Emerging Cyber risk Challenges in Maritime Transportation

Jussi Simola and Jouni Pöyhönen
University of Jyväskylä, Finland
jussi.hm.simola@jyu.fi
jouni.a.poyhonen@jyu.fi

Abstract: Maritime security and surveillance have become one of the main areas in managing overall situational awareness. For example, the growing importance of maritime traffic in cross-border trade has created new pressures to develop new technologies for accident prevention, especially in the ports. Maritime safety is also a matter of concern for continuity management. Automatic ship alarm systems, coastal radars and coastal cameras are not alone sufficient equipment to build maritime awareness. The Universal Shipborne Automatic Identification System (AIS) is a ship transponder system that is a globally used tracking system, but highly vulnerable to hacking. A major maritime traffic problem arises if transponders are switched off. Hybrid threats need coordinated hybrid responses; therefore, a cyber situational picture is also needed. Cyber situational awareness is an essential part of the management of maritime situational awareness. The lack of using real-time data from the maritime actors affects the correct formation of the common situational picture—for example, from the site of an accident. Cyber security is an essential factor in developing fairway navigation and all terminal (port-to-port) activities. This research will be done as a part of the SMARTER (Smart Terminals) -project that belongs to the SEA4VALUE program. The project aims to develop unique digitalized concepts that enhance safe transportation and reduce emissions in the port and the terminal areas. By using the multiagent system with sensor technology, e.g., in the harbors, it is possible to gather and share meaningful maritime security-related data. The study's primary purpose is to describe the operating environment and make an initial analysis of system requirements for optimizing situational awareness in the area of western ports of Finland.

Keywords: Situational awareness, port systems, cybersecurity, risks, information sharing

1. Introduction

"Maritime transport is a crucial activity for the European Union economy. It enables import and exports of goods, supply in energy, trade within the European Union and transport of passengers and vehicles. This activity relies on more than 1 200 seaports within the European Union, each with 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. This development can help create safer, more efficient, sustainable, and reliable service chains to meet the requirements for a better quality of life and global prosperity. Harbor operations connect the maritime transport to other modes of transportation and enable multimodal transportation. Smart harbors are in a central role in future transport logistics and supply chains. Well-build digital harbor infrastructure is essential in optimizing operations and planning for future investment and maintenance needs. Progressive data management and data sharing are the key issues for transparent, interoperable, safe, effective and environmentally friendly operations.

In Finland Smart Terminals (SMARTER) research project enlarges the scope of DIMECC Sea4Value program (DIMECC, 2020 a) to harbors and ports by develop solutions that benefit maritime transportation harbors in reducing emissions by optimizing harbor operations and improving cargo and people flow while improving the experience 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, 2020 b).

At the same time of the development of digitalization, it also includes the existing maritime cyber environments. Therefore, it is necessary to address the relevant safety aspects of the maritime autonomy solutions. In any cyber environment, it is crucial that there are trustable information networks. In addition, the usability, reliability, and integrity of systems data needs to be high within the operating environment, where cyber security risks are continuously being highlighted by the threatening scenarios posed by the digital world. A modern society depends entirely on a cyber environment that provides dynamic services.

Especially the development of Information and Communication Technology (ICT) or Information Technology (IT) and Industrial Control System (ICS) or Information Technology (IT) systems will make different kinds of autonomy

solutions possible in all kinds of infrastructures. For example, in maritime systems the Universal Shipborne Automatic Identification System (AIS) is a ship transponder system that is currently used by most actors in the commercial shipping industry. The transponder transmits and receives information on VHF channels and thus enhance situation awareness in ships, but this globally used tracking system is highly vulnerable to hacking. For the maritime system of systems point of view, a major maritime traffic problem arises if transponders are forced to switch off in case of wrong operating. System-level threats are needed to be coordinated like hybrid responses; therefore, a system of systems-level cyber situational picture is also needed.

