Basic Elements of Cyber Security for a Smart Terminal Process

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

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

Abstract: Global maritime transportation and logistics systems are essential parts of critical infrastructures in every society, and a crucial part of maritime logistics processes are seaports. Digitalization helps improve the efficiency of terminal systems in the processes of these ports. In Finland this development is going on and it is called SMARTER research program. In the best cases, digitalization can also promote the reduction of emissions by optimizing port operations and enhancing cargo and people flows while improving the experience for all stakeholders. The improvement of port processes relies on the development of Information and Communication Technology (ICT) and as well as on Industrial Control Systems (ICS) or Operation Technologies (OT). At the same time, the cyber security aspects of maritime logistics also need to be addressed. In Finland, the SMARTER research program has been established to create port services by using, among other tools, Industry 4.0 solutions. As critical systems become more complicated in terms of users, processes and technology, the entire port infrastructure becomes a complex system of systems environment characterized by a conglomeration of interconnected networks and dependencies. ICT systems are significant parts of the operations and core processes, and are related to the administration and management of information in the network. The components of process levels include ICS/OT systems as well. This paper presents findings related to the SMARTER research goal on cyber security, which is a comprehensive cyber security architecture for port services at the system level. The paper emphasizes the importance of system description and recognizing basic system elements and their description in the first phase of the research process. The descriptions of these elements are needed to answer the following question at the beginning of the research: "What are the basic elements of cyber security for a smart terminal process?" The main elements identified in this paper are activities, the recognition of every stakeholder and the relationships between them, security dimensions, security capabilities, and system views of organizational criteria for cyber security in the SMARTER system. The solution can be called the Smart Port Cyber Security Management System (PortCSMS).

Key words: Maritime Logistics, Smart Port, Cyber Security Management, SMARTER

1. Introduction

The ENISA port cybersecurity report (2019) emphasizes the importance of maritime transport systems for the economy of the European Union. The report refers to activity that encompasses more than 1,200 seaports within the European Union, each of them with different organization, interests, challenges, and activities. On future development, the report states the following: "The global digitalization trend and recent policies and regulations require ports to face new challenges with regards to Information and Communication Technology (ICT). Ports tend to rely more on technologies to be more competitive, comply with some standards and policies and optimize operations" (ENISA, 2019).

International and national maritime transportation systems are essential parts of critical global infrastructures. Digitalization and increased levels of autonomy in logistics transport chains are expected to take leaps forward in the coming years. This development can help create safer, more efficient, sustainable, and reliable port services and operations that will have a central role in future transport logistics and supply chains. At the same time, as stated in the ENISA report: "This brings new stakes and challenges in the area of cybersecurity, both in the Information Technologies (IT) and Operation Technologies (OT) worlds" (ENISA, 2019). Digitalization makes it possible to create smart ports and terminals by utilizing the latest Industry 4.0 technology. A well-built digital port infrastructure is essential for optimizing operations and planning for future investment and maintenance needs.

In Finland, the Smart Terminals (SMARTER) research project, which runs to the end of February 2023, addresses the digitalization development of ports. The research work for port solutions benefits maritime transportation in many ways. For example, it will enable ports to reduce emissions by optimizing operations and improving cargo and people flows while improving the expertise for all stakeholders. 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 (DIMECC, 2020b).

The digitalization of ports means the development of solutions for Information and Communication Technology (ICT), Information Technology (IT) and Industrial Control System (ICS) or Operation Technologies (OT). The maritime ports consist of digitalized system of systems where responses to system-level threats need to be coordinated as hybrid responses, hence the need for a system-of-systems–level research view. Such a view is necessary to address the relevant cyber safety aspects of the overall maritime solutions. In any cyber environment, trustable information networks are crucial. In addition, within operating environments where cyber security risks are continuously being highlighted by the threatening scenarios posed by the digital world, the usability, reliability, and integrity of systems data needs to be high. A modern society depends entirely on a cyber environment that provides dynamic services.

