyberrisk management: identify, protect, detect, respond, and recover. ‘Identify’ covers all personnel roles and responsibilities that need to be defined for cyberrisk management and all systems, assets, data, and capabilities that when endangered can pose risks to the port and its ships. A decision must be made as to what information technology security standards are most suitable to the organization’s systems. Next, the systems and standards must be checked for similarities and to ascertain that the latest updates are downloaded. (Sanger et al. 2014; IMO 2016.)

‘Protect’ refers to implementation of risk control processes and measures and the contingency planning to protect cyberactivities and confirm the continuity of operations. It is not only the main organization that is at risk for cybersecurity threats, but also its suppliers, customers and other operators. The main organizations needs to involve its interest groups in the discussion of cybersecurity threats and vulnerabilities. (Sanger et al. 2014; IMO 2016.)

‘Detect’ means the development and implementation of all necessary activities that a port and its facilities need to detect a cyberattack in time. The chosen cybersecurity practices need to be run and checked through drills and exercises to identify possible gaps and shortages for improvement. ‘Respond’ refers to the activities that are needed to provide resilience and to restore systems that are necessary for operations and services. (Sanger et al. 2014; IMO 2016.)

‘Recover’ means the identification of measures that are necessary for back-up or restore of cybersystems for operations. All these selected strategies and processes for cyberthreats need to be reviewed and evaluated for the new cybersystems. These five functional elements include the activities and wanted outcomes of effective cyberrisk management in all the critical systems that affect maritime operations and information exchange (Sanger et al. 2014; IMO 2016.)

4.4 Code of Practice for ports and port systems

The Institution of Engineering and Technology (IET) has created the Code of Practice concept based on visits to numerous ports in the United Kingdom, together with the Defence Science and Technology Laboratory. The Code of Practice concept defines why it is important that cybersecurity is joined to a holistic approach for the entire life cycle of the assets. This approach can identify potential economic, reputational, and security outcomes that could emerge when threats are undetected. The concept is intended to be part of an organization’s comprehensive risk management system and business plan. This means that cybersecurity is maintained as a cost-effective part of the main business. (Boyes et al. 2016.) Figure 4 shows two main strategies of the Code of Practice and what these strategies include.

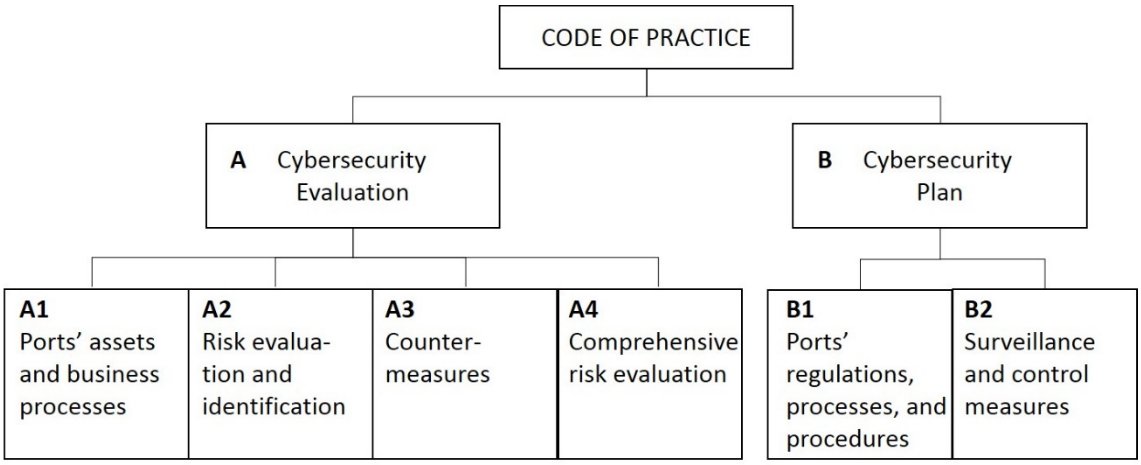

CODE OF PRACTICE
A Cybersecurity Evaluation
B Cybersecurity Plan
A1 Ports' assets and business processes
A2 Risk evaluation and identification
A3 Countermeasures
A4 Comprehensive risk evaluation
B1 Ports' regulations, processes, and procedures
B2 Surveillance and control measures

Figure 4 Structure of Code of Practice (modified from Boyes 2015; Boyes et al. 2016)

According to agreements on port security standards, cybersecurity evaluations are done on premises of ports and port facilities. The objective of security evaluations is to identify the vulnerabilities of physical structures, personnel safety systems, and business processes that may lead to security conflicts or accidents. (Boyes 2015.)