Digital assets of ports have two main digital assets groups. Information Technology (IT) systems, focused on the use of data as information, and Operational Technology (OT) systems, which use data to control and/or monitor physical processes (encompasses Industrial Control Systems including Supervisory Control and Data Acquisition and Distributed Control Systems) (ENISA 2019).

The SMARTER project aims are to develop unique digitalized concepts that enhance safe and effective transportation logistic in port and terminal areas. By using the multiagent system with sensor technology, e.g., in the harbors, it is possible to gather and share meaningful maritime security-related data. In that sense securing the cyber aspects of an interconnected system of maritime hosted by multiple stakeholders requires a system-of-systems view in cyber security. The main cyber security research question in this project is the following: How can a comprehensive cyber security architecture for smart port terminal be developed? However, we must first find an answer to the next question: Where can we direct the cyber security research to cover whole system of systems entity in port operation? A situation awareness from whole process elements is needed. Authorities and those involved in transporting goods and people need autonomous solutions and a logistical situational picture of both the port and the fairway. It is also about risk management, emissions, efficiency and continuity management. Consumers also need smooth port operations but a reliable picture of cargo and passenger traffic.

This paper provides a research approach for the investigation of cyber security at the system level and gives an answer to the question of where to direct cyber security research in the case of the SMARTER program. The paper emphasizes the importation of system description of the port process and its elements at the beginning of the research program. After that, the research will be able to continue to specify the comprehensive cyber security aspect of architecture like threat and vulnerability investigations, risks assessment and cyber security measures for the SMARTER project by the end of 2023.

2. The research objectives and port operations

2.1 Essential maritime security actors in the European Union

European Maritime Safety Agency (EMSA) works under the European Union and serves the EU maritime interests for a safe, secure, green and competitive maritime sector in Europe and worldwide. EMSA is the essential stakeholder in the maritime cluster in Europe and beyond. It provides services to the EU Member States and the Commission but also an innovative knowledge hub for the European maritime environment (European Maritime Security Agency 2022)

European Union Agency for Cybersecurity (ENISA) is the agency that works under the European Union purposed to achieve a high common level of Cybersecurity across Europe. ENISA contributes to EU cyber policy, aims to enhance the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperate intensively with the Member States and the EU bodies, and help Europe to prepare for the cyber challenges.

The International Maritime Organization (IMO) is the agency of the United Nations, which is responsible for measures to improve the safety and security of global shipping and prevent pollution from ships involved in legal matters, including liability and compensation issues and the facilitation of international maritime traffic (IMO 2019).

The International Maritime Cyber Centre of Excellence (IMCCE) consists of a Maritime Cyber Emergency Response Team (MCERT) and a cyber academy. The MCERT is an international cyber intelligence and incident support platform for the entire maritime ecosystem by providing international intelligence feeds, advice and support, including real-time assistance to members on cyber-attacks and incidents, and a Cyber Security

Reporting Portal (CSRP) for its members. The IMCCE will provide a focal point for the industry to help drive cyber awareness and response to cyber incidents (Container-News 2018).

2.2 Earlier investigations related to challenges of maritime security

Operators as Vessel Traffic Systems Operator tracks vessels to ensure that traffic is safe and safe distance between vessels is standard. Challenges of border guard operational work have listed below. Following challenges of formation of situational awareness have been investigated earlier by Simola & Rajamäki (2018). The challenges may be reflected more broadly in the port and fairways activities if physical and hybrid threats are not recognized.

1. The West Finland Coast Guard District is responsible for security in the whole sea area in Western Finland. The area of operations of the West Finland Coast Guard District covers the emergency area of four emergency centers.
2. The monitored area is quite broad, and they have to share the groups between the different workstations when a major accident occurs.
3. System-based obstacles in cross-border cooperation. Small ships or boats that are attempting to cross the Schengen border create additional challenges.
4. The situational picture of an individual patroller is based on the Virve communications and background information that has been collected before via radio communication.
5. Lack of automated functions and resources

Operational fieldwork covers statutory tasks involving the leading positions of other authorities as provided by the law on the Border Guard (Border Guard Act), such as executive assistance tasks and the management of Maritime Rescue.

