Smart Terminal System of Systems' Cyber Threat Impact Evaluation

Jussi Simola, Jouni Pöyhönen and Martti Lehto
University of Jyväskylä, Jyväskylä, Finland

Jussi.hm.simola@jyu.fi
jouni.a.poyhonen@jyu.fi
martti.j.lehto@jyu.fi

Abstract: Systems of system-level thinking is required when the purpose is to develop a coherent understanding of the ecosystem where every user and system requirements are divided into specific parts. The smarter project, as a part of the Sea4value program of DIMECC, aims to develop harbor operations, including passenger and cargo transportation, in a way that port processes will improve, emissions will decrease, and overall security will enhance in smart ports. This paper describes cyber-attack impacts against the Smart terminal system of systems in the cyber realm by utilizing the MITRE ATTACK® framework to map the objectives of threat actors. The Smart Terminal system environment includes ICT, ICS networks and components, communication systems, and port service systems. Internal and external threat sources or actors are hard to divide exactly because of the diversity of the threats. Hybrid threats challenge maritime domain awareness globally. The cyber threat impacts on IT and OT environments are connected to each other because of the use of internal and external networks that impact each other by combining vulnerabilities and threats. Well-working port and terminal operations require not only protected operational systems or sensor systems, but human errors must also be minimized. Objectives of threat actors are presented, categorized, and listed. Threat scenarios illustrate that cyber threats and risks are mainly similar in the maritime global-linked port community and basic hinterland trade. The networked supply chain of the business causes evolving and combined threat scenarios. European and international standards, regulations, policies, recommendations, and, e.g., guidelines by the IMO, set new cyber-threat requirements for port and terminal services and facilities. Therefore, overall security must be considered when cyber-security is the development area. Information exchange in an understandable form is essential for maintaining business continuity. Threat information has to be transferred among stakeholders as well as cyber security codes have to be followed in the port operations of partners that are involved, for example, in operational and system-level actions. Digitalization in smart ports and terminals enhances the capacity to handle cargo and passengers more efficiently, but cyber threats evolve.

Keywords: Business Continuity, ICT, ICS, Threat (Impacts), Cyber Ecosystem, Terminal Systems of Systems

1. Introduction

This research belongs to the cyber security research actions of the SMARTER. The project goals are conducted to the reduction of emissions by optimizing harbor operations and improving cargo and people flow while improving the experience for all stakeholders. (DIMECC, 2020).

The harbor environment or maritime domain is a more changeable and challenging cyber security environment than other domains in urban areas. The diversity of the port ecosystem creates challenges for the stakeholders to maintain cyber situational awareness as a part of the port overall situational awareness. It is not enough that necessary Information and Communication Technology (ICT) and Industrial Control Systems (ICS) or Operational Technology (OT) systems aided port facilities and functions such as communication, equipment operation, cargo, and other internal and external business work independently. Separated systems challenge cybersecurity management as a part of overall security & safety management. Well-organized port governance with a business continuity strategy plan has to be implemented in an upper-level framework for the other plans of security & safety management -sectors. For example, human resources plans must be in a form that has a connection to cybersecurity plans. Human resources are a crucial part of overall cyber security, where human errors are essential factors in the cyber-physical threat world. Individual skills and abilities to percept the environment must be considered in continuous work education. Threat and risk assessments have to be clearly defined. Port authorities are crucial actors in the area of cybersecurity, The instance that owns and govern the harbors area is responsible for overall security being realized, and the maritime ecosystem stays as safe as possible. That requires shared situational awareness of the maritime domain and supply chain dependencies.

Cyber threats have risen to a top threat list in harbor areas because of digitalization, transport volumes, foreign political change, and business transformation (Atlantic Council, 2020; ENISA, 2019). Enhancing transportation and people flow is not straightforward because we must protect all procedures and processes that new political risks and threats may cause. An unstable political atmosphere expands the need for new threat-prevention mechanisms. The protected maritime domain is the crucial entity for securing intelligent systems that use multiagent AI -solutions in ports and terminals. The cyber-physical security of ports is emphasized because of

the development of political polarization. Core stakeholders and all other operators involved should follow common guidance in the future.

This fourth Smarter paper is the next step of our research process and handles phenomena of cyber threat impacts and risk scenarios. The paper concentrates on the importance of threat impact awareness in the terminal and the port process. It gives an answer at this phase of the research by using the question of what objects of cyber-attack impacts in Smart Terminal System of Systems have to take into account in cyber threat impact evaluation. The research will specify the comprehensive cyber security aspects to architect risk scenario assessment and cyber security measures for the SMARTER project. This paper is one of the outcomes of the project's final report.

2. Central concepts related to smart ports and terminals

2.1 IAPH and ICCA

The International Association of Ports and Harbors (IAPH) was founded in 1955. Member ports of IAPH handle over 60 percent of global maritime trade and around 80 percent of world container traffic. IAPH has a consultative Non-Government Organization (NGO) -based status with several United Nations agencies (IAPH, 2022a). Authorities of the state define the Port area and the ISPS -Code defines its facilities in which maritime and other activities occur (IET, 2022). Almost equal old association to IAPH, The International Cargo Handling Coordination Association (ICHCA) is dedicated to improving the safety, security, sustainability, productivity, and efficiency of cargo handling by all modes and through all phases of national and international supply chains. ICHCA International's privileged NGO status enables it to represent its members and industry at large in front of national and international agencies and regulatory bodies, including IMO. The International Technical Panel of ICHCA also provides technical advice and publications on a wide range of practical cargo handling issues. (IAPH, 2022b).