Figure 4 identifies four key elements of cybersecurity evaluation. Identification of the port's assets and resources relates to the port's different facilities, buildings, systems, and data. These assets are very important and they need to be protected. Identification and evaluation of risk helps to observe the threats that can damage the assets, infrastructure, and vulnerabilities in time. With countermeasures, ports are prepared proactively for any possible cyberattacks and cyberthreats. They also help to reduce risks and any other effects that can appear to operations from cyberthreats. Comprehensive risk evaluation consists of human factors, weaknesses of infrastructure, regulations, and methods. All these sectors are based on selected countermeasures. (Boyes et al. 2016.)

Cybersecurity plans are based on cybersecurity evaluations and the risk and threat factors that were detected by the evaluation. They should highlight and improve both the ports and the security plans of their operations. The cybersecurity plan takes into consideration the effects of port operations that have been measured in the security plan. (Boyes et al. 2016.)

For a functional cybersecurity plan, it is important that the approved approach is adopted through humans, processes, physical and technological aspects of the port. From the cybersecurity perspective, the plan should include or refer to the port's own regulations, processes, and procedures. Regulations are usually based on security influenced business regulations that are guiding the cybersecurity plan. Processes are managed with the security regulations and produce instructions for their constant production through use of port assets throughout the entire life cycle. Procedures contain detailed instructions that are linked to repeatable and constant mechanisms. With these instructions, mechanism processes can be implemented and operationally produced. (Boyes et al. 2016.)

The plan should be properly embedded into the operational timeline mechanism at least on a yearly level; it should also be inspected to make sure that it is in line with the desired intentions. The plan should be updated every time gaps, shortages or organizational changes appear, which can result from political, economic, social, technological, legal, or environmental factors. The plan should set proper and relative surveillance and control measures to be implemented throughout the life cycle of every port asset, i.e. port and security control and administration, customs and border control, cargo reception, storage and handling, and supply chain facilities. These measures should include implementation of every security regulation, processes, and procedures that affects the assets of the port. (Boyes et al. 2016.)

5 SUMMARY AND CONCLUSIONS

This report has focused on the concepts of cybersecurity and ports, and how ports are affected by cybersecurity. It has also helped to understand and clarify the aspects of cybersecurity that ports are going to face in the future.

Chapter 2 focused on cyberspace and cybersecurity. Cyberspace has been researched very extensively, unlike cybersecurity, which it is a relatively new concept. Both these concepts should be researched continuously because of the development speed of technologies and information systems. Several key driving forces helps organizations, and especially ports, to see how cyberspace performs. In cyberspace there is no fixed time, and cyberattacks can occur either immediately or take longer to have an influence the target. 'Space' refers to the fact that no one is safe from cyberattacks and there are no fixed boundaries in cyberspace. The key challenge in cyberspace is that anyone can operate in it while remaining anonymous. 'Asymmetry' refers to the exploitation of an opponent's weak point and maximization of the competitive advantage gained from the cyberattack. 'Efficiency' aims to disrupt an opponent's operations in cyberspace by performing multiple actions simultaneously in different dimensions.

The key concern of cybersecurity is that today, individuals with a bare minimum of equipment and knowledge of cyberspace or its techniques can launch a cyberattack. Usually, smaller cyberattackers aim to draw attention to how easily the ICT systems of organizations and ports can be hit, but cyberattacks are also happening on a large scale with severe consequences. Although five cyberthreats have been identified so far (hacktivism, cybercriminality, cyberespionage, cyberterrorism and cyberwar), new threats continue to emerge. Especially for ports the threats focus on cyberespionage and cybercriminality, because their data systems contain huge amounts of information relating to transport schedules and customers. Vulnerabilities are usually malfunctions or gaps in ICT systems.