This paper follows our first SMARTER paper – "Emerging cyber risk challenges in maritime transportation" (Simola & Pöyhönen, 2022) – and leverages the research approach for the investigation of cyber security aspects at the system level in the study case. This is the next step in our research process and provides a description of a port environment and its basic elements. The paper highlights the importance of system description of the port process and its elements at the beginning of the research program. It also addresses our initial research question: "What are the basic elements of cyber security for a smart terminal process?" Once this question is addressed, the research will be able to specify the comprehensive cyber security aspects of architecture, such as threat analysis, risks assessment and cyber security measures, for the SMARTER project. This paper is one of the outcomes of the project's final report.

2. Smart Terminals (SMARTER) research project in Finland

In Finland, the Sea4Value / Fairway (S4VF) research program (DIMECC, 2020a) has moved on to its second phase. The SMARTER project enlarges the scope of DIMECC Sea4Value program to harbors and ports by developing digitalization and solutions that benefit RoPax and RoRo harbors. The project goals are the reduction of emissions by optimizing harbor operations and improving cargo and people flows while improving the experience for all stakeholders (DIMECC, 2020b). The first stage of the program concerns automated remote pilotage fairway navigation. The SMARTER project can be enlarged and complemented to develop harbors and ports so that they meet the forthcoming needs of autonomous traffic and business. SMARTER has two main objectives (DIMECC, 2020b):

- Reduce emissions by optimizing port logistics.
- Enable exceptional flow and experience for passengers and cargo.

The structure of the project is built around three use cases (Figure 1): ship turnaround, truck traffic, and passenger flow. These use cases are designed to support one another and there is linkage between them. The applied research work is organized into five work packages, each led by a responsible team of researchers. Cyber security research actions are included in Work Package 4 (WP4). (DIMECC, 2020b)

The research items in Work Package 3 (WP3) on data collection and management are related to sensors, data processing, and connectivity to support data collection from diverse use cases. WP4 also provides cyber security research for comprehensive security management in the port environment. Cyber security will be integrated into the solution because information connections have high-level risks for attack vectors of adversarial actors. (DIMECC, 2020b)

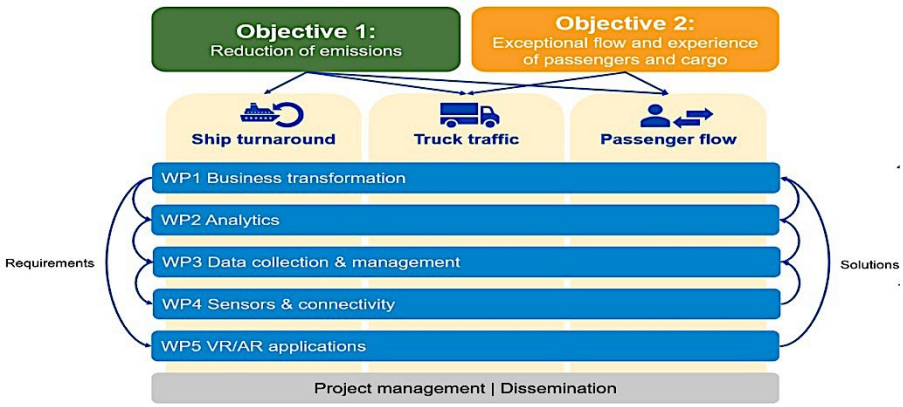

Figure 1: Project structure

The case of a port in a maritime transportation system includes processes such as ship approach from the open sea via a fairway to berthing at a pier, as well as port services, port logistics, and connections to land transportation. It is also obvious that the entity requires cooperation and communication with different stakeholders of the process elements. 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 2 presents these processes. (Simola & Pöyhönen, 2022)