2.2 BIMCO

It is the most prominent international organization representing the interests of ship owners, charterers, brokers, and agents. The Bimco's primary role is the preparation of global regulations and policy recommendations in many areas related to the MTS, from the environment, crew support, and insurance to maritime safety and security and digitalization, including guidelines for maritime cybersecurity. (Atlantic Council, 2021).

2.3 IMO and ENISA

The maritime agency of the United Nations, the International Maritime Organization (IMO) mission is to develop a regulatory framework for international shipping. The IMO Maritime Safety Committee released a set of Maritime Cyber Risk Management recommendations for safety-management systems that IMO recommended shippers implement before the first annual verification of a vessel's Document of Compliance and Safety Management in 2021. (Atlantic Council, 2021; IMO, 2021). The European Union Agency for Cybersecurity (ENISA) is the EU's lead agency for common standards of cyber defense throughout Europe. It has introduced four cyberattack scenarios at the port community level as table 1 demonstrated (ENISA, 2019).

Table 1. Cyber-attack Scenarios selected by ENISA (2019).

Scenario A	Compromising on critical data to steal high-value cargo or allow illegal trafficking through a targeted attack
Scenario B	Propagation of ransomware leading to a total shutdown of port operations
Scenario C	Compromise of Port Community System for manipulation or theft of data
Scenario D	Compromise of OT systems creating a major accident in port areas

2.4 Maritime domain awareness

The maritime domain consists of several maritime-based sectors that create the interacting entity. Achieving common Situational Awareness (SA) requires shared situational awareness that consists of similar unchanged elements at every stage. Separate sectors of the maritime domain cannot cooperate by forming their understanding of the atmosphere independently from other actors. Therefore, a crucial factor in undistributed continuity management is common maritime situational awareness. It is helpful to classify sector-based situational awareness for creating an understandable entity. System of system-level thinking depends on the

human ability to understand the dependencies of supply chains. If we can't make a network regarding the system and business dependencies, it is challenging to develop a framework from the smaller components.

It is essential to divide different parts of situational awareness: technological SA.– organizational SA. – SA of human resources – SA. of business management – SA. of transportation – SA of regulations and policies. If all segments are well-defined and linked to each other in a way that information sharing and exchange support core functions, shared situational awareness could be achievable. Common SA. differs from Shared SA. In a concept meaning, common means a level of understanding.

Stakeholders of the harbors have to create a preliminary risk assessment where every potential threat has been considered. Previous studies related to Simola & et al. (2021) realized hybrid threats where cyber and physical risk elements are combined based on crucial human factors. It is not appropriate that risk classifications have been done separately from other risk assessments. The cyber risk assessment is an essential part of the overall risk assessment in the port. **Figure** 1 illustrates how the critical elements of the port have to analyze precisely. The risk management framework for the port functionalities may support the decision-making process, in which essential operators of infrastructure or partners undertake to cooperate in influencing the selection of risk management measures. It can be tailored to different operating environments and applies to all threats (DHS, 2013). Risk management is the "process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level at an acceptable cost (DHS, 2013). In this study, the last three sections of the framework are under consideration for risk and continuity management. We cannot eliminate threats, but we can eliminate their realization and manage them. Analyzing potential threat scenarios and objects helps to identify the tools and solutions what to use in proactive cyber-physical threat prevention mechanisms (the green and blue arrow).

Figure 1 Critical Infrastructure Risk Management (Modified from DHS 2013)

Using the simple risk management concept allows security&safety operators (e.g., Situation Center or Security Operations Center) to focus on those threats that are likely to cause risks and to use approaches designed to prevent or mitigate the effects of these potential incidents. Cybersecurity and security plans have to be a part of overall risk management and continuity management activities, where policies, processes, and procedures are defined and implemented.

3. Port and terminal system of systems

Port systems consist of several systems that handle information sharing between ICT and ICS/OT systems. Fully automated terminals exploit artificial intelligence systems by using smart sensor technology. System complexity creates challenges because several functionalities are crucial for the maritime entity. Well-scheduled port processes are a vital element for the flowing operations. For example, If timetables are not synchronized, delays may happen between the operators. Interrupted extension connections from harbors by trains and airplanes affect the whole transport supply chain. If a potential cyber-attack risk scenario is realized, functional cargo and passenger traffic faces challenges. Delays impact all stakeholders' continuity management.

3.1 Managing cyber security & Security operation centers (SOC)

Cyber Security Assessment (CSA) & Cyber Security Plan (CSP) are essential elements when establishing a cyber security management framework as part of a business continuity management framework. According to (IET, 2016; U.S Coast Guard, 2020) operational arrangement includes, for example:

- The identification of the individual(s) responsible for the cyber security of the ports and port facilities. The responsible Cyber Security Officer (CySO) is responsible for ensuring the development and maintenance of the Cyber Security Plan (CSP) and implementing and exercising the CSP.