Chapter 3 presented a literature perspective on ports and how they see their security operations. Ports have a long history of being the main link between nations and international trade. They are not an easy subject of researches due to the many operators inside the port area. Even though a port itself may have developed usable strategies and processes for cybersecurity, its operators may not belong to the port's strategies and may therefore need to develop their own cybersecurity approaches. The development of ports is still ongoing, and operations depend heavily on ICT systems. The journey of ports in the context of cybersecurity started only few years back, which means that few frameworks have been established to help them understand cybersecurity issues.

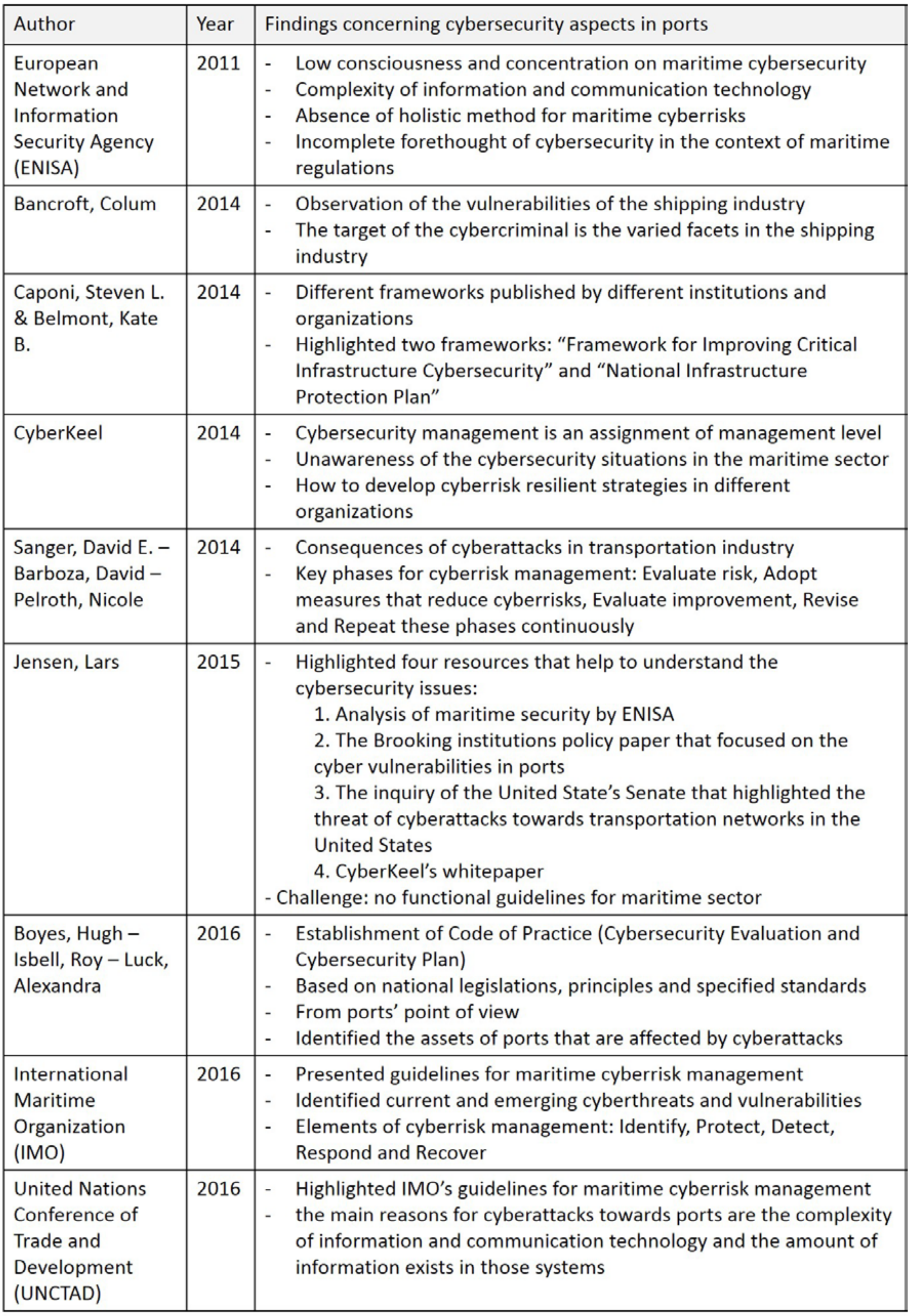
Chapter 4 looked at a few examples of how ports can manage their cybersecurity and several frameworks were examined. It would be good to understand the advantages that can be gained from even partial use of the given. There are three main methods that they can use for adoption of the frameworks: 1) Ports should develop information campaigns about cyberrisks that may threaten the maritime sector. Such campaigns would help employees and port operators adapt to and deal with cyberrisks and cyberthreats. 2) Ports should discuss and develop strategies regarding cyberthreats together with their customers, who will usually be fully aware of cyberthreats that their cargo faces during transport. 3) Ports should establish “cyberpremiums” on their insurance policies, which would highlight the degree to which they follow to these optional frameworks.

