Assessment of Cyber Security risks: A Smart Terminal Process

Jouni Pöyhönen[1], Jussi Simola[1], Irfan Khan[2], Martti Lehto[1] and Syed Wali[2]
[1]University of Jyväskylä, Jyväskylä, Finland
[2]Texas A&M University, Galveston, TX USA

jouni.a.poyhonen@jyu.fi
Jussi.hm.simola@jyu.fi
irfankhan@tamu.edu
martti.j.lehto@jyu.fi
syedwali@tamu.edu

Abstract: In Finland, the connections to global maritime transportation logistics systems are an essential part of the national critical infrastructure. As a part of maritime logistics systems, the port's operations are important elements for global maritime traffic and the transportation supply chain. Digitalization of seaport services makes it possible to increase the efficiency of terminal systems in the logistic processes. At the same time, port logistic processes can notably reduce its CO2 emissions by optimizing port operations. The improvement of port processes relies very much on the development of Information and Communication Technology (ICT) and Industrial Control Systems (ICS) or Operation Technologies (OT) systems. In port environment there are parts that are controlled (ICS/OT) from the cyber environment but directly interact with the physical surroundings. These are called Cyber-Physical Systems (CPS). In this environment, the cyber security aspects of the port logistic need to be addressed. In Finland, the Port SMARTER research program has been on the way since 2021. The aim of the program is to create port services within new technology solutions, and that way improve cargo and people flows while improving the experience for all stakeholders. However, this development increase also complicated system dimensions in the use of ports and makes port operations complex systems of systems environment characterized by a conglomeration of interconnected networks and dependencies. This paper describes a practical approach to risk assessment work regarding the SMARTER research case. It provides a comprehensive cyber security investigation approach to port operations at the system level. In risk assessment work, the paper emphasizes the importation of description of probabilities to defend the system element against estimated probabilities of cyber-attacks at all parts of port processes. The findings of the study are related to the comprehensive cyber security architecture of the SMARTER research goals. The following research interests are related to the issue: "How a comprehensive cyber security investigation can be conducted in smart ports operations?" This paper emphasizes cyber security risks assessment work should be covered from services for operation, information flows in and between systems, as well as electricity supplies to achieve holistic risks assessment in the smart terminal process.

Keywords: Maritime Logistic, Smart Terminal Process, Cyber Security Management, Risk Assessments

1. Introduction

ENISA port cybersecurity report (2019) emphasizes the importance of maritime transport systems for the European Union economy. It means the activity that relies on more than 1 200 seaports within the European Union. Each of them is with a different organization, interests, challenges, and activities. (ENISA, 2019)

International and national maritime transportation systems are essential parts of critical global infrastructures. Digitalization and increased levels of autonomy in logistic transport chains are expected to take leaps forward in the coming years. In Finland Smart Terminals (SMARTER) research project consists of ports digitization by the end of 2023. The mission of SMARTER is to create replicable models for digitalization, service innovation, and data usage and sharing in the harbor environment and prepare for the future by taking steps towards smart and autonomous maritime transportation. 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 structure of the project has been planned to have three use cases. The use cases are ship turnaround, truck traffic, and passenger flow. Use cases are designed to support one another, and there are linkages between the use cases. The applied research work is organized into five work packages, including cyber security research actions in Work Package 4. (DIMECC, 2020)

Modern society depends entirely on a cyber environment that provides dynamic services. The port cases digitalization means the development of Information and Communication Technology (ICT), Information Technology (IT), and Industrial Control Systems (ICS) or Operation Technologies (OT) solutions. The maritime ports are digitalized System of Systems (SoS) where system-level threats are needed to be coordinated like hybrid responses. Therefore, a system of systems-level research view is also needed. Thus, it is necessary to address the relevant cyber safety aspects of the overall maritime solutions. In any cyber environment, it is crucial that there are trustable information networks. In addition, the usability, reliability, and integrity of systems data need to be high within the operating environment, where cyber security risks are continuously being highlighted by the threatening scenarios posed by the digital world. ENISA Threat Landscape Report 2016 emphasizes all elements covered within an attack on a business process. It means that not all artifacts/components used are IT-related; there are steps/procedures used within an attack, that are performed by just having knowledge or information about the details of the business process at stake (ENISA, 2017).