- Port Security Committee (PSC) is needed. It is one possible way to manage stakeholders who can aid in ensuring the security of port facilities. The scope of the committee should include cyber security. The development and implementation of security procedures and measures can be enhanced by forming a Port Security Committee (PSC) (IET, 2016; International Port Security Program, 2020).
- Security Operations Center (SOC)
- Arrangements for providing information to third parties (reducing risks of sensitive information).
- Arrangements for managing security incidents and breaches (handling security breaches).

The importance of SOC´s (name varies depending on the purposes of the centers) in harbors has risen as the potential for hybrid threats increases in the maritime domain (U.S Coast Guard, 20020). Cyber and physical threats as a part of overall security management must be understood so that security personnel and the cyber emergency response team maintain shared situational awareness based on joint guidance and codes. The SOC has a centralized role as a dealer of security issues, including cyber security aspects that affect a port and port facilities. It may form a part of operations, an operations center supervising the port, controlling access, and managing business continuity and disaster recovery. The main key functions may be a) Observing by maintaining situational awareness (understanding potential threats to port facilities), b) orientation to proactive measures, and c) decisions about actions that may be appropriate to deny further access to the port asset (IET, 2016).

3.2 System complexity of port community system (PCS)

Port authorities have to coordinate and implement new digital technology as Artificial Intelligence solutions by improving service across supply chains. Port Community System is a common system for digital trade logistics, as Figure 2 demonstrates.

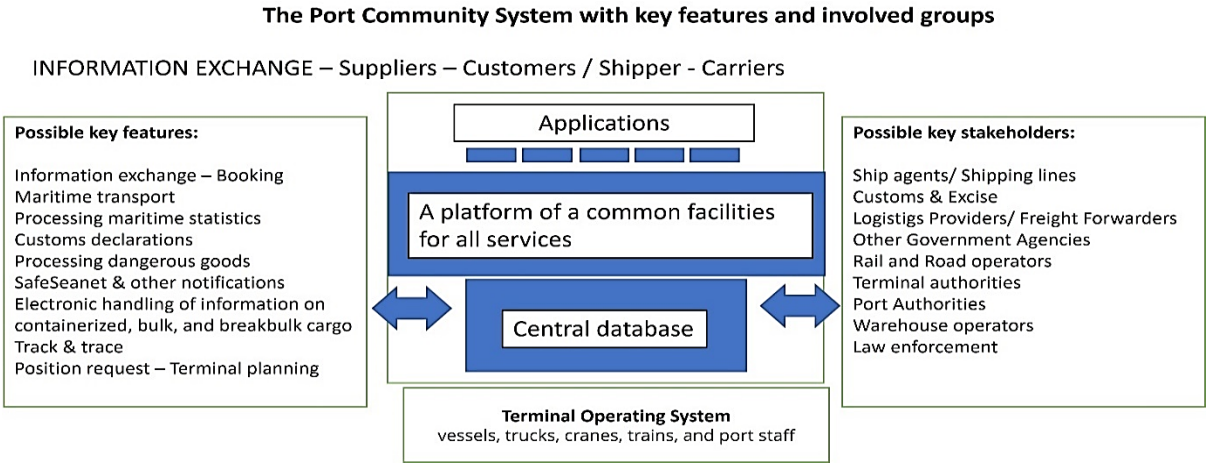

Figure 2. The Port Community System

In Finland, we do not have a long history of using PCS because our corresponding system does not have advanced digital features (IPCSA, 2022a; IPSCA2022b). We have a Portnet system by Traficom and a couple of separate systems that allow for creating situational awareness for cargo and passenger traffic in harbors. It is crucial to notice that there is globally several port -systems titled Portnet. The Port Community Systems is an open electronic platform that connects existing individual and separate systems and databases of distinct companies and organizations. The main focus of the PCS is to enable secure and intelligent operational data exchange and consolidation within the port network. Two possible seaport categories involve public and private stakeholders. a) Users who send information (e.g., shipping lines and agents, freight forwarders, and logistic actors). b) Official entities who are receiving information (port managers and operators, customs authorities, government agencies as safety authorities) (IPCSA, 2022; Sinay, 2022).

The Finnish system titled Portnet does not correspond to the requirements of international smart port system development. Finland's decentralized system governs all traffic data concerning arriving vessels, their containers, and port and terminal activities. For example, the ship reporting system Gofrep, that is developed with the neighboring county in the east, is used as a separate tool with Portnet and other operational tools that collects the vessel's information in the Gulf of Finland area (Gofrep, 2020). The Portnet has been one kind of inefficient Finnish version of the PCS. The Portnet II is under development. It should consist of more features to achieve the requirements that IMO and other international security organizations have set.

3.3 Risks, threat, and Vulnerabilities

Risk means the potential for abnormal processes or adverse circumstances of event outcomes (IAPH, 2020). Risk scenarios illustrate them. Vulnerabilities refer to the quality of state of being exposed to the possibility of being attacked or harmed, either physically meaning or emotionally meaning. **Error! Reference source not found.** above illustrates potential cyber and physical threat types in ports.