2.3 Smart Terminals (SMARTER) research project in Finland

In Finland, the Sea4Value / Fairway (S4VF) research program has been established to create autonomy in maritime solutions (DIMECC, 2020 a). The first stage of the program concerns on automated remote pilotage fairway navigation. Now in the second phase of the program will leverage to harbor operations. This Smart Terminals (SMARTER) research project 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, 2020 b)

- The first is the reduction of emissions by optimizing port logistics.
- The second objective is to enable exceptional flow and experience for the passengers and cargo.

The structure of the project has been planned to have three use cases (Figure 1). The use cases are: Ship turnaround, truck traffic and passenger flow. Use cases are designed to support one another and there is a linkage between the use cases. The applied research work is organized into five work packages led by a responsible team of researchers. Cyber security research actions are included to Work Package 4 (WP4).

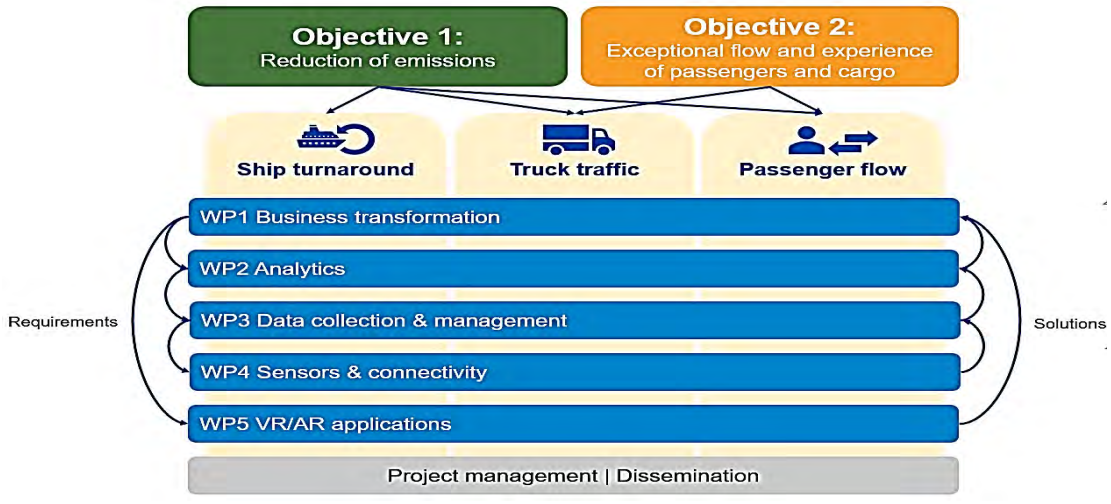

Figure 1: Project structure

In maritime transportations, the sea areas can be distributed to different approach areas of ports and ports itself. A ship proceeding to any port from the open sea through a fairway faces different demands during its transit, such as shallow waters, narrow shipping lanes, environmental effects and heavy traffic. After that a ship is ready to berth to a pier in the destination port and load or unload its goods, trucks/cars, or passengers. Port stakeholders and logistic systems are needed in successful port operations. Land transportation and its systems are included to port facilities. After that, it is also obvious that the regulatory requirements and needs for cooperations and communication with different stakeholders have been considered as part of port operations. In all cases of port processes, the information requirements and the amount of information needed are related to the accuracy and reliability of safety services. Figure 2 presents these processes. Cyber security awareness and information should cover all process elements.