In Finland, the Sea4Value research program has been established to increase digitalization for fairway and smart port (SMARTER) services. This paper follows our four previous research papers in smart port study concerning cyber risk challenges in maritime transportation, basic elements of cyber security, cyber threat analysis, and cyber threat impact evaluation. This paper counts on the importation of system of systems description of the port process and specifies the comprehensive cyber security architecture by exploiting the risks assessment process for cyber security measures for the SMARTER project. The whole Sea4Value cyber security study is a set of papers of our research team and together is also an example of soft systems research methodology used to improve cyber security management in a system of systems environment.

2. Risk assessment for Smart Terminal

The case of port in maritime transportation system includes processes to produce all needed services, like ship approached from an open sea via fairway to berthing to a pier, general port services, port logistics, and connections to land transportation. There are identified the key elements associated with processes used in the smart terminal in our previous paper, "Basic Elements of Cyber Security for a Smart Terminal Process" (2023). These are Activities, Stakeholders, Organizational relationships, Security dimensions, Security capabilities, and Criteria (Pöyhönen, Simola, Lehto, 2023). It is also evident that this entity needs communication systems within process elements and electricity systems to support the functions of processes. In all cases of port processes, the information requirements and the amount of information needed are related to the reliability of safety and security services. Cyber security awareness and information should cover all process elements. Figure 1 presents these processes (Simola & Pöyhönen, 2022).

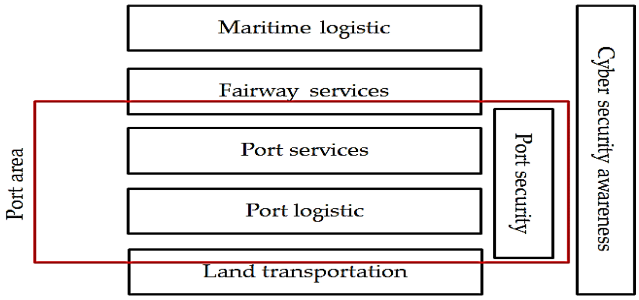

Figure 1 Port Processes

A block diagram is a useful way to describe cyber security's main dimensions for a SoS approach in terms of general smart port elements. Figure 2 illustrates the functional blocks of port operations (Simola & Pöyhönen, 2022). Communication lines between blocks are needed to identify and understand the basic architecture of its cyber security management.

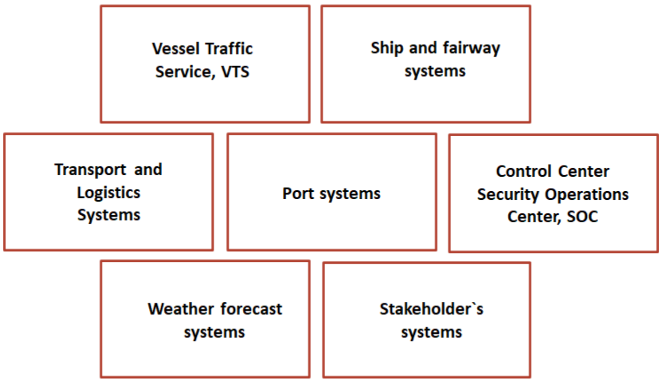
Vessel Traffic Service, VTS
Ship and fairway systems
Transport and Logistics Systems
Port systems
Control Center Security Operations Center, SOC
Weather forecast systems
Stakeholder`s systems

Figure 2. Block diagram for the Port Operations

The functional blocks of the port make it possible to produce in process context necessary services to port operations. In addition to information flows that are needed to produce services, the electricity supply for the port processes is also important to secure. According to our previous articles (Pöyhönen & Lehto, 2017; Pöyhönen, 2022), the concept of national critical infrastructure can be simplified into three essential layers. At the base layer is the electric network, above that is the data/information transmission layer and above theirs are services. In SoS thinking, all layers together is a comprehensive cyber entity. That is the case in port operations also. The function of an entity depends on the process reliability and continuity of these layers. It can be considered that port services, according to block diagram systems and communication between them, are the main systems. All structures of electric power systems are the support systems for the port services. Thus, these systems are security dimensions to be considered as part of cyber security estimation.

Cyber security estimation is very much a question of correctly implemented and appropriately functioning risk management of an organization or process. Assessment of cyber risks is the most important process behind all digital security, including data security, privacy protection, and business continuity management. Risk management is increasingly important as the need for improving the various areas of security has increased. The need for improvement has arisen from the digitalization of operations, the possibilities offered by new technologies, and the new threat and risk types that have evolved rapidly. Without an appropriately functioning risk management, the organization may not be able to recognize the significant threats that could prevent the achievement of its objectives or that are related to its daily operations and will not be able to control these threats (Ministry of Finance, 2017).