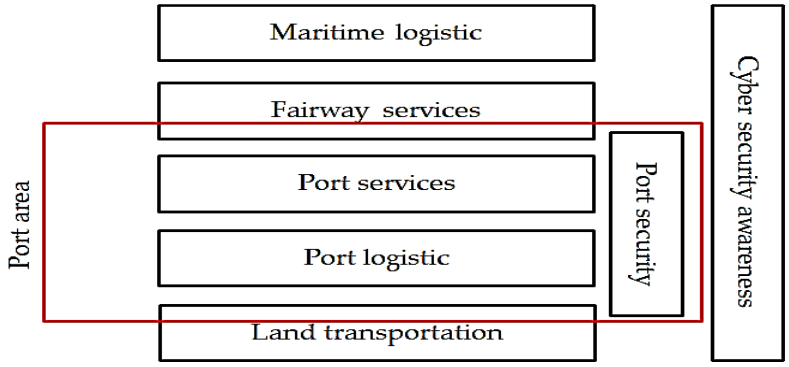

Figure 2: Port Processes

3. Industry 4.0 in the port processes

PwC's 2016 Global Industry 4.0 Survey mentions that the move to Industry 4.0 "is being driven by digitization and integration of vertical and horizontal value chains, digitization of product and service offerings and the development of new digital business models and customer access platforms" (PricewaterhouseCoopers, 2016). Since that time, an increasing number of papers have addressed, for instance, Industry 4.0 ontology, related technologies and manufacturing solutions. Moreover, ports and terminals in the 2010s have been seen to evolve to a new stage of industrial evolution, one characterized by their digital transformation and alignment with Industry 4.0 practices (de la Peña Zarzueloa, Soeanea & Bermúdez, 2020).

SMARTER acknowledges the need for new technologies and solutions that are necessary to tackle the challenges set by the use cases (DIMECC, 2020b). This set of technologies and solutions can be identified by the terminology of Industry 4.0. The development of smart port processes in the work packages, from control management and data collection to sensors and connectivity, needs to include definitions from big data, data lake, data analytics, information fusion, AI, 5G, IoT, edge processing and so on. From the Industry 4.0 point of view, this terminology is quite the same, so it is logical to speak about Industry 4.0 technology development as a general term related to smart terminal research goals. The future of smart ports will lead to increasing digital entry points to networks and thus connections between ICT systems and ICS or OT systems. The article "Cybersecurity Risks and Automated Maritime Container Terminals in the Age of 4IR (Fourth Industrial Revolution)" (Beaumont, 2018) presents a case study of automated maritime Container Terminals (CT) and demonstrates that the risks derived from the use of technology associated with the Fourth Industrial Revolution (4IR, referred to here as Industry 4.0) are both real and dangerous. He argues "that many CT operations are likely to be exposed to significant cyber-based risks and that this exposure will increase with the roll-out of further 4IR technologies unless appropriate control measures are implemented" (Beaumont, 2018).

Digital transformation also changes our thinking about separated systems. According to Accenture (2022), one example of digital transformation and converging IT/OT systems has been introduced in the mining industry. A copper mining company combined separated IT and OT systems under a joint governance structure where the management of IT and OT together were unified into one centralized technology organization.

4. Smart Port Cyber Security Management System

In their paper, "The Maritime Security Management System: Perceptions of the International Shipping Community" Thai and Grewal (2007) emphasize the importance of identifying key shore-based and near-shore activities associated with maritime security management. In their paper "Basic Elements of Cyber Security for an Automated Remote Piloting Fairway System" Pöyhönen, Kovanen and Lehto (2021) presents the findings of

cyber security research on the Sea4Value / Fairway (S4VF) project in the same way as in the fairway remote pilotage environment. Based on these papers there are similar needs to identify key elements associated with operations and processes used in the SMARTER research areas. These are listed on the heading level as follows: activities, stakeholders, organizational relationships, security dimensions, security capabilities, and criteria. Figure 3 illustrates the cyber security elements of this study. To cover all these, the result can be called Smart Port, Cyber Security Management System (PortCSMS). The cyber security elements are explained after the figure.