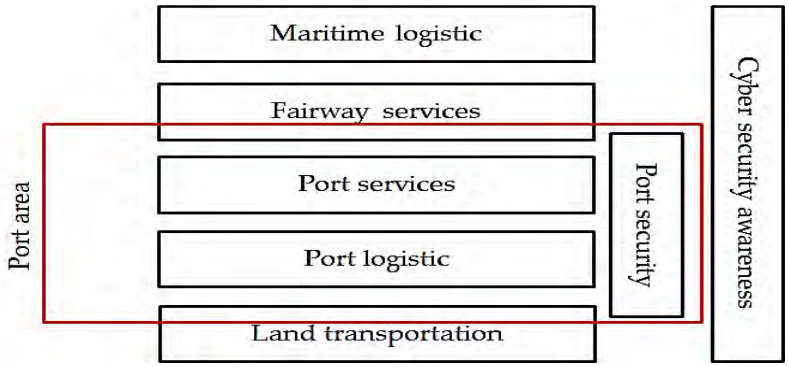

Figure 2: Port Processes

The research concentrates on examining and determinate impacting cyber risk factors and analyzing initial system requirements for the fairway navigation in the area of western ports of Finland. As figure 2. illustrates, the Port area consists of several functionalities. In addition to divided three sections, “Port Services, Port Logistic, and Port Security”, the port area expands its impacts to fairway services and land transportation. From the viewpoint of exploring the operating environment, it is necessary to understand the interaction between different functionalities. Working business continuity management means unexpected interruptions are removed or minimized. All sections of the process have to work under the umbrella of cyber security awareness. Cyber security is one crucial part of business continuity management.

The IMO Resolution Maritime Safety Community 428(98) states guidelines for Maritime Cyber Risk Management in Safety Management systems. Cybertechnologies are crucial to the operation and management of several systems critical to the safety and security of shipping and protection of the marine environment. The vulnerabilities of accessing, interconnecting, and networking of these systems may lead to realized cyber threats. (The, Maritime Safety Committee 2017).

A Mentioned above, a stable controlling system for transportation and other processes require a command and control or situation center that combines and analyze relevant data from the port, port facilities and functions. All kinds of practical information are needed. Monitoring different kind of threats is one crucial element, but it is required to monitor systems health also. Cyber domains have inner and outer vulnerabilities and threats. The port area consists of several of systems that have to be connected or integrated with each other. Efficient information sharing and updating situational awareness belong to each other. Improved situational awareness needs predictive functionalities that alert before any threats are realized.

3. Cyber security research framework

Traffic and transportation supply chains and their critical stakeholders’ systems are complex systems of systems characterized by a conglomeration of interconnected networks and dependencies. According to the EU Commission, ICT systems are significant parts of the operations and core processes. ICT systems are related to administration and to the management of information in the network. The components of the process levels also include ICS systems (EU Commission, 2009).

Martin C. Libicki (2007) has created a model of the cyber world based on The Open Systems Interconnection Reference Model (OSI), which has the following four layers: physical, syntactic, semantic, and pragmatic. Martti Lehto, a professor of cyber security at the University of Jyväskylä, has updated the four layers in Libicki’s (2007)

cyberworld model by adding a fifth layer that considers organizations' networks, ICT and ICS systems and the components of the systems (Lehto & Neittaanmäki, 2018). The five-layer structure for the cyber world of organizations is considered the research framework in this study on the cyber security of the port operations.
An organization's cyber security operations require comprehensive awareness on the system level. The awareness of an organization and decision-makers can be seen as system-level awareness arrangement.

. It is possible to integrate an organization's three decision-making levels into a five-layer cyber structure in order to have a comprehensive system view of that organization's cyber security environment. 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 is described in Figure 3 (Pöyhönen & Lehto, 2020).