Risk management is also an excellent tool for the organization when it develops the processes, actions, and services to improve its security. Risk management helps achieve cost-efficiency, allowing development measures to be targeted at matters that have a significant impact on decreasing the probability or mitigating the impact of a recognized threat. In addition to risk management, the guideline discusses the recognition of opportunities. The failure to take advantage of opportunities could pose a threat to improving the organization's operations or achieving its targets, for example. Increased digitalization of operations is a good example of such an opportunity; it should be seen as an important player in developing operations. However, the threats related to digitalization must also be recognized.

Following figure 3 illustrates the risk assessment work as a part of the holistic cyber security architecture process.

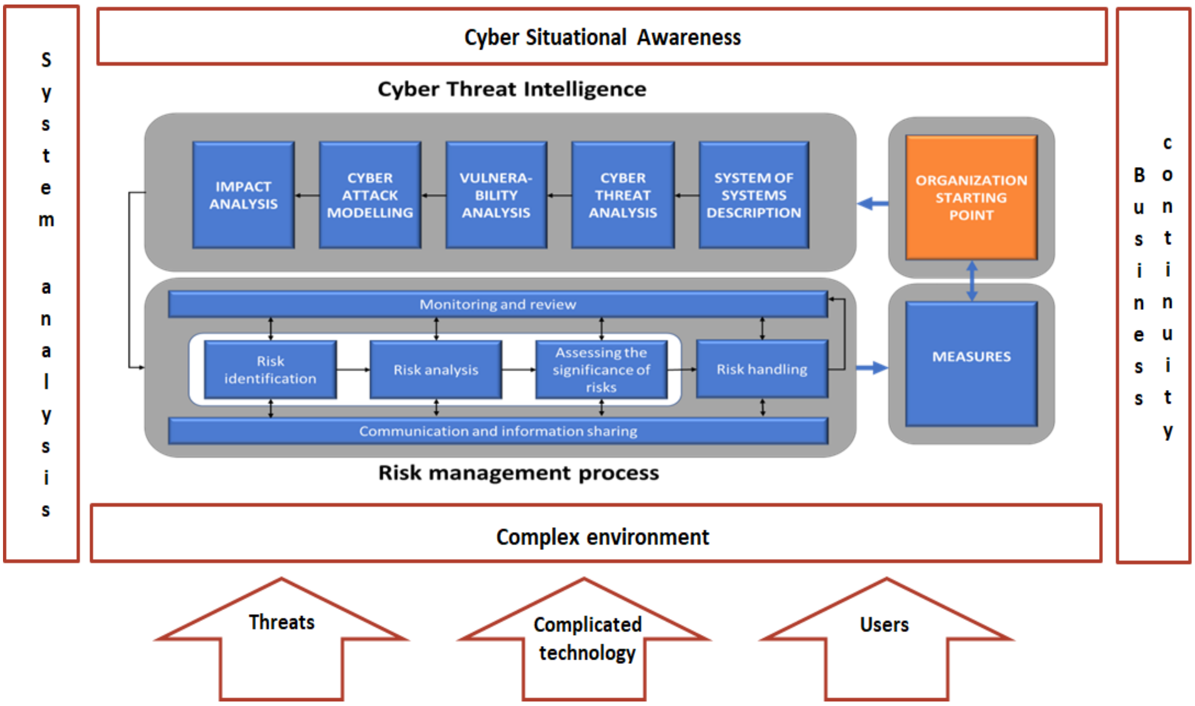

Figure 3. Risk assessment as a part of the holistic cyber security architecture process

3. Research environment for the risks assessment process

This section is based on authors work used research framework in Sea4Value research program and it also underlines our definitions of relevant smart port elements for cyber security investigation. Firstly we have a description of a research framework for cybersecurity study of the system of systems in our previous papers concerning maritime cyber security outcomes. It is a combination of a five-layer cyber structure of an organization and the maritime security management system with aspects of cybersecurity and the block diagram of a process of main maritime systems. In addition to this, an organization's cybersecurity management requires comprehensive awareness at the system level. The awareness of an organization and decision-makers can be seen as a system-level awareness arrangement. It is possible to integrate an organization's three decision-making levels into a five-layer cyber structure (Figure 4) in order to have a comprehensive system view of that organization's cybersecurity environment (Pöyhönen & Lehto, 2020).