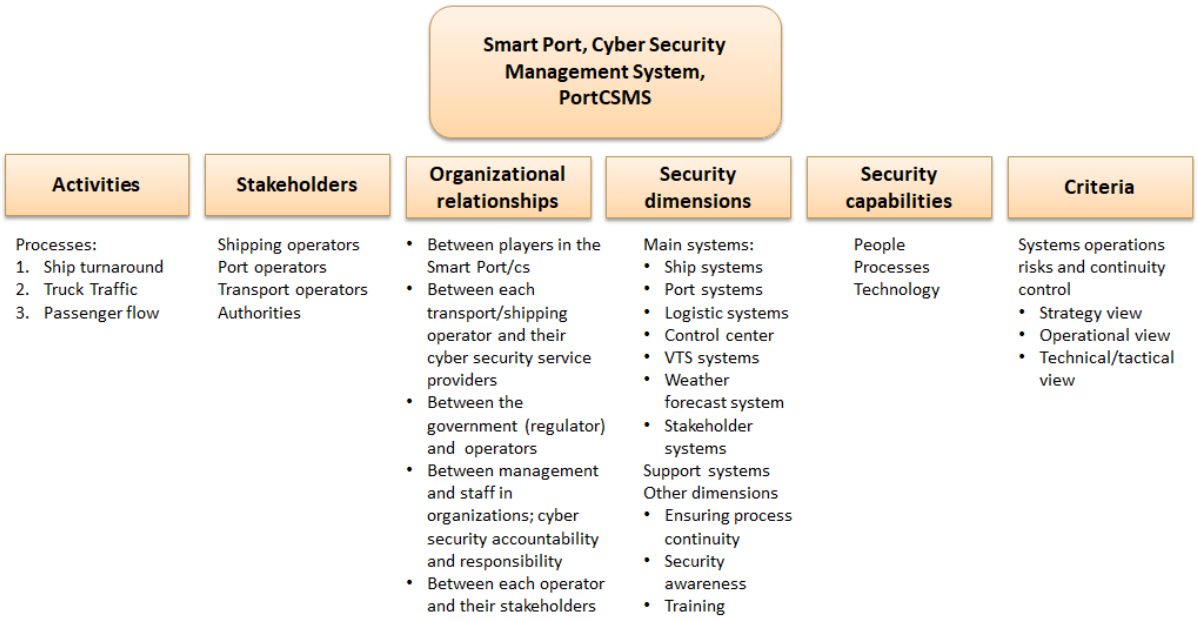

Figure 3: Elements of smart port cyber security management, PortCSMS.

4.1 Activities

The activities in this port research are ship turnaround, truck traffic, and passenger processes. They also comprise the use cases of the research. "The ship turnaround use case focuses on optimizing the various processes associated with ship visits in harbor. The truck traffic use case focuses on developing a predictive real-time traffic situational awareness model to optimize the cargo logistics to and from the port. The passenger flow use case improves the passenger flow on RoPax ports by developing models and solutions to support collective transportation, ride sharing and other mechanisms to relieve the congestion at ports." (DIMECC, 2020b)

All ports play an important role in maritime business processes and, by extension, in global logistics. Ports are the place where maritime logistics connect to land logistics, making them one of the main gateways in the international trade system. The strategic positioning of ports has significantly changed in the last two decades. The standards of their operations and service management have increased because of the global competitive landscape. In addition, the ongoing digitalization of ports is going to be a major driver in their development in the near future. Smart solutions for ports enable identifying new growth areas as well as changing the revenue mix, logistics operations, and port services. In this environment the largest challenge can be tackled by using the latest solutions for digitalization. (DIMECC, 2020b)

The ENISA Threat Landscape Report 2016 emphasizes all elements covered within an attack on a business process. It means that not all of the artefacts/components used are IT related. There are steps and procedures used within an attack that are performed by just having knowledge or information about the details of the business process at stake. Business-related issues are key areas, both in the planning of an attack by an adversary and in analyzing an incident by a defender of activities: "Asset exposure can be grouped based on a business process or an asset owner" (ENISA, 2017).

4.2 Stakeholders

A modern seaport can include dozens of stakeholders interacting to run the port processes. In a stakeholder organization, the cyber security capabilities are based on the expertise of people, trustable processes and security technology in products and services. At the strategy level this means that company management includes organization leaders who consider cyber security issues as a strategic goal, a published cyber security policy, and risk-based management as part of overall cyber security and business activity (Pöyhönen & Lehto, 2017).

At the operational level, the strength of the stakeholder cyber security approach may be based on the use of the best partners in outsourcing, clustering, public–private partnerships (PPP) and international cooperation. A good reputation among stakeholders is needed in this approach. Of course, stakeholders should work without conflict between a company's business activity and the national supply security requirements (resourcing) for critical infrastructure. (Pöyhönen & Lehto, 2017)

The technological-tactical level implementation focus should be on staff competence, cyber and information security products and services. In the best cases, the strength of companies is based on ensuring the continuity of operations through training, planning exercises, and preparedness plans. Real-time situation awareness of ICT assets and ICS/OT systems is mandatory to have at least in technological-tactical level. (Pöyhönen & Lehto, 2017)