Table 1. Categorization of Emerging Threats and Vulnerabilities (George Washington University, 2021)

Threats	Vulnerabilities
Cyber	Port Infrastructure
Advanced Technologies and weapons	Automation
Violent Extremism	Port Operations
Unmanned Aerial Systems	Opportunities for Smuggling/Trafficking
	Human Factors

The threat may be an action or event that can, through the exploitation of ICT and ICS/OT, or communications infrastructure vulnerability, cause a risk to become loss or damage. Cyber-physical threats form potential risks for port infrastructure and port operations. Combined threat platforms consisting of ICT and ICS/OT and Industrial Internet of Things (IIoT)-create a potential goal for “lonely wolves” and state-level attackers.

3.4 Method of the research

This paper describes attack impacts against the Smart terminal system of systems in the cyber realm by utilizing the MITRE ATTACK framework (Mitre, 2022a; Mitre, 2022b) with official reports and other publications for analyzing the realized worldwide cyber threats and scenarios. We also used Framework for Improving Critical Infrastructure Cybersecurity, which is included in the section (analyze) in DHS's Critical Infrastructure framework. The NIST Cybersecurity Framework, and NASA's Risk-Informed Decision-Making (RIDM) framework to map and classify the objectives of threat actors and threat scenario impacts (NIST, 2018a; NASA, 2015). Concentrating on the background factors of recognized risks creates the basis for threat and risk management. The research aimed to analyze threat impacts and potential risk scenarios. The Delphi method we used is a very common cooperation model among experts and specialists. Experts use research experience in their work and assessment of the research data based on a systematic analysis of the research target.

4. Threat scenarios, consequences, and objects

Cyber-attacks set challenges not only to smart port systems but also to the whole business supply chain. For example, the scenario of Rotterdam Smart Port's intelligent features exposes it to huge vulnerabilities. Or in another scenario, APM systems which is a daughter company of maritime multi-sector operator Maersk affected by Notpetya ransomware that interrupted all terminal services in the port. The Harbor of Rotterdam has a traditional and new smart-based terminal available. The old terminal is not fully automated and can also handle containers manually. Option for another, for example, container handling method or feature (for example, manual), must be possible also in new smart ports despite the trend of digitalization. The consequences developed into a widespread chain reaction due to the form of multidisciplinary enterprise. Several ICT systems of separate business units went down, consisting of a thousand computers (George Washington University, 2021). The situation where all processes are set down causes continuity management problems and sets possibilities for added expenses and sanctions to stakeholders. For example, the customer or buyer may have the right to penalize the product sellers, transportation companies, port operators, or other stakeholders involved in the transport supply chain, especially if cyber security is mismanaged. Realized threats and their consequences often start new potential threats in new business areas. Digitalization with sensor technology requires backup & recovery systems and alternative options to use equipment in the port area.

Cyberattacks against port systems; XXX means very high supply-chain impact level, XX means high impact, and X means moderate impact, as the table illustrates. The analyzed cyber-physical risk scenarios are listed as table 3. shows. The results of the table are comparable with threat scenarios in the port and terminal system of the systems in Finland.

Table 2. Cyber-physical risk scenarios and impact rate (Mitre, 2022a).