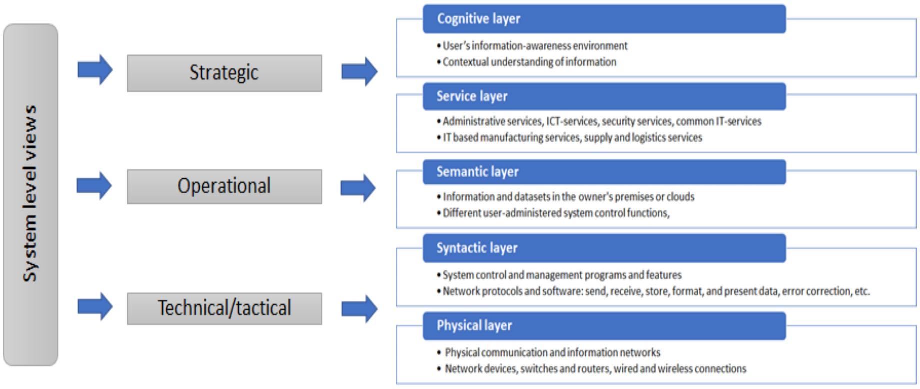
System level views
Strategic
Operational
Technical/tactical
Cognitive layer
• User's information-awareness environment
• Contextual understanding of information
Service layer
• Administrative services, ICT-services, security services, common IT-services
• IT based manufacturing services, supply and logistics services
Semantic layer
• Information and datasets in the owner's premises or clouds
• Different user-administered system control functions,
Syntactic layer
• System control and management programs and features
• Network protocols and software: send, receive, store, format, and present data, error correction, etc.
Physical layer
• Physical communication and information networks
• Network devices, switches and routers, wired and wireless connections

Figure 4. System-level view of organizational cybersecurity (Pöyhönen & Lehto, 2020)

Secoudly of our previous work, the paper "Basic Elements of Cyber Security for a Smart Terminal Process" (2023) presents the findings of cyber security research on the SMARTER project (Pöyhönen, Simola & Lehto, 2023). The key elements associated with operations and processes used in the SMARTER research areas are listed in the headlines level as follows: Activities, Stakeholders, Organizational relationships, Security dimensions, Security capabilities, and Criteria. Figure 5 (Pöyhönen, Simola & Lehto, 2023) illustrates the cyber security elements and features of this study . To cover all these, the result can be called a Smart Port, Cyber Security Management System (PortCSMS). In this case, these key elements and features can be considered root definitions of relevant systems for cyber security investigation (Checkland, 1981).

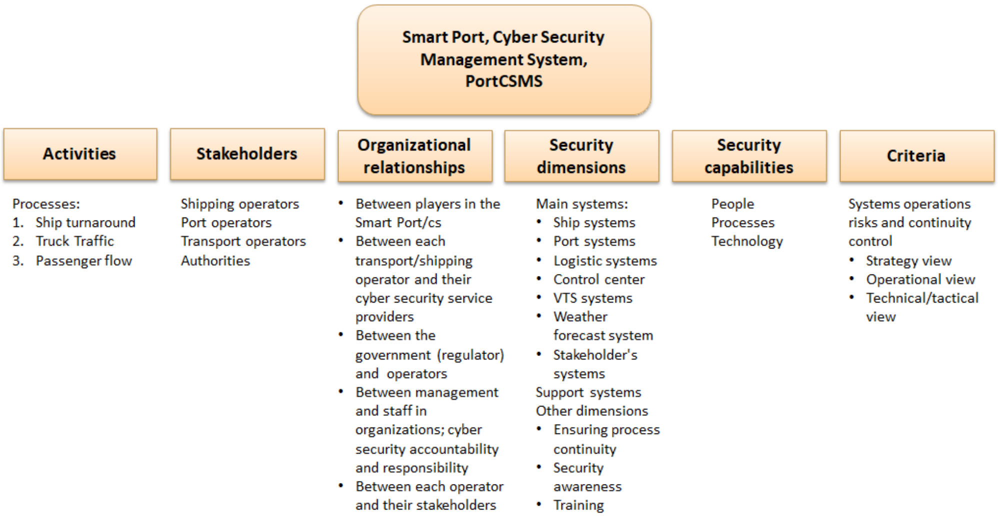
Smart Port, Cyber Security Management System, PortCSMS
Activities
Stakeholders
Organizational relationships
Security dimensions
Security capabilities
Criteria
Processes:
1. Ship turnaround
2. Truck Traffic
3. Passenger flow
Shipping operators
Port operators
Transport operators
Authorities
• Between players in the Smart Port/cs
• Between each transport/shipping operator and their cyber security service providers
• Between the government (regulator) and operators
• Between management and staff in organizations; cyber security accountability and responsibility
• Between each operator and their stakeholders
Main systems:
• Ship systems
• Port systems
• Logistic systems
• Control center
• VTS systems
• Weather forecast system
• Stakeholder's systems
Support systems
Other dimensions
• Ensuring process continuity
• Security awareness
• Training
People
Processes
Technology
Systems operations risks and continuity control
• Strategy view
• Operational view
• Technical/tactical view

Figure 5. Elements of smart port cyber security management, Port CSMS.