At the time writing, we recognized that the work and research on cybersecurity is still in its infancy. Much work needs to be done between nations, governments, the private sector, and individual citizens. This requires a complete strategy involving coordinated actions between the above-mentioned groups. Because cyberthreats are growing, there has to be instant action and cooperation between members of the global community and ongoing attention to, and study of, this subject.

Table 1 lists the articles used in the writing this report that deal with the concepts of cybersecurity and ports. The earliest article on this topic was ENISA’s paper published in 2011. It concentrated on defining what cybersecurity means for the maritime sector and what aspects of the port environment are affected by it. ENISA also highlighted the concerns that needs to be researched and identified in the future, so that cybersecurity is fully understood and managed across the maritime sector.

We noticed that the latest articles used the same definitions and frameworks to indicate cybersecurity. For example, Jensen (2015) used four frameworks to determine how cybersecurity is largely seen in the maritime sector. Our report took a closer look at two of these frameworks. We used ENISA’s analysis for cybersecurity in the maritime sector and the whitepaper of CyberKeel.

Table 1 List of articles that have researched cybersecurity in ports



Author	Year	Findings concerning cybersecurity aspects in ports
European Network and Information Security Agency (ENISA)	2011	- Low consciousness and concentration on maritime cybersecurity - Complexity of information and communication technology - Absence of holistic method for maritime cyberrisks - Incomplete forethought of cybersecurity in the context of maritime regulations
Bancroft, Colum	2014	- Observation of the vulnerabilities of the shipping industry - The target of the cybercriminal is the varied facets in the shipping industry
Caponi, Steven L. & Belmont, Kate B.	2014	- Different frameworks published by different institutions and organizations - Highlighted two frameworks: "Framework for Improving Critical Infrastructure Cybersecurity" and "National Infrastructure Protection Plan"
CyberKeel	2014	- Cybersecurity management is an assignment of management level - Unawareness of the cybersecurity situations in the maritime sector - How to develop cyberrisk resilient strategies in different organizations
Sanger, David E. – Barboza, David – Pelroth, Nicole	2014	- Consequences of cyberattacks in transportation industry - Key phases for cyberrisk management: Evaluate risk, Adopt measures that reduce cyberrisks, Evaluate improvement, Revise and Repeat these phases continuously
Jensen, Lars	2015	- Highlighted four resources that help to understand the cybersecurity issues: 1. Analysis of maritime security by ENISA 2. The Brooking institutions policy paper that focused on the cyber vulnerabilities in ports 3. The inquiry of the United State's Senate that highlighted the threat of cyberattacks towards transportation networks in the United States 4. CyberKeel's whitepaper - Challenge: no functional guidelines for maritime sector
Boyes, Hugh – Isbell, Roy – Luck, Alexandra	2016	- Establishment of Code of Practice (Cybersecurity Evaluation and Cybersecurity Plan) - Based on national legislations, principles and specified standards - From ports' point of view - Identified the assets of ports that are affected by cyberattacks
International Maritime Organization (IMO)	2016	- Presented guidelines for maritime cyberrisk management - Identified current and emerging cyberthreats and vulnerabilities - Elements of cyberrisk management: Identify, Protect, Detect, Respond and Recover
United Nations Conference of Trade and Development (UNCTAD)	2016	- Highlighted IMO's guidelines for maritime cyberrisk management - the main reasons for cyberattacks towards ports are the complexity of information and communication technology and the amount of information exists in those systems

The articles highlighted in Table 1 give an excellent picture of cybersecurity aspects in the maritime sector. However, what we found lacking was differences of opinions by the authors of these articles. They had very similar opinions about cybersecurity, but some had also found new aspects to add to their results. For example, the two articles that contained frameworks such as the Code of Practice by Boyes, Isbell and Luck (2016) and the guidelines for maritime cyberrisk management by IMO (2016) contained a great amount of information and different concepts of cybersecurity.

