Newsletter No 4 Issued September 2017

MITIGATING THE EFFECTS OF EMERGENCIES IN THE BALTIC SEA REGION PORTS 2016-2019

blogit.utu.fi/hazard

HAZARD project aims at mitigating the effects of emergencies in major seaports in the Baltic Sea Region. The types of safety and security emergencies include, for example, leakages of hazardous materials, fires on passenger ships at ports, oil spills in port areas as well as explosions of gases and chemicals. The project enables better preparedness through joint exercises, improved communication between authorities in emergencies, better compliance of regulatory framework and better use of risk assessment methods and as well as faster adoption of state-of-art technologies.

CYBERSECURITY IN PORTS SEMINAR, 5 JUNE 2017

HAZARD project arranged together with the Finnish Port Association and the Finnish Port Operators Association a seminar on Cyber-security in Ports.

In the afternoon event, four presentations were performed by: Miikka Salonen from the National Cyber Security Centre Finland, Antti Arkima from the Finnish Transport Agency, Kalle Luukkainen from the National Emergence Supply Agency, and Sami Rakshit from the Customs.

More information on the event can be found from the project's website: blogit.utu.fi/hazard

Photos: Mariikka Whiteman

LITERATURE REVIEW ON CYBERSECURITY IN PORTS

HAZARD project has published a conceptual report *Cybersecurity in Ports*, which was built upon a comprehensive literature review conducted by research assistant Ms. Jenna Ahokas.

Aim of the report is to clarify the main points and definitions of cyberspace and cybersecurity for ports and port operators.

You can find and download the report from project's website: blogit.utu.fi/hazard/what-effects-does-cybersecurity-have-on-ports

From the project's website can also be found a few Excel-files that contain cybersecurity related references and information concerning cyberattacks.

A rewritten version of the report, which was conducted by Ms. Jenna Ahokas, Dr Tuomas Kiiski, Dr Jarmo Malmsten and Prof Lauri Ojala, was accepted to the Hamburg International Conference of Logistics on 12-13 Oct 2017.

CYBERSECURITY IN GENERAL

The complexity of cyber-related issues and missing terminology make it difficult to establish efficient strategies and/or guidelines for mitigation of cyberrisks and cyberthreats.

Figure 1 presents the conceptual description of the role of cybersecurity (C) is as follows. All action is taking place in cyberspace (A), where a system (B) is located and is protected by cybersecurity (C). System vulnerabilities (D) with existing cyberthreats (F) and the level of cybersecurity (C) comprise the level of cyberrisk (E) at any given time.

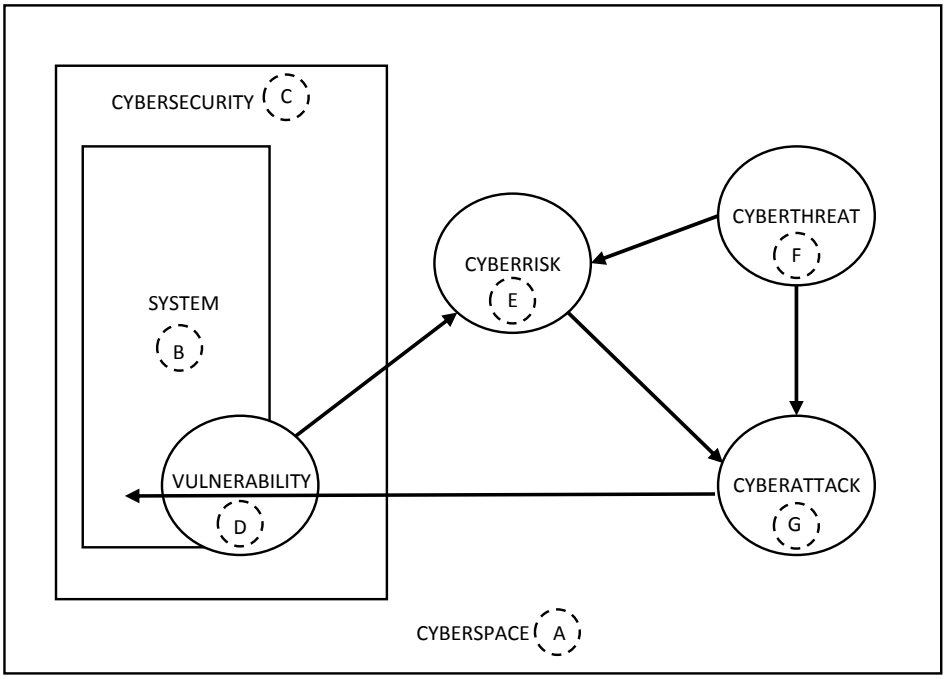

Figure 1 Simplified process chart of concepts related to cybersecurity

In case of cybersecurity (C) is not at adequate level, cyberrisk (E) may be realized, resulting a cyberattack (G), which targets the system (B) through noticed vulnerability (D).

In practice, cyberattack (G) can be considered as a materialized cyber-threat (F), which contains also specific technical methods to inflict damage.

To create a cyberattack (G), a cyber-attacker may use methods such as phishing, malicious software i.e. malware, and Denial-of-Service (DoS) attack.

PORTS IN THE CONTEXT OF CYBERSECURITY

A port is a complex cyberenvironment which contain the interconnected networks of both information and cyber physical systems (CPS) in its operations on land and at sea.