In the SMARTER research project is acknowledged that there is a need for new technologies and solutions that are necessary to tackle the challenges set by the use cases (DIMECC, 2020). It is identified as a set of technologies and solutions that belongs to the terminology of Industry 4.0, like big data, data lake, data analytics, information fusion, AI, 5G, IoT, edge processing etc. It is reconditioned in the article of "Cybersecurity Risks and Automated

Maritime Container Terminals in the Age of 4IR (Fourth Industrial Revolution)" by Peter Beaumont (2018) that "the risks derived from the use of technology associated with the Fourth Industrial Revolution (4IR) are both real and dangerous unless appropriate control measures are implemented" (Beaumont, 2018). It is also important to recognize and knowledge legacy systems in use with a different timeframe of technology solutions. In that sense, the SoS environment of the port process is complicated from a technological point of view. In this SMARTER cyber security research, either new and legacy technologies should be covered in bout security dimensions, main and support systems of the case.

The main systems of this study are described in a block diagram (Figure 2). It describes the cyber security main dimensions of the SoS approach in port operations (Simola & Pöyhönen, 2022). The figure shows the functional sides of the port that are needed in order to understand the basic architecture of its cyber security management. Communication and relationships between the blocks in the port systems are one of the key features of its operational processes. Next, they are emphatical to be studied in this research process (Pöyhönen, Simola & Lehto, 2023).

The support systems are related to national critical infrastructure; electric power systems, information networks and other services that are needed to support systems for the port services and thus also taken as security dimensions as a part of cyber security estimation.

The concept of national critical infrastructure can be simplified in accordance with three layers of services. At the base layer is the electric network, above that, is the data transmission layer, and above theirs are services. The base layer of smart terminals is crucial from the perspective of security and operational integrity. Major port operations can be easily disrupted by a power outage in smart ports. An adversary can easily achieve a power outage by manipulating artifacts or parameters of the control system. This outage can be regarded as a Denial of Service (DoS) attack because its primary outcome is to shut down the power of essential port services. Unavailability of power for a long period can produce serious consequences. For instance, the main concern of a port specialized in cargo will be related to cargo maintenance and storage. Forexample, refrigerated containers consume up to 40% power of a terminal for storing consumer goods (FCH, 2017; Duin, Geerlings, Tavasszy, & Bank, 2019). However, depriving them of their essential power requirement for a longer period may result in content spoilage and monetary loss to stakeholders.

The second critical layer of smart ports is the data transmission layer that allows human-to-machine, machine-to-machine, and human-to-machine connections. It transfers data between different components of a port and is extremely critical for a series of services. Port ICT system usually hosts databases, storing vessel and port information, and Terminal Operating System (TOS), performing critical stowage planning operations. All port ICT systems having network interfaces for external connections must be thoroughly assessed for potential vulnerabilities and their impact. Since an adversary can easily disrupt port operations and availability of TOS by exploiting vulnerabilities of the data transmission layer, rigorous risk assessment and risk management must be performed to protect the ports' operational integrity.

On top of the port infrastructure, there is a service layer that utilizes physical assets and communication channels for performing essential maritime operations (DNV GL, 2015). Smart ports are enormous implementations of software, hardware, and communications channels (Gary C. Kessler & Steven D. Shepard, 2020). The potential for attacks on port hardware or software is always present and evolving with respect to time. Emerging cyber threats with an increased dependency on vulnerable communication channels have jeopardized all stakeholders, making as like Intrusion Detection Systems (IDS) the essential network security requirement. However, the introduction of adversarial attacks in the cyber domain highlights the need to upgrade these existing systems because they can be exploited by modern attack vectors (Wali & Khan, 2021). Now an adversary can hack or manipulate sensor data to disguise a cyberattack as legitimate network traffic. In addition, they could sorely disrupt vessel traffic by sending false tidal window messages, berthing data, or clearance time to enter the port. Any of these scenarios could disrupt port operations, potentially for days at a time (Kessler & Shepard, 2020).