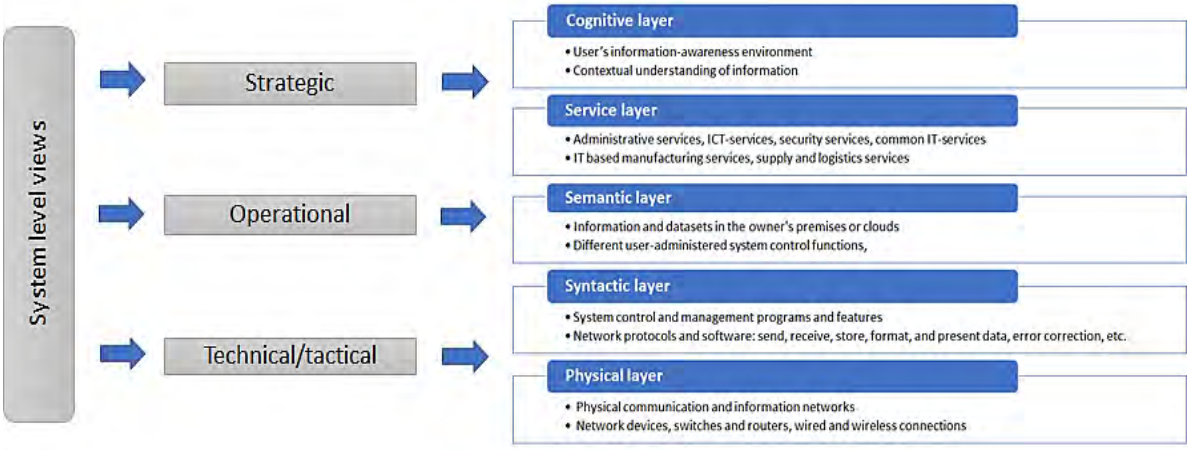

Figure 3: System-level view on organizational cyber security (Pöyhönen & Lehto 2020)

This case study is carried out with the guidance of Yin (2014). The case study illustrates the attempt to produce detailed information about the object being researched. The materials collected for this case study are based on publications, official reports, articles and other literary material.

The aim is to utilize the framework to define IT and OT ecosystem in the port environment that affects flowing port activities. Enhanced formation of situational awareness, information sharing and efficient decision-making processes are essential elements for the business continuity management. How and where to enhance and implement organizational cyber-physical security practices and how to create a hybrid secure umbrella for the port functionalities is the relevant issue in this initial research. As the simplified figure 3 illustrates, the maritime cyber-physical ecosystem consists of different systems and systems of systems. The crucial challenge encompasses several "system entities". Coherent formation of Maritime Situational Awareness requires functional interfaces from the systems. The separate system requirements of public authorities and commercial activities need to be coordinated. Vessel Traffic Services provider Finntraffic maintains maritime situational awareness, separate Control Center as Security Operations Center follow up their own situational picture and in addition to this, Coast Guard follow their own screens in the Maritime Rescue Command Center (Simola, Rajamäki 2018).

The following types of information and communication systems are used in maritime area for example; GOFREP (Gulf of Finland Reporting System), PORTNET Ship and port traffic notification system maintained by the authorities in Finland, Vessel Monitoring Systems (VMS), RFID (Radio Frequency Identification), AIS (Automated Identification System), VIRVE- KEJO-, POKE-equipment for authorities, RVT-mepe, NERCS, CleanSeaNet (CSN) the Union maritime information and exchange system, GPS-systems, Radar systems. SARSURPIC is the Search and Rescue for European Union authorities.

Figure 3: Communication Relationships between the Blocks in the Port Operations

4. Port operations and cyber security awareness

In their paper, "The Maritime Security Management System: Perceptions of the International Shipping Community" (2007), Vinh V. Thai and Devinder Grewal from Australian Maritime College emphasize the importance of identifying key shore-based and near-shore activities associated with maritime security management. The paper presents the findings of a research project on the Maritime Security Management System (MSMS). The principles of the paper can also be used for cyber security analyses in maritime environment. Then the main tasks are related to identifying key cyber security features associated with maritime operations. (Thai & Grewal, 2007, Pöyhönen, Kovanen & Lehto, 2021).