4.3 Organizational relationships

Port processes and services include the relationships among organizations within the harbor as well as those outside of it. It is possible to have companies' common situation awareness and to have the opportunity to learn about threats often directly from the operating network or partners and the use of announcements of the National Cyber Security Centre Finland. On the other hand, overall situation awareness is often based on scattered data, and obtaining situation awareness of the entire operating network is useful but could be at the same time challenging. (Pöyhönen & Lehto, 2017)

A common port facility cyber security plan (CSP) is needed to manage the risks of a security incident. It is intended that wherever appropriate, the CSP will build upon the existing port security plan (PSP). (IET, 2020)

In general, a CSP covers the strategy, policy, procedures, and technologies of an organization. The port facility security plan is intended to ensure port processes, stakeholders, and relationships between them and as well as the port systems. Port stakeholders can leverage expert services as a strength in different audits and in solving problem situations also by utilizing best practices and national research programs (Pöyhönen & Lehto, 2017).

4.4 Security dimensions

A. Main systems

A block diagram makes a description of the cyber security main dimensions for a system-of-systems approach in port operations. Figure 4 illustrates these blocks (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 functional relationships between the blocks in the port systems are one of the key features of its operational processes. They are essential elements to be studied in this research process.

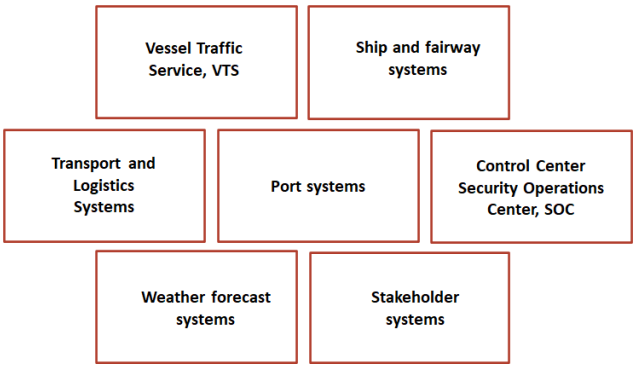

Figure 4: Block diagram for Port Operations

Figure 4 specifies the key cyber security subsystems in a block diagram created as part of the SMARTER project. Its foundation is the main port process, including transport and logistics systems, port systems and control center systems. The port operations also need support processes such as vessel traffic service (VTS) and weather forecast services. Ship and fairway systems and stakeholder operations are also essential information sources and support processes. The main process elements of the port are outlined in the middle row and the support processes are in the top and bottom rows in the figure. The complete system configuration is a complex system-of-systems environment. All of these systems could face cyber threats in many ways.

B. Support systems

Based on our previous articles (Pöyhönen & Lehto, 2017; Pöyhönen, 2022), the concept of national critical infrastructure can be simplified in accordance with three essential system layers. At the base layer is the electricity network, above that is the information network layer and above these are services. Each layer in system-of-systems thinking can assume its own strategic role and identify its operation as part of an entity whose other parts depend on a reliable functioning of these layers. This also facilitates the identification of cyber dependencies within the layers so that they can be secured with the most efficient and practical measures. In this port research project, electrical power systems and networks are the support systems for the port services. Due to known threat scenarios, these are also security dimensions that should be taken into account as part of any cyber security assessment.

C. Other dimensions

Ensuring process continuity. Process continuity is related to the systems of critical infrastructures. In 2016, the European Parliament adopted the Directive on security of network and information systems (the NIS Directive), with the aim of bringing the cybersecurity capabilities for the essential services of critical infrastructures to the same level of development in all EU Member States. Doing so means that exchanges of actions, information and cooperation should be efficient within and between the organizations of essential services, including at the cross-border level. Operational risk is a crucial part of the prudent regulation and supervision in the sectors of critical infrastructures. It covers all operations including the security, integrity and resilience of network and information systems. The core idea of the NIS directive is that the relevant service operators must ensure business continuity in the case of adverse information security disruptions and report any substantial information security breaches to authorities. According to ANNEX-II of the directive, the transport sector is one of the sectors to be covered by the regulations of the NIS Directive. (EU, 2016; Vähäkainu, Lehto, & Kariluoto, 2022)

Smart ports, as part of critical infrastructure, are facing various cyber threats that may lead to the appearance of events that will cause the disruption or failure of services processes. It is useful to minimize the impact of cyber disruptions and thus ensure the continuity of services by strengthening system resilience. Resilience can be seen as an organization's capacity and capability to achieve its purposes in both predictable and unpredictable situations or under continuous stress caused by cyber security threats (Pöyhönen et al., 2018). The resilience metrics framework proposed by Linkov et al. (2013a) is utilized by applying resilience measures to an organization's operational processes. The framework combines the four stages of a system (plan/prepare, absorb, recover, and adapt) with the four domains of a system (physical, information, cognitive, and social). Later Linkov et al. (2013b) have applied their model further to cyber systems.