4. Risks assessment principles and estimation process

The information flows use legacy as well as new technologies, and electric supply chains are very important parts of cybersecurity risk analysis work from the port service point of view. The recognition of these technologies enables us to identify different functions at the system level, carry out risk assessments and identify their residual risks with sufficient accuracy. In the same way, the dependencies of different systems need to be considered, and based on these dependencies, security and cybersecurity risks need to be identified. In our previous papers, we have presented a probability approach to cyberattacks versus a probability to defend attacks and, in the end, to evaluate cybersecurity risks related to the relevant service operations.

A cyber-threat model captures information about potential cyber threats against a system, an enterprise, an SoS, a region, or a critical infrastructure sector. A cyber-threat model can serve as a basis for a variety of tasks in different scopes. Comprehensive cybersecurity needs a wide scale of analysis of a system of systems (or subsystem) against a set of threat events. It can often be impractical, and, in that sense, analysis of SoS could rely on the development and use of threat scenarios. A threat scenario could include the picture of a potential threat and the result of harmful consequences (Bodeu & McCollum, 2018). This has been part of our work in previous papers in this study.

The Bayesian attack graph model has been studied in several areas of security risk management. The paper "Dynamic Security Risk Management Using Bayesian Attack Graphs" (Poolsappasit, Dewri & Ray, 2012) proposes a risk management framework using Bayesian networks in order to quantify the chances of network compromise at various levels of system constructions. In the same sense, various threat risk analysis schemes have been developed to recognize the attack and implement the security safeguards to protect the system asset from cyber-attacks (Wang & Liu, 2014). Attack trees (AT) technique plays an important role to investigate the threat analysis problem to known cyber-attacks for risk assessment. An attack graph is based on a probabilistic metric model and can be used to quantify the cybersecurity issues of an SoS environment.

In our paper "Assessment of cybersecurity risks - Maritime automated piloting process" (2022), an attack tree graph is used to represent the relationship between threat and defense actions in the relevant case process. At the SoS level, it is more than a metric model, a way of thinking, because there are many layers in the system configuration. Exact quantitative probability calculation is therefore complicated, and results can be inaccurate. According to our experiences, we are familiar with the attack tree graph as a tool for risk assessment. The result of this represents the likelihood of an attack against the likelihood of defense against attacks. The final probability of success of defense measures versus attacks will be estimated, and the most serious attacks will be recognized and prioritized. This probability evaluation (not exact calculation) work is proposed to be done by cybersecurity experts by utilizing all relevant information available from the cybersecurity features of the used technology in the current case and information from stakeholders' capabilities to have defense measures. In this sense, we have been to propose the use of the Delphi method principle to make relevant threat analysis and risk level estimations from the systems. In the Delphi methode we need to use several estimation cycles in order to have sufficient results. The recommendation is three or more. It is a useful way of thinking about likelihood and probabilities at the system level of a process or an organization. (Pöyhönen & Lehto, 2022)

The risks probability estimation can be extended to the system level as described below. The National Institute of Standards and Technology (NIST) released recommendations as "Framework for Improving Critical Infrastructure Cybersecurity" (2018) for owners and operators of critical infrastructure to help them identify, assess, and manage cyber-risks. The Framework Core part of the guidance has a set of cybersecurity activities, outcomes, and informative references that are common across sectors and critical infrastructure. Elements of the Framework Core provide detailed guidance to help an organization align and prioritize its cybersecurity activities with its business/mission requirements, risk tolerances, and resources. The Framework Core consists of five concurrent and continuous Functions: Identify, Protect, Detect, Respond, Recover. There is mentioned that "The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure" (NIST, 2018).

The probabilistic success of attacks, P(t), against the defense of system x can be evaluated and calculated as follows, adapting the principle in "Threat Analysis of Cyber-Attacks with Attack Tree+" (Wang & Liu, 2014, mod.)

$$P_{Ax}(t) = P_A P_{D`} = (P_{SOT})(1 - p_P(t))(1 - p_D(t))(1 - p_M(t))(1 - p_R(t)) \qquad (1)$$

where, as a function of time t, a successful attack against a system x, P_{Ax} has attack identify for success probabilities P_A (P_{SOT}: Strategy level S; Operational level, O; Technical/tactical level, T) reduced by a defending mechanism, $P_{D`}$: Protection P, Detection D, Countermeasure M and Recovery R having the respective success probabilities p_P, p_D, p_M and p_R. (Pöyhönen & Lehto, 2022)