Future research should focus on measuring how different kinds of frameworks and strategies have influenced ports' operations and strategies. In this report we mentioned a few of these frameworks and strategies, but those articles do not define the outcomes. It is necessary for ports to compare their strategies and processes in order to cooperatively enhance their resilience to cyberattacks. Some suggestions for future research could be:

- What existent cybersecurity frameworks do ports use or have they used?
- How do ports see their current situation in respect to cyberattacks?
- What is the concrete number of systems in the ports that rely on information and communication technologies?
- How are the information and communication technologies of ports protected from cyberattacks?

Future researches will need the cooperation of a great number of experts and port operators. Collaboration between different port operators and experts in cyberspace and cybersecurity could establish new specified frameworks and concepts. Countries have started to establish overall directions for individuals, organizations and institutions that help them observe and understand in what ways cybersecurity issues affect daily life. Some countries such as United States and United Kingdom have developed specified directions for their maritime sector and ports to use and adopt in their business strategies. However, there is need for a global cybersecurity framework for ports, or at least a regional one such as a European cybersecurity framework.

In future, the key development scene in cyber security will be the development of a specific cyberthreat intelligence service. It would compile basic information patterns and could help improve or repair endangered systems. It could also be customized entirely to the needs of individual clients and offer the future threat analysis, factors and methods that can be used for both tactical functions and long-term security strategies.

REFERENCES

Afful-Dadzie, Anthony – Allen, Theodore T. (2014) Data-Driven Cyber-Vulnerability Maintenance Policies. *Journal of Quality Technology*. Vol 46 (3), 234–250.

Alderton, Patrick M. (2008*) Lloyd's Practical Shipping Guides*. Port Management and Operations. Third ed. Informa, London.

Ashby, W. Ross (1956) *An Introduction to Cybernetics*. John Wiley and Sons Inc., New York.

Babcock, Chris (2015) Preparing for the Cyber Battleground of the Future. *Air & Space Power Journal*. November-December 2015, Vol 29 (6), 61–73.

Bancroft, Colum (2014) *Cyber Crime and the Shipping Industry*. Published 3.11.2014.

Benedikt, Michael (1991) *Introduction to Cyberspace: First Steps*. MIT Press.

Bichou, Khalid (2004) the ISPS Code and the Cost of Port Compliance: An Initial Logistics and Supply Chain Framework for Port Security Assessment and Management. *Maritime Economics & Logistics*. Vol 6 (4), 322–348.

Bichou, Khalid – Gray, Richard (2004) A logistics and supply chain management approach to port performance measurement. *Maritime Policy & Management*. Vol 31 (1), 47–67.

Boyes, Hugh (2015) Cyber Security and Cyber-Resilient Supply Chains. *Technology Innovation Management Review*. Vol 5 (4), 28–34.

Boyes, Hugh – Isbell, Roy – Luck, Alexandra (2016) *Code of Practice. Cyber Security for Ports and Port Systems*. Institution of Engineering and Technology. 28.6.2016. United Kingdom.

Caldeirinha, Vitor P. – Felício, J. Augusto (2014) the relationship between 'position-port', 'hard-port' and 'soft-port' characteristics and port performance: conceptual models. *Maritime Policy & Management*. Vol 41 (6), 528–559.

Caponi, Steven L. – Belmont, Kate B. (2014) *Maritime Cybersecurity: A Growing Threat Goes Unanswered*. Published 22.10.2014.

Chertoff, Michael (2008) the cybersecurity challenge. *Regulation & Governance*. Vol 2, 480–484.

Colesniuc, Dan (2013) Cyberspace and Critical Information Infrastructure. *Informatica Economica*, Vol 17 (4), 123–132.

Craigen, Dan – Diakun-Thibault, Nadia – Purse, Randy (2014) Defining Cybersecurity. *Technology Innovation Management Review*. Vol 4 (10), 13–21.

CyberEdge Group (2014) *2015 Cyberthreat Defense Report North America and Europe*. Published 2014.

CyberKeel (2014) *Maritime Cyber-risks*. Copenhagen, Denmark. Published 15.10.2014.

Düerkop, Sascha – Huth, Michael (2016) Risk analysis and evaluation for critical logistical infrastructure. *Ekonomski Vjesnik/Econviews.* Vol 29, 11–19.