A cyber security situation model captures information about potential cyber threats against a system of systems (SoS) including operational and technical systems, an enterprise, a region, or a critical infrastructure (CI) sector. A comprehensive cyber security needs wide scale of analysis of a system of systems (or sub-system) against a set of threat events. Using threat scenarios makes it possible to get a picture of potential threats. This could materialize and result of harmful consequences and eventually lead thought to risk analysis and cyber security measures. Potential uses of threat scenarios should cover three scopes or scales involving systems of systems: the mission or business function, the enterprise, and the sector (or sub-sector) or region. (Bodeu & McCollum, 2018)

In the port research environment and in the cyber security investigation, there are three main processes, Ship Turnaround, Truck Traffic, and Passenger flow. On the other hand there are processes, relevant stakeholders, within organizations, operational regions and the maritime CI sector. Security elements like people, processes and technology are the key capabilities in the cyber environment, but at the same time they include vulnerabilities. In addition of processes and relevant stakeholders, people, processes, and technology are the third part of cyber security investigation. All these parts should be covered in order to have good situational awareness to relevant threats, vulnerabilities, risks and cyber security measures.

As an answer to the question: Where can we direct the cyber security research to cover the whole system of systems entity in port operation? the following consideration take place:

4.1 People: Stakeholders

Different surveys state that even though organizations have made significant security improvements, they have not kept pace with today's determined adversaries and, as a result, many rely on yesterday's security practices to combat today's threats. It is obvious that a new model of cyber security that is driven by knowledge of vulnerabilities threats, assets, potential attack impacts, and the motives and targets of potential adversaries is required and extends to the entire maritime ecosystem from fairway piloting to all port operations.

Securing the cyber aspects of an interconnected system of maritime hosted by multiple stakeholders requires a system-of-systems view in cyber security. Digital transformation in providing safe maritime environment requires holistic approaches to analyze the whole operating environment. Digital transformation promotes reassessing and redesign of existing maritime services. The organizations of port stakeholders should have strategic, operative and tactic/technic views to the cyber structure of their own operational environment.

The strategic level, choices are primarily related to organization social responsibility, organization reputation, and ensuring business continuity (Finnish Standards Association SFS, 2016). The leadership is expected to make concrete strategic choices to guide and support the execution of relevant cyber situation awareness throughout the organization (Pöyhönen & Lehto 2020). The chosen measures should be comprehensively communicated to the organization's interest groups (Stouffer K., Falco J. and Scarfone K., 2011).

The measures at the operational level promote the strategic goals and thus comprehensive measures will increase situational awareness for holistic cyber security management. It must be based on risk assessment and analyses of the measures based on the assessment. It is also important that the organization declares and communicates the policy with which the leadership commits to the measures required to develop cyber security management. The declaration of a policy that ensures cyber security and the development of related procedures must be integrated with the organization's general policies (Pöyhönen & Lehto 2020). The highest organizational level is responsible for creating a policy that defines acceptable risk levels and the measures used in the reduction of risks (Stouffer et al., 2011). The maintenance of situational awareness regarding the cyber environment of the organization's processes makes possible to monitor and react efficiently to risks that constitute a threat within the organization's operating environment.

The tactical organization level encompasses the services and technologies that comply the processes with the structure of the cyber world (Pöyhönen & Lehto 2020). Consistent and predictable results are achieved more efficiently when operations are handled and managed as interrelated processes that function as a coherent system (Finnish Standards Association SFS, 2016). Cyber security threats and risks set special requirements for these processes and need for situation awareness at this level in addition to other operational requirements. In the cyber environment, the target can be achieved by defining the processes to be protected, choosing process control mechanisms successfully, and by using expedient technological solutions and services to protect the processes (Stouffer et al., 2011).

4.2 Process: Ship Turnaround, Truck Traffic, and Passenger flow

Processes are key to the implementation of an effective cyber security strategy. Processes are crucial in defining how the organization's activities, roles and documentation are used to mitigate the risks to the organization's information. Processes also need to be continually reviewed: cyber threats change quickly, and processes need to adapt with them. But processes are nothing if people don't follow them correctly (Dutton 2017).

4.3 Technology: Ship systems, Port systems, Port logistic systems, Truck Traffic systems

Technology is obviously crucial when it comes to cyber security. By identifying the cyber risks that your organization faces you can then start to look at what controls to put in place, and what technologies you'll need to do this. Technology can be deployed to prevent or reduce the impact of cyber risks, depending on your risk