5. SMARTER cyber security risks assessment

Conclusively, all layers of smart terminals in the system of systems thinking can position their own strategic role and identify their operation as part of an entity whose other parts depend on reliably functioning of the three layers of national critical infrasrtucture. This also facilitates the identification of cyber dependencies within the layers so that they can be secured with the most efficient and practical measures. For that reason, risk assessment work should be covered all those levels and related elements whit in a five-layer cyber structure as well as all organizations decisions levels. (Pöyhönen & Lehto, 2017; Pöyhönen, 2022). However, maritime cyber risk assessment is relatively new (IMO, 2017), and it has been highlighted as an emerging need of the maritime sector by several nations over the last few years (Wilshusen, 2015). Since all layers of smart terminals are interconnected and function together to achieve a specific task, conventional risk assessment models are inaccurate in mirroring the actual dynamics of port operations (Polemi, Ntouskas, Theoharidou, & Gritzalis, 2013; Tam & Jones, 2019). The static nature of conventional approaches cannot examine the cyber-physical aspect of port operations, as unique, physical accidents can take place due to cyber intrusions or vice versa. Risk assessment of each layer separately cannot address emerging threats associated with the interconnection of layers. Therefore, the risk assessment process of smart terminals must consider a multi-dimensional model of port operations, such that all layers and cyber-physical elements of port operations must be included. This multi-dimensional risk assessment process, shown in Figure 3, consists of the following four steps:

a. **Risk Identification:** All possible sources of cyberattacks, vulnerabilities, their causes, and potential impact are identified at this stage of risk assessment. Therefore, in the case of smart terminals, Grid vulnerabilities and possible cyber-physical attack vectors in the communication and port services layer must be identified at this phase. Moreover, existing safeguards (intrusion detection system, prevention, or cyber-defensive strategies) capable of reducing or mitigating the consequences of any hazardous event must be identified.
b. **Risk Analysis:** The frequency and consequences of any identified risk is determined at this phase. A hazardous event may have multiple consequences, including unavailability of port services, downtime of the power utility, and failure of the communication system. Consequences should not be limited to any individual layer because problems can traverse from one layer to another. For instance, intrusion in the communication layer may hijack port operations. Therefore, risk analysis should consider all potential consequences.
c. **Risk Evaluation.** Evaluation of identified risks and their potential consequences is performed at this phase. Depending on the severity and impact, a quantitative value is assigned to every possible risk. In the case of smart terminals, every risk ranging from the base layer (electrical system) to the port services will be assigned a value. This value depicts the severity of all possible risk factors.
d. **Risk Handling.** Risk handling utilizes the quantitative data produced from the risk evaluation phase. This data helps the stakeholders to develop and implement an appropriate mitigation plan and invest in cybersecurity. A wide range of risk handling strategies can be selected at this phase, including physical system upgradation, implementation of the automated intrusion detection system, and integration of AI-driven cyber defensive strategies.

The proposed risk handling plan is then evaluated against financial feasibility, and only those plans are selected by stakeholders that balance costs and efforts of implementation against obtained benefits. Moreover, periodic monitoring and review of the risk assessment process must be carried out to incorporate defensive measures against emerging cyber threats and vulnerabilities within the cyber-physical layers of smart terminals.

6. Conclusion

The Finnish smart port research program concerns port services for ship turnaround, truck traffic, and passenger processes. It is called SMARTER, and the research activities are related to the digitalization survey with the use of new technologies in order to achieve the main objectives, the reduction of emissions by optimizing port logistics, and is to enable exceptional flow and experience for the passengers and cargo.

Smart ports are enormous implementations of hardware, software, and communications, including the development of new apps. The potential for attacks directly on physical surroundings, CPS, via hardware or software is always present and evolving. All emerging vulnerabilities associated with the interconnection of ICT and ICS/OT layers in smart terminals must be thoroughly assessed. The vulnerable cyberspace and systems of future ports pose a serious threat to both the economy and security as cyberattacks continue to become more sophisticated and more difficult to detect in real-time. Therefore, dynamic risk assessments of port infrastructure, encompassing all layers and components of the port, must be carried out to improve cyber resiliency and operational integrity in the smart terminals.

This paper provides a research approach for needs of cyber security risks assessment work of the system element of the smart terminal process. The research approach includes the system of systems thinking. The risk findings of the study are related to the coverage of port services, information flows in and between systems as well as electricity supplies in the port process.