Electronic Communication Networks <http://www.businessdictionary.com/definition/Electronic-Communication-Network-ECN.html> retrieved 24.5.2017.

ENISA (2011) *Analysis of cyber security aspects in the maritime sector*. European Network and Information Security Agency.

Eski, Yarin (2011) ‘Port of call’: Towards a criminology of port security. Criminology & Criminal Justice. Vol 11 (5), 415–431.

European Commission (2017) *Critical Infrastructure*. <https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en> retrieved 17.2.2017.

FireEye and Marsh & McLennan Companies (2017) *Cyber Risk Report 2017 – Cyber Threats: a Perfect Storm about to Hit Europe?* Published January 2017.

Fitzpatrick, William M. – Dilullo, Samuel A. (2015) Cyber Espionage and the S.P.I.E.S Taxonomy. *Competition Forum*. Vol 13 (2), 307–336.

Fok, Edward (2013) an Introduction to Cybersecurity Issues in Modern Transportation Systems. *Institute of Transportation Engineers Journal*. Vol 83 (7), 18–21.

Geers, Kenneth (2009) The Cyber Threat to National Critical Infrastructures: Beyond Theory. *Information Security Journal: A Global Perspective*, Vol 18 (1), 1-7

Graham, Chris (2017) NHS cyber attack: Everything you need to know about ‘biggest ransomware’ offensive in history. *The Telegraph*. Published 20 May 2017. <http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything--know-biggest-ransomware-offensive/>

Hanska, Jan – Limnéll, Jarno (2013) *The Driving Forces in Cyberspace are Changing the Reality of Security*. Stonesoft Corporation International Helsinki, Finland. Stonesoft Inc. Americas Headquarters Atlanta, USA.

Ho, Mun Wai – Ho, Kim Hin (2006) Risk Management in Large Physical Infrastructure Investments: The Context of Seaport Infrastructure Development and Investment. *Maritime Economics & Logistics*. Vol 8, 140–168.

Homeland Security (2016) Consequences to Seaport Operations from Malicious Cyber Activity. *National Protection and Programs Directorate*. Published 03.03.2016.

Hult, Fredrik – Sivanesan, Giri (2013) Introducing Cyber. *Journal of Business Continuity & Emergency Planning*. Vol 7 (2), 97–102.

IMO (2016) *Interim Guidelines on Maritime Cyber Risk Management*. London, United Kingdom. MSC. 1/Circ. 1526, Published June 2016.

Jensen, Lars (2015) Challenges in Maritime Cyber-Resilience. *Technology Innovation Management Review*. Vol 5 (4), 35–39.

Khan, Omera – Burnes, Bernard (2007) Risk and supply chain management: creating a research agenda. *The International Journal of Logistics*. Vol 18 (2), 197–216.

Kurapati, Shalini – Lukosch, Heide – Verbraeck, Alexander – Brazier, Frances M. T. (2015) Improving Resilience in Intermodal Transport Operations in Sea-port: a Gaming Approach. *EURO J Decis Process*. Vol 3, 375–396.

Limnéll, Jarno – Majewski, Klaus – Salminen, Mirva (2014) *Cyber Security for Decision Makers*. Docendo, Jyväskylä.

Lee, Robert M. (2013) the Interim Years of Cyberspace. *Air & Space Power Journal.* January-February 2013, 58–79.

Lewis, James A. (2002) Assessing the Risk of Cyber Terrorism, Cyber War and Other Cyber Threats. *Centre for Strategic & International Studies (CSIS).*

Lewis, James A. (2006) Cybersecurity and Critical Infrastructure Protection. *Centre for Strategic and International Studies*. Published January 2006.

Loh, Hui Shan – Thai, Vinh V. (2015) Management of disruptions by seaports: preliminary findings. *Asia Pacific Journal of Marketing and Logistics*. Vol 27 (1), 146–162.

Luppicini, Rocci (2014) Illuminating the dark side of the Internet with actor-network theory: An integrative review of current cybercrime research. *Global Media Journal – Canadian Edition*. Vol 7 (1), 35–49.

Ma, Shuo (2002) Economics of Maritime Safety and Environment Regulations. In: *The Handbook of Maritime Economics and Business*. Editor Costas Th. Grammenos. London and Hong Kong. 399–425.