The amount of information that a port holds itself, large monetary transfers and the number of stakeholders involved in the supply chain attract cyberattackers to target ports and port facilities.

In the next page is presented the known cyberattacks that have impacted ports in one way or another.

Photo: Esko Keski-Oja

Newsletter No 4 Issued September 2017

CYBERATTACKS IN THE MARITIME SECTOR

A successful cyberattack on a port or maritime transport system could result, for example, in physical damage to critical infrastructure, disruption to supply chains, theft of sensitive information and/or support to criminal activities such as smuggling or cargo theft.

The concerns relating to cybersecurity have already materialized as the number of cyberattacks have shown a year-by-year increase, causing substantial financial losses to society in general and business in particular. Table 1 presents the cyberattacks in the maritime sector around the globe.

YEAR	ATTACKED PORTS	ATTACKED OPERATIONS	DURATION
2017	80 APM Terminals of Moller-Maersk	ICT systems, and vessel handling operations	From June 28 to July 9
2016	Unknown port in the United States	Business email of CEO of a port facility	Unknown
2016	Numerous ports in the United States	Navis, a maritime transport logistics software suite	Took place in August 2016
2014	Unknown port in the United States	Global Positioning Systems of four port cranes	Seven hours
2013	Numerous port in Japan and Korea	Container information systems	Started 2011 and ended 2013
2012	Australian Customs and Border Protection	Cargo systems	Unknown
2011	Port of Antwerp in Belgium	Container information systems	From June 2011 to 2013

Table 1 Recent cyberattacks in the maritime sector

CYBERSECURITY GUIDELINES AND STRATEGIES FOR THE MARITIME SECTOR

Few voluntary maritime cybersecurity strategies have been published by maritime authorities and international organizations. In general, it can be seen that each of the maritime cybersecurity publications approach the subject from the general risk management perspective.

Table 2 shows that in 2016 was published a large number of different cybersecurity guidelines and strategies for the maritime sector.

In the project's website can be found a list of the current cybersecurity guidelines and strategies for the maritime sector. The Excel-file also includes a list of maritime cybersecurity reports by international organizations.

YEAR	AUTHOR	TITLE
2017	BIMCO, CLIA, ICS, INTERTANKO and INTERCARGO	The Guidelines on Cyber Security Onboard Ships, Vol 2.0
2016	American Bureau of Shipping (ABS)	ABS CyberSafetyTM Series (Volume 1, 2 and 3)
2016	BIMCO, CLIA, ICS, INTERTANKO and INTERCARGO	The Guidelines on Cyber Security Onboard Ships, Vol 1.0
2016	Institution of Engineering and Technology (IET)	Code of Practice: Cyber Security for Ports and Port Systems
2016	International Maritime Organization (IMO)	Interim Guidelines on Maritime Cyber Risk Management MSC.1/Circ.1526
2016	Transport Canada	Understanding Cyber Risk: Best Practices for Canada's Maritime Sector
2015	Coast Guard of the United States	Cyber Strategy

Table 2 Current maritime cybersecurity guidelines and strategies

CONTACT **Project Director**
Prof Lauri Ojala
E-mail: lauri.ojala@utu.fi
Mobile: +358 50 502 7031

Project Manager
Dr Jarmo Malmsten
E-mail: jarmo.malmsten@utu.fi
Mobile: +358 50 409 1493

Communication Manager
Mariikka Whiteman
E-mail: mariikka.whiteman@utu.fi
Mobile: +358 40 779 9490

Post address:
Turku School of Economics
FI-20014 University of Turku
Finland

NEXT STEPS OF CYBERSECURITY IN THE MARITIME SECTOR

Current studies and publications show that regardless of the growing awareness of cybersecurity, much work needs to be done in order to mitigate the cyberthreats in ports. Maritime sector needs to adopt industry standards and practical level coordination.

Multiple studies have pointed out the low awareness of cybersecurity in the maritime sector. Many maritime authorities and international organizations have started to develop strategies and standards for ports, port facilities and ships against cyberthreats.

Still there is lack of mandatory regulations concerning cybersecurity. However, the International Maritime Organization (IMO) has taken a major leap in terms of awareness of cybersecurity. IMO is going to make the Interim Guidelines on Maritime Cyber Risk Management (MSC.1/Circ.1526) mandatory onboard ships after 1 January 2021. Similar steps for ports are still pending.

In the future, it is desired to establish a fixed and clear terminology for cybersecurity issues. Future studies should be focused on the current cybersecurity practices and the empirical evidence of their implementation. For example, on how different cybersecurity strategies have been implemented empirically and how effective they are in terms of mitigating cyberthreats.

Photo in bottom left corner: Esko Keski-Oja
Other photos: Päivi Söderholm

CONTACT **Project Director**
Prof Lauri Ojala
E-mail: lauri.ojala@utu.fi
Mobile: +358 50 502 7031

Project Manager
Dr Jarmo Malmsten
E-mail: jarmo.malmsten@utu.fi
Mobile: +358 50 409 1493

Communication Manager
Mariikka Whiteman
E-mail: mariikka.whiteman@utu.fi
Mobile: +358 40 779 9490

Post address:
Turku School of Economics
FI-20014 University of Turku
Finland