Security awareness. Efficient cyber security management in general and, in this case, for smart ports requires close collaboration among management, situational awareness (SA), and communication. In that sense, good management requires the casting of different port operators and their decision-making ability and the building of real-time situation awareness of ICT and ICS/OT assets as well as a common cyber environment (situational understanding, evaluation of situational development). The capabilities of crisis communication, information sharing, and supporting technical solutions, business continuity management, and cooperation are also needed for the good practice of security management. Such management is a combination of the actions of all the organization's decision-making levels (strategic, operational, and technical/tactical) and utilizes the national and international strengths of information sharing. (Pöyhönen, et al. 2021)

The security operation center (SOC) is a centralized cyber security feature of an organization employing people, processes, and technology to continuously monitor an organization's security situation. It has the ability to prevent, detect, analyze, and respond to cybersecurity incidents. In the case of ports, it is recommended as a good practice: "The SOC acts as a centralised unit dealing with security issues that affect a port/port facility, including those relating to cyber security, and may form part of an operations centre supervising the port,

controlling access and managing business continuity and disaster recovery activities" (Boyes, Isbell, & Luck, 2020).

SA can be implemented based on SOC information and national as well as international information sources. Ensley (1995) has developed an SA model when working in the service of United States Air Force. According to her, the core of SA consists of three basic levels: detection (Level 1), situational understanding (Level 2), and its impact assessment towards the future (Level 3) (Ensley, 1995). A comprehensive SA of port processes provides a foundation for conclusions and the subsequent decision-making in cyber security incidents.

Training. The continuous improvement of activities related to the development of staff competence enhance an organization's capability. Taking the staff into account at all organizational levels, as well as focusing on competence and the possibilities it opens to fully influence in the organization, develops the overall operations of the organization (Finnish Standards Association SFS, 2016). Cyber security training as well as other development of staff competence enhance an organization's capability to proactively prevent disturbances and tolerate potential changes in process operation such disturbances might cause.

The maritime sector is increasingly at risk of cyber-attacks due to advances that are already in the process of being implemented, such as port services that utilize new technologies. For that reason, the level of knowledge and training on cyber security and its interaction with the marine ecosystem must be continuously maintained. Recent research results on the topic show a lack of general knowledge in the field of maritime cyber security. Therefore, it is necessary to establish cyber security training as one of the security dimensions in the maritime field. (Alcaidea & Llave, 2019)

4.5 Security capabilities

Different cyber security elements are related to various components, including people, processes, and technology. In their framework, Thai and Grewal emphasize people, processes, and systems/technology as one of the most important elements. The human factor has always been seen as a key factor in any security management system. Concurrently, the importance of people and several combinations of this element, such as people and communication, people and processes, and people and systems/technology, are highly visible. (Thai & Grewal, 2007)

Jacobs, von Solms, and Grobler (2016) state that "the governance documents of an organization typically [prescribe] sets of controls to be implemented, such as technical controls, administrative controls, and physical controls." In many cases these documents describe very specific capabilities that are needed and have to be developed in securing operational continuity in the cyber domain. Capabilities consisting of "people, processes and technology" are key elements in achieving secure outcomes or effects.

4.6 Criteria

An organization's cyber security operations require comprehensive awareness on the system level. Apropriate awareness thus supports cyber risk management and, more extensively, the evaluation of an organization's whole cyber capability. By integrating an organization's three main decision-making levels (strategy, operational, and technology/tactical) into the structure of its cyber operating environment, it is possible obtain a holistic system view of an organization's cyber security tasks. It is a system-based approach to the topics and principles of an organizations comprehensive cyber security. The combination of system views, decision-making levels, and an organization's cyber structure can be considered a framework for evaluating cyber security management. (Pöyhönen & Lehto, 2020).