Victim/ Place	Attacker	Type of attack	Impact/ Impact rate X-XXX	Consequences /chain-reaction	Period
Hurtigruten public transporter, Norway (Coffey H., 2020; Crew-Center,2020'; DigitalShip,2021; Naveen G.,2022; Stormshield, 2021).	Russian military hackers	Ransomware	Ransomware blocks access to files, internal email and websites. Phone lines went unavailable, and passengers' sensitive data were leaked. **Impact Rate XXX**	Loss of Business Continuity management, global I.T. infrastructure affected, major financial consequences. /Several sectors of vital functions fall under disturbances (e.g., parliament, telecommunication companies), customer cancellations, decrease in profitability, and customer relationships. Disrupted supply chain	Several months
Port of Antwerp, Belgium (Seatrade Maritime News, 2013; Stormshield, 2021).	Drug cartel group	Industrial Espionage by a keylogger.	Hijacked container management system. Allowed hackers to record the keystrokes used by the loading/unloading operators. **Impact Rate XXX**	Several containers disappeared without explanation. Hackers broke offices by deploying computers. /The supply chain and comprehensive information security were compromised.	Two years, starting from data phishing
Port of Los Angeles (BBC,2022; Greenberg, A. 2020; CBS,2017; Stormshield, 2021).	Russian military hackers - Sandworm Team/APT29	Modified (Petya) Notpetya ransomware	It affected multiple sites and selected business units. **Impact Rate XXX**	Operations of APM Terminal owned by Moller-Maersk halted. /Cargo moving operations around the docks on the landside stopped	Weeks
Rotterdam – Holland - Smart port/ APM terminal division (17 container terminals) (Dutch News, 2017; Greenberg, A. 2020; Stormshield, 2021).	Russian military hackers - Sandworm Team/APT29	Modified (Petya) NotPetya ransomware called Petrwrap	Ransomware blocks access to computer-based systems and cranes. Destroyed computer systems. **Impact Rate XXX**	The fully automated terminal went disabled. Loss of Terminal services disturbed Cargo handling and transport chain. /The operational functions of several companies were interrupted. E.g., containers and daughter companies of Maersk. Disrupted supply chain.	Several weeks, despite the backup and recovery methods.
Cosco operations in Port of Long Beach, USA. (Seatrade Maritime News, 2018; Stormshield, 2021)	Russian military hackers - Sandworm Team/APT29	Series of international NotPetya ransomware attacks	Disrupted the activities of several international ports. **Impact Rate XX**	Access was denied to the U.S. website, stoppage on the email and phone. /Email communication problems with carriers' U.S. operations and its customers. Impact on WAN and VPN gateways.	Weeks
Port operator of Barcelona, Spain. (DHS, 2019; Stormshield, 2021).	Unknown actor	Ransomware	Affected internal land operations and its systems, disrupted e.g., loading and unloading of boats. **Impact Rate XX**	Transport operations stopped.- The potential connection between case Barcelona and case San Diego cyber attack	A few Days
Port operator of San Diego, USA. (DHS, 2019; San Diego Union Tribune, 2018; Stormshield, 2021).	Iranian Cybergang	Samsam Ransomware - a highly sophisticated cyberattack	Public agency's ability to process and perform services discontinued. **Impact Rate XX**	The attack shut down port services-ability to pay traffic tickets and bills./The port has an integral role in public safety via connection to the Harbor police. The same attacker disrupted wireless communications at Atlanta airport.	Weeks
Vancouver, Canada. (Pesanti, D., 2017; Stormshield, 2021)	Unknown actor	A Distributed Denial of service attack (DDoS) - Brute force attack	Affects sending many work requests in the systems. **Impact Rate XX**	225000 user accounts were propped./Wifi-connected computers caused the spread of the virus. Networked and Connected computers were affected.	Months
Marseilles, France (CERT-FR,2020; MITRE;2022a.	Opportunistic	Ransomware Mespinoza/Pysa	PYSA ransomware is a ransomware-as-a-service (RaaS) tool that disables	Interconnected information systems with Aix-Marseille-Provence/ Organizations in	A couple

Victim/ Place	Attacker	Type of attack	Impact/ Impact rate X-XXX	Consequences /chain-reaction	Period
; Stormshield, 2021)	unknown actor		some security solutions. **Impact Rate XX**	Provence caused a chain reaction within vital functions.	of weeks
Vard of Fincantieri, Langsten, Norway. (Stormshield, 2021)	Unknown Actor	Ransomware attack	**Impact Rate unknown**	Has declined to give details.	-
Kennewick, USA. (Maritime-Executive 2020; (Stormshield, 2021;Wingrove, M.,2020).	Military hackers	Ransomware demanded $200,000 in ransom to restore access to the port's servers and files.	Criminals locked the port administration, bypassing firewalls and antivirus software. **Impact Rate XX**	Port of Kennewick was unable to use these locked servers.	A couple of Weeks
Transnet National Port Authority, South Africa. (Reuters,2021; Stormshield, 2021)	Unknown Actor	a case of cyber-force majure by ransomware	Force majeure against container terminals. **Impact Rate XXX**	Four major ports were paralyzed. /Backlogs and hamper exports from the region.	Several weeks
Port of Houston, USA. (Lyngaas, S., 2021; Donelly, J.,202); Infosecurity,2021; Stormshield,2021)	State-sponsored actor	Hackers exploit a vulnerability in password management software titled "ManageEngine ADSelfService Plus," which is used for password management and single sign-on (CVE-2021-40539).	Attackers broke into one of the port's web servers and installed malicious code to expand their access to the system. Then exfiltrated all the log-in credentials for a piece of Microsoft password management software used to control network access. **Impact Rate X**	Potential consequences if compromise had not been detected: Unrestricted remote access to the (IT.) network./Compromised supply chain operations.	Several days

Five risk scenarios achieved supply-chain impact level 3x, Table 3. Achieving this level requires widespread consequences and unexpected supply-chain impacts abroad.

Table 3. Supply-chain impacts

Norway, Case Smart Port in Hurtigruten - Ransomware	xxx
Belgium, Industrial Espionage port of Antwerpen - Supply chain attack	xxx
Holland, Rotterdam, collateral damage – NotPetya ransomware	xxx
South Africa, a case of cyber - force majeure by ransomware	xxx
USA, Port of Los Angeles – Notpetya ransomware	xxx

As research outcomes, potential threat scenarios may start from ransomware or phishing attack. Some attackers exploited weaknesses in the system, and human errors and activities have caused others. We have investigated and analyzed the most significant cyber-threat cases that are spread widely and cause major problems to the business continuity management of the enterprises. Petya-ransomware cyber-attack affected infected terminal systems so that several vessels were diverted to other terminals to ensure that customers' cargoes were not unduly delayed (MSC, 2017). Attacks against maritime supply chains have raised the most popular target by attackers. Therefore, e.g., the port of Los Angeles in the U.S. cooperates with the cyber resilience center of the FBI (BBC, 2021; Safety4sea, 2022b; Safety4sea, 2022c). Cybersecurity Supply Chain Risk Management (C-SCRM) is a usable process for managing exposure to cybersecurity risks throughout the supply chain and developing appropriate response strategies, policies, processes, and procedures. It helps the enterprise manage to cybersecurity risks throughout the supply chain (NIST, 2021). Cybersecurity supply chain risk management (C-SCRM) activities described in this publication are closely related to the Risk Management Framework described in NIST SP 800-37, Rev. 2. (NIST,2018b), SP 800-30, Revision 1, Guide for Conducting Risk Assessment (NIST, 2012). Figure 3. demonstrates how business continuity and port requirements are connected to each other. Supply chain risks are possible to tackle only by creating a common situational understanding of stakeholders operational working culture and working process/procedures.