Marsh & McLennan Companies (2014) *Ports and Terminals – risk challenges and solutions*. Global Infrastructure and Marine Practices. Published 7/2014.

Ministry of Defence of Finland (2011) *Security Strategy for Society*. Government Resolution 16.12.2010. Ministry of Defence, Helsinki.

Miron, Walter – Muita, Kevin (2014) Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure. *Technology Innovation Management Review*. Vol 4 (10), 33–39.

Muegge, Steven – Craigen, Dan (2015) a Design Science Approach to Constructing Critical Infrastructure and Communicating Cybersecurity Risks. *Technology Innovation Management Review*. Vol 5 (6), 6–16.

NIST (2014) *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology. Version 1.0. Published February 12, 2014.

NIST (2017) *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology. Version 1.1. Published January 10, 2017.

Notteboom, Theo E. – Rodrigue, Jean-Paul (2005) Port regionalization: towards a new phase in port development. *Maritime Policy & Management*. Vol 32 (3), 297–313.

O'Rourke, T. D. (2007) Critical Infrastructure, Interdependencies, and Resilience. *The Bridge - Linking Engineering and Society.* Vol 37 (1), 22–29.

Pettit, S. J. – Beresford, A. K. C. (2009) Port development: from gateways to logistics hubs. *Maritime Policy & Management*. Vol 39 (3), 253–267.

Pinto, C. Ariel – Talley, Wayne K. (2006) the Security Incident Cycle of Ports*. Maritime Economics & Logistics*. Vol 8, 267–286.

Platt, Victor (2011) Still the fire-proof house? An analysis of Canada's cybersecurity strategy. *International Journal*. Published winter 2011-12, 155–167.

Prezelj, Iztok – Ziberna, Ales (2013) Consequence-, time- and interdependency-based risk assessment in the field of critical infrastructure. *Risk Management*. Vol 15 (2), 100–131.

Rinaldi, Steven M. – Peerenboom, James P. – Kelly, Terrence K. (2001) Identifying, Understanding, and Analysing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine*. Vol 21 (6), 11–25.

Rupert, Kendrick (2010) Cyber Risks for Business Professionals - a Management Guide. IT Governance Publishing, United Kingdom

Sanger, David E. – Barboza, David – Pelroth, Nicole (2014) *Cyber Security*. United States Coast Guard. Published 31.10.2014.

Shackleford, Dave (2015) *Combatting Cyber Risks in the Supply Chain*. SANS Institute. Published September 2015.

Song, Dong-Wook – Panayides, Photis M. (2008) Global Supply Chain and Port/Terminal: Integration and Competitiveness. *Maritime Policy and Management*. Vol 35 (1), 73-87.

Thai, Vinh V. – Grewal, Devinder (2007) the Maritime Security Management System: Perceptions of the International Shipping Community. *Maritime Economics & Logistics*. Vol 9 (2), 119–137.

UNCTAD (2016) *Review of Maritime Transport 2016*. United Nations Conference on Trade and Development. United Nations Publication. ISBN 978-92-1-112904-5

9/11 attacks < http://www.history.com/topics/9-11-attacks>, retrieved 29.5.2017.

HAZARD project has 15 full Partners and a total budget of 4.3 million euros. It is executed from spring 2016 till spring 2019, and is part-funded by EU's Baltic Sea Region Interreg programme.

HAZARD aims at mitigating the effects of major accidents and emergencies in major multimodal seaports in the Baltic Sea Region, all handling large volumes of cargo and/or passengers.

Port facilities are often located close to residential areas, thus potentially exposing a large number of people to the consequences of accidents. The HAZARD project deals with these concerns by bringing together Rescue Services, other authorities, logistics operators and established knowledge partners.

HAZARD enables better preparedness, coordination and communication, more efficient actions to reduce damages and loss of life in emergencies, and handling of post-emergency situations by making a number of improvements.

These include harmonization and implementation of safety and security standards and regulations, communication between key actors, the use of risk analysis methods and adoption of new technologies.

See more at: http://blogit.utu.fi/hazard/

EU STRATEGY FOR THE BALTIC SEA REGION FLAGSHIP

HAZARD

Interreg Baltic Sea Region

EUROPEAN UNION EUROPEAN REGIONAL DEVELOPMENT FUND