For the goals of cyber security in a smart port environment, the risk management and continuity enhancement of system operations establish criteria for security management. In that sense, the strategy, operational and technology/tactical viewpoints on the systems of stakeholders support a holistic approach to security.

5. Discussion

ENISA report (2019) "Port Cybersecurity" identifies good practices for cybersecurity in the maritime sector taking care undergoing digital transformation in ports operations and processes. In order to meet emerging challenges is recommended to optimise existing processes and introduce new capabilities, such as automation and real-time monitoring of operations. Digital transformation trends and policies and regulations require ports to face new challenges with regards to the Information and Communication Technology (ICT) and as well as on Industrial

Control Systems (ICS) or Operation Technologies (OT) worlds. The report underlines need to have a high-level reference model based on the research and information of port structure. Its objectives are to list, from a high-level perspective, the main port systems, data flows and interactions with external systems.

The Institution of Engineering and Technology, IET, (2020) in "Good Practice Guide, Cyber Security for Ports and Port Systems", says that "a port is a complex cyber environment that encompasses both land and waterside activities and systems". The loss of cyber security in one section, or more, of port assets has the potential to impact upon efficiency at the port operations, safely of operations or the health and safety of staff and other people.

The Directive 2016/1148 (NIS Directive) is an EU-wide cybersecurity legislation. It covers the maritime sector as one of the essential services under Union legal acts in people, processes and technologies of ports. It recommends also that member States should take into account existing and future international codes and guidelines developed in particular by the International Maritime Organisation. (EU, 2016)

IMO (2017) "Guidelines on Maritime Cyber risk Management" provides high-level recommendations for maritime cyber risk management as an essential measure to ensure the continuity of operations and processes in maritime.

The aim of this paper "Basic Elements of Cyber Security for a Smart Terminal Process" is to give the description of the smart port environments at the system of systems level and thus makes it easier to perceive the cyber security requirements described above.

6. Conclusion

This paper provides a holistic research approach for the investigation of the cyber security of the system elements of smart terminal processes in the development of port operations. It includes system-of-systems thinking and it emphasizes the importation of system description at the beginning of the research project. The findings of the study are related to the basic elements of port operations. These are port services for ship turnaround, truck traffic, and passenger processes. SMARTER research activities are related to digitalization survey with the use of new technologies in order to achieve the main objectives, which are the reduction of emissions by optimizing port logistics and enabling exceptional flow and experience for passengers and cargo.

Comprehensive cyber security research needs to understand the basic system elements of smart terminals as well as the content of those elements. The basic elements have been identified and the result can be called PortCSMS. According to PortCSMS, these elements are as follows: activities, stakeholders, organizational relationships, security dimensions, security capabilities, and criteria. The contents of these are also listed. In addition to these elements, a research framework is needed to address the questions. The next steps are to study the comprehensive cyber security architecture as part of SMARTER program.

Future research on cyber security in the SMARTER project will now be based on what the basic elements of the port are determined to be. After this, it will be possible to work towards answering the main research question of the project: How can a comprehensive cyber security architecture for smart port processes be developed?

References

Accenture. 2022. Digital Transformation through IT/OT convergence. Accessed: 26/9/2022. https://www.accenture.com/fi-en/case-studies/natural-resources/digital-transformation-through-it-ot-convergence

Alcaidea, J. I. & Llave, R.G., 2019. Critical infrastructures cybersecurity and the maritime sector. AIIT 2nd International Congress on Transport Infrastructure and Systems in a changing world (TIS ROMA 2019), 23rd-24th September 2019, Rome, Italy. ScienceDirect. Transportation Research Procedia 45 (2020) p. 547–554.

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

Boyes, H., Isbell, R: & Luck, A., 2020. Good Practice Guide Cyber Security for Ports and Port Systems. Institution of Engineering and Technology, London, United Kingdom.

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, 2020a. SEA FOR VALUE (S4V). 12.2.2020. https://www.dimecc.com/dimecc-services/s4v/

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

Endsley, M.R., 1995. Toward a theory of situation awareness in dynamic systems. Hum Factors Ergon Soc 37(1), p. 32–64.