References

Beaumont, P., 2018. Cybersecurity Risks and Automated Maritime Container Terminals in the Age of 4IR [Fourth Industrial Revolution], Chapter in 'Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution', pp. 497–516, https://doi.org/10.4018/978-1-5225-4763-1.ch017

Bodeu, D. J. & McCollum, C. D., 2018. System-of-systems threat model. The Homeland Security Systems Engineering and Development Institute (HSSEDI) MITRE: Bedford, MA, USA

Checkland, P., 1981. Systems Thinking, Systems Practice, John Wiley & Sons, Ltd., 330 s.

de la Peña Zarzueloa, I., Soeanea M. J. F. & Bermúdez, B. L., 2020. Industry 4.0 in the port and maritime industry: A literature review. Journal of Industrial Information Integration 20 (2020) 100173.

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

DNV GL., 2015. Ship connectivity . Strategic Research & Innovation Position Paper

Duin, J., Geerlings, H., Tavasszy, L. & Bank, D., 2019. Factors causing peak energy consumption of reefers at container terminals. Journal of Shipping and Trade.

ENISA, 2017. Threat Landscape Report 2016, 15 Top Cyber-Threats and Trends.

ENISA, 2019. PORT CYBERSECURITY. Good practices for cybersecurity in the maritime sector. NOVEMBER 2019. https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector

FCH, 2017. Development of Business Cases for Fuel Cells and Hydrogen Applications for Regions and Cities. Brussels.

International Maritime Organization, IMO, 2017. Guidelines on Maritime Cyber Risk Management. MSC-FAL.1/Circ.3 5 July 2017

Kessler, G. C. & Shepard, S. D., 2020. *Maritime Cybersecurity: A Guide for Leaders and Managers* .

Ministry of Finance, 2017. Risk management guideline. Kimmo Rousku (editor). Ministry of Finance publications 22/2017. Finland.

National Institute of Standards and Technology, NIST, 2018. Framework for Improving Critical Infrastructure Cybersecurity, April 16, 2018

Polemi, D., Ntouskas, T., Theoharidou, M. & Gritzalis, D., 2013. S-Port: Collaborative Security Management of Port Information Systems. Conference: Information, Intelligence, Systems and Applications (IISA).

Poolsappasit, N., Dewri, R. & Ray, I., 2012. Dynamic Security Risk Management Using Bayesian Attack Graphs. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 1, JANUARY/FEBRUARY 2012

Pöyhönen, J. & Lehto, M., 2017. Cyber security creation as part of the management of an energy company. ECCWS 2017: Proceedings of the 16th European Conference on Cyber Warfare and Security (pp. 332-340). Published by Academic Conferences and Publishing International Limited. Reading. UK.

Pöyhönen, J. & Lehto, M., 2020. Cyber security: Trust based architecture in the management of an organization security. The proceedings of the 18th European Conference on Cyber Warfare and Security ECCWS2020, 25-26 June 2020, University of Chester, UK, pages 304-313

Pöyhönen, J. & Lehto, M., 2022. Assessment of cybersecurity risks - Maritime automated piloting process. The proceedings of the 17th International Conference on Cyber Warfare and Security. State University of New York at Albany Albany, New York USA 17-18 March 2022. pp 262-271.

Pöyhönen, J., 2022. Cyber Security of an Electric Power System in Critical Infrastructure. Cyber Security, Critical Infrastructure Protection. Martti Lehto Pekka Neittaanmäki Editors. Springer. Computational Methods in Applied Sciences. Volume 56. Chapter 9. (pp. 217-254). ISSN 1871-3033. ISBN 978-3-030-91292-5 ISBN 978-3-030-91293-2 (eBook) https://doi.org/10.1007/978-3-030-91293-2

Pöyhönen, J., Simola, J. & Lehto, M., 2023. Assessment of cyber security risks – Smart terminal process. The proceedings of the 22nd European Conference on Cyber Warfare and Security. ECCWS-2023

Simola, J. & Pöyhönen, J., 2022. Emerging cyber risk challenges in maritime transportation. Proceedings of the 17th International Conference on Information Warfare and Security, 2022. pp 306-314

Tam, K. & Jones, K., 2019. Situational Awareness: Examining Factors that Affect Cyber-Risks in the Maritime Sector. International Journal on Cyber Situational Awareness

Wali S. & Khan I., 2021. Explainable AI and random forest based reliable intrusion detection system.

Wang, P. & Liu, J. C., 2014. Threat analysis of cyber-attacks with attack tree+. Journal of Information Hiding and Multimedia Signal Processing, 5(4).

Wilshusen, G., 2015. Maritime critical infrastructure protection: DHS needs to enhance efforts to address port cybersecurity. GAO-16-116T.