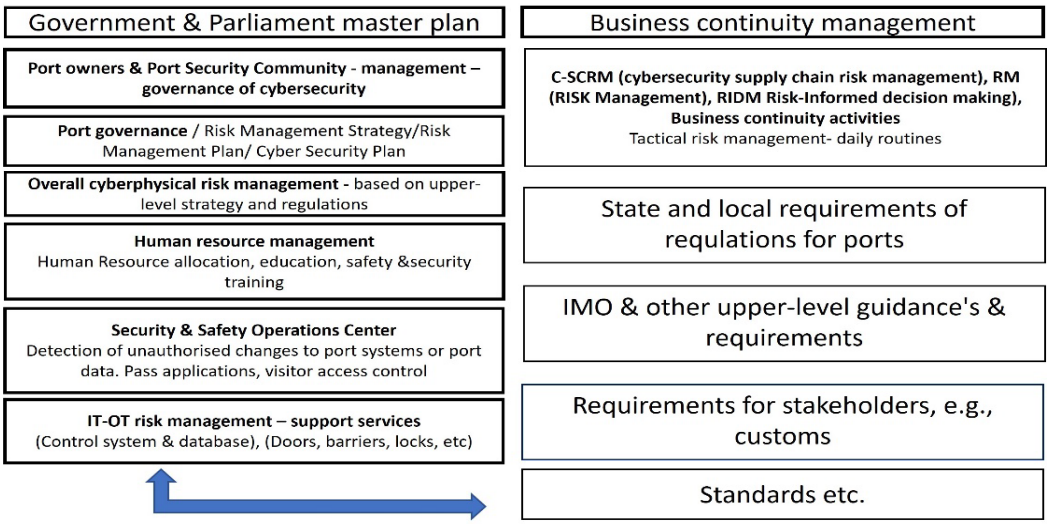

Figure 3. Supply Chain Risk Management

As research data analysis indicates, there is no cyber-threat-free or protected business sectors. Many infected companies of realized threats in terminal areas are seamlessly connected to other industries that are linked with each other through shared systems. This kind of information-sharing and communication cycle creates more possibilities for cyber attackers.

The most challenging threats to detect and potential risk scenarios in the future are related to 3rd party services NSC.gov.uk. (2019), which may cause uncontrollable supply chain attacks that evolve into the other business domain as listed above. The potential reputational harm is not limited to the company under cyber-attack; cyber-attacks against the supply chain may cause reputational damage to several business sectors as Figure 4. clarify.

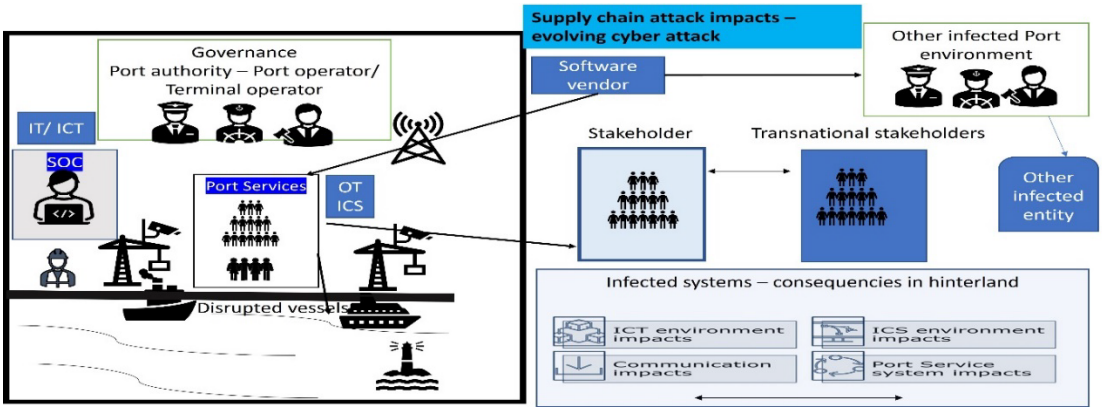

Figure 4 Supply-chain attack impacts.

The third relevant risk scenario is based on the lack of human resource management, which may be due to a lack of data protection and information security training. Lack of understanding of cyber and physical threats.