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

EU, 2016. Directive (EU) 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. The European Parliament and the Council of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148

Finnish Standards Association SFS, 2016. Johdanto laadunhallinnan ISO 9000 -standardeihin. Available on 20th September 2022: slideplayer.fi/slide/11133323/

IET, 2020. Good Practice Guide. Cyber Security for Ports and Port Systems. The Institution of Engineering and Technology. UK.

IMO, 2017. GUIDELINES ON MARITIME CYBER RISK MANAGEMENT. MSC-FAL.1/Circ.3 5 July 2017. International Maritime Organization.

Jacobs, P. C., von Solms, S. H. & Grobler, M. M., 2016. Towards a framework for the development of business cybersecurity capabilities. International Conference on Business and Cyber Security (ICBCS), London, UK. The Business and Management Review, Volume 7 Number 4, p. 51–61.

Linkov, I., Eisenberg, D., Bates, M., Chang, D., Convertino, M., Allen, J., Flynn, S. and Seager, T., 2013a. Measurable Resilience for Actionable Policy. Environmental Science & Technology.

Linkov, I., Eisenberg, D., Plourde, K., Seager, T., Allen J. and Kott, A., 2013b. Resilience metrics for cyber systems. Environment Systems and Decisions, 33(4), p. 471-476.

PricewaterhouseCoopersin (PwC), 2016. Industry 4.0: Building the digital enterprise. https://www.pwc.com/gx/en/industries/industrial-manufacturing/publications/assets/pwc-building-digital-enterprise.pdf

Pöyhönen, J. & Lehto, M., 2017. Cyber security creation as part of the management of an energy company. Proceedings of the 16th European Conference on Cyber Warfare and Security ECCWS2017. 29 - 30 June 2017, Dublin, Ireland. Published by Academic Conferences and Publishing International Limited. Reading. UK. p. 332-340.

Pöyhönen, J., Nuojua, V., Lehto, M. & Rajamäki, J., 2018. Application of Cyber Resilience Review to an Electricity Company. Proceedings of the 17th European Conference on Cyber Warfare and Security ECCWS2018, 28 – 29. June 2018, Oslo, Norway. Published by Academic Conferences and Publishing International Limited. Reading. UK. p. 380-389.

Pöyhönen, J., Rajamäki, J., Nuojua, V., & Lehto, M., 2021. Cyber Situational Awareness in Critical Infrastructure Organizations. In T. Tagarev, K. T. Atanassov, V. Kharchenko, & J. Kacprzyk (Eds.), Digital Transformation, Cyber Security and Resilience of Modern Societies (p. 161-178). Springer. Studies in Big Data, 84. https://doi.org/10.1007/978-3-030-65722-2_10xx

Pöyhönen, J., Kovanen, T. & Lehto, M., 2021. Basic Elements of Cyber Security for an Automated Remote Piloting Fairway System. Proceedings of the 16th International Conference on Cyber Warfare and Security ICCWS2021, 25 - 26 February 2021, Tennessee, USA. Published by Academic Conferences and Publishing International Limited. Reading. UK. p. 299-308

Pöyhönen, J. & Lehto, M., 2020. Cyber security: Trust based architecture in the management of an organization security. Proceedings of the 18th European Conference on Cyber Warfare and Security ECCWS2020, 25-26 June 2020, Chester, UK. Published by Academic Conferences and Publishing International Limited. Reading. UK. p. 304-313

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. (p. 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

Simola, J. & Pöyhönen, J., 2022. Emerging cyber risk challenges in maritime transportation. Proceedings of the 17th International Conference on Information Warfare and Security ICCWS2022. 17-18 March 2022, Albany, New York, USA. Published by Academic Conferences and Publishing International Limited. Reading. UK. p. 306-314.

Thai, V.V. & Grewal, D., 2007. The Maritime Security Management System: Perceptions of the International Shipping Community, 2007. Article in Maritime Economics & Logistics, June 2007.

Vähäkainu, P., Lehto, M. & Kariluoto, A., 2022. Cyberattacks Against Critical Infrastructure Facilities and Corresponding Countermeasures. Cyber Security, Critical Infrastructure Protection. Martti Lehto Pekka Neittaanmäki Editors. Springer. Computational Methods in Applied Sciences. Volume 56. Chapter 11. (p. 255-291). 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