- 3d party Compromised legitimate software (hijacked ICS software)
- 3d party hardware, port equipment, cameras, drones, routers, sensors, devices, and other unknown adverse components
- Lack of human resource management - Intentional and unintentional human errors caused by lack of training, changing personnel, management of rights of access and use

5. Conclusion

As the survey indicates, it is not enough to have a Cyber Incident Response plan in port and terminal processes. To have overall protection against cyber security incidents or hybrid threats, cyber incident response plans and other security plans have to be flexible, and they have to be linked to each other and continuously updated. It means nothing to have only a plan without implementing and systematically auditing it. It seems that the same (selected) assessment tools or frameworks have to be used by all who are involved. Practical operational

fieldworkers must understand the meaning of cybersecurity and the effecting elements of it in their daily routine and working procedures. Threat information exchange via the security operation center with the nation's official cyber incident response team requires workable connection and information-sharing methods among private-public-private information sharing. Multinational and multisectoral companies have to arrange their daily operative working procedures by implementing and following guidelines for overall security management that consist of human resource & control management but also cybersecurity management of ICT/ICS/OT resources. System-level thinking requires an understanding of maritime diversity with supply chain dimensions because supply chain attacks are a crucial risk in the port ecosystem. Risk management is a crucial part of business continuity management. Aware that personnel training for maintaining cyber security is equally essential as updated software and hardware in all systems. Maintaining situational awareness in terminals and ports comprises elements that are introduced in this research. Mapping of threat scenarios aids managers and authorities in preparing against the most adverse threats. Therefore, supply chain has to see the broader framework where critical infrastructure and its vital functions are protected in a way that smart solutions such as sensor systems may support port services and facilities continuously without essential breaks in cargo transportation and passenger traffic. Port authorities, with other selected crucial actors, have to coordinate cyber security platforms in their community in a way that each level and each corporate t communicate with the same “language”. A mental model of the terms has to be at the same level. If this fundamental factor is not recognized, everything else is pointless and energy will flow to solving information-sharing problems and lack of understanding. The system of system-level thinking in the global-linked port community has to have common terms and language that form cybersecurity requirements for all stakeholders involved. Everything can be built on top of this platform, from management to responsibilities, standards, guidelines, policies, and other rules.

The paper provides a research approach to realized risks and the potential threat and risk scenarios/impacts on the port systems and facilities of those. The research approach uses the system of systems (SoS) thinking. The findings of the study propose the main cyber-physical risks and impacts of risk factors that affect business continuity management, supply chain, transport, and the whole maritime domain. The proposal indicates the issues that have to recognize in a part of the entire management system. Companies in the port area and collaborated organizations must maintain and update a risk threat scenario tool similar to Table 3. in their risk scenario and impact assessment work, which has been used to evaluate the impacts and consequences of cyber threats in the port area. It will help to focus on the potential threat impacts, threat objects, and proactive measures.

References

Atlantic Council. (2020). Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity

BBC. (2022). Cyber-attacks on the port of Los Angeles have doubled since the pandemic. Https://www.bbc.com/news/business-62260272.

CBS. (2017). L.A.Port terminal still shut down following cyber-attack. https://www.cbsnews.com/losangeles/news/la-port-terminal-still-closed/

CISA. Port Facility Cybersecurity risks https://www.cisa.gov/sites/default/files/publications/port-facility-cybersecurity-risks-infographic_508.pdf

Coffey, H. (2020). Cruise company hit by “comprehensive” cyberattack. https://www.independent.co.uk/travel/news-and-advice/hurtigruten-cruise-company-ransomware-cyber-attack-b1774890.html

Crew-center. (2020). Cyberattacks on the rise: Norwegian Cruise Company latest victim on Ransomware https://crew-center.com/cyberattacks-rise-norwegian-cruise-company-latest-victim-ransomware

Customs City. (2022). What is a port community system (PCS)?. https://customscity.com/what-is-a-port-community-system-pcs/

Cybermaretique. (2020). Le croisiériste norvégien Hurtigruten victime d’une attaque par rançongiciel https://cybermaretique.fr

DCSA. (2020). DCSA Implementation Guide for Cyber Security on Vessels v1.0. https://dcsa.org/wp-content/uploads/2020/03/DCSA-Implementation-Guideline-for-BIMCO-Compliant-Cyber-Security-on-Vessels-v1.0.pdf

DHS. (2019). Northern California area maritime security committee cyber security newsletter. DHS. https://homeport.uscg.mil/Lists/Content/Attachments/40226/1901.pdf

DHS. (2013). NIPP 2013 - Partnering for Critical Infrastructure Security and Resilience.

Digital Ship. (2021). Passenger data leaked in the Hurtigruten cyber-attack. https://thedigitalship.com/news/maritime-satellite-communications/item/7147-passenger-data-leaked-in-hurtigruten-cyber-attack

DIMECC Oy, (2020). DIMECC Sea4Value/Smart Terminals (SMARTER). Project proposal for One Sea – autonomous maritime ecosystem.

Donelly, J. (2021). Port Houston targeted by suspected nation-state actor in cyber-attack. Port Technology International. https://www.porttechnology.org/news/port-houston-targeted-by-nation-state-actor-in-cyber-attack/

Dutch News. (2017). Smart port in Rotterdam confounded by cyber attack. Http://www.dutchnews .nl/news/2017/06/smart-port-in-rotterdam-confounded-by-cyber-attack-

ENISA. (2019). Port Cybersecurity – Good practices for cybersecurity in the maritime sector.

European Parliament. Directive (E.U.) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

Fintraffic. (2020). GOFREP. https://www.fintraffic.fi/sites/default/files/2021-09/GOFREP_MG_2021_09_03.pdf

George Washington University, (2021). Emerging Risks in the Marine Transportation System (MTS), 2001-2021. NCITE

Greenberg, A. (2018). The untold story of Notpetya, the most devastating cyberattack in history. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

IAPH. (2020a). Port Community Cyber Security. https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf

IAPH. (2020b). Cybersecurity Guidelines for Ports and Port Facilities. https://sustainablewoelports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf.

IET. (2020). Institution od Engineering and Technology 2016. Cyber Security for Ports and Port Systems. Department of Transport.

IMO. International Maritime Organization. (2022). Maritime safety. https://imo.org/en/OurWork/Safety/Pages/default.aspx

Infosecurity. (2021). Port of Houston quells cyberattack. https://www.infosecurity-magazine.com/news/port-of-houston-quells-cyberattack/

IPCSA. International Port Community Systems Association. (2022a). Port Community Systems. Https://ipsca.international/pcs/pcs-general/

IPCSA. International Port Community Systems Association. (2022b). How to develop a Port Community System. https://ipcsa.international/publications/how-to-develop-a-port-community-system/

Lyngaas Sean. (2021). Hackers breached the computer network at a key U.S. port but did not disrupt operations.CNN.https://edition.cnn.com/2021/09/23/politics/suspected-foreign-hack- houston/index.html.

Maritime-Executive. (2020). Ransomware Cripples IT Systems of Inland Port in Washington State. https://www.maritime-executive.com/article/ransomware-attack-cripples-systems-of-inland-port-in-washington-state

MBLT. Maritime Bulk Liquids Transfer Cybersecurity Framework Profile

Mitre. (2022a). "ATT&CK Matrix for Enterprise", [online], https://attack.mitre.org/.

Mitre. (2022b). "Attack Navigator", [online], https://mitre-attack.github.io/attack-navigator/

Naveen Goud. (2022). Hurtigruten suffers a serious Ransomware Attack. Cyber-Security Insiders. https://www.cybersecurity-insiders.com/hurtigruten-suffers-a-serious-ransomware-attack/

NASA. (2015). Considering Risk and Resilience in Decision-Making.

NIST. (2021). NIST Special Publication NIST SP 800-161r1 Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

NIST. (2018a). Framework for Improving Critical Infrastructure Cybersecurity.

NIST. (2018b). SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy:''

NIST. (2017). Special Publication 1500-201 Framework for Cyber-Physical Systems: Volume 1, Overview. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf

NIST. (2012) Guide for Conducting Risk Assessments.

NSC.gov.uk. (2019). Third-party software providers. www.nsc.gov.uk./collection/suplly/-chain-security/third-party-software-providers

Pesanti D. (2017). Port of Vancouver meeting hindered by cyberattack. The Columbian

Reuters. (2021). South Africa's Transnet restores operations at ports after cyber attack https://www.reuters.com/article/us-transnet-cyber-idUSKBN2EZ0RQ

Safety4Sea. (2022a). USCG: Be aware of typosquatting of port facility websites. https://safety4sea.com/uscg-be-aware-of-typosquatting-of-port-facility-websites-typosquatting

Safety4Sea. (2022b). Us ports and terminals targets of increased cyber security attacks https://safety4sea.com/us-ports-and-terminals-targets-of-increased-cyber-security-attacks/

Saety4Sea. (2022c). Port of LA: Cyber-attacks have doubled since the pandemic. https://safety4sea.com/port-of-la-cyber-attacks-have-doubled-since-pamdemic/

San Diego Union Tribune. (2018). https://www.sandiegouniontribune.com/business/growth-development/sd-fi-port-cyberattack-20180926-story.html

Seatrade Maritime News. (2013). Antwerp incident highlights maritime I.T. security risk. https://www.seatrade-maritime.com/europe/antwerp-incident-highlights-maritime-it-security-risk

Seatrade Maritime News. (2018). Americas coscos us operations hit by cyber attack. https://www.seatrade-maritime.com/americas/coscos-us-operations-hit-cyber-attack

Simola, J., Lehto, M., Rajamäki, J. (2021). Emergency Response Model as a part of the Smart Society

Sinay. (2020). What is port community systems? https://sinay.ai/en/what-is-port-community-system/

MSC Mediterranean Shipping Company. (2017). Customer update: Petya Cyber-Attack. Https://www.msc.com/en/newsroom/news/2017/july/customer-update-petya-cyberattack

Stormshield. 2021. Cybermarétique: a short history of cyberattacks against ports. https://www.stormshield.com/news/cybermaretique-a-short-history-of-cyberattacks-against-ports/

U.S: Coast guard. (2020). Inter-American Committee on ports. International Port Security Program. Stakeholders management - Port security committees.

Walker, J. (2022). Ports and Terminals Cybersecurity Survey.

Wingrove, M. (2020). Riviera. Cyber attack shuts down US port servers. https://www.rivieramm.com/news-content-hub/news-content-hub/cyber-attack-shuts-down-us-port-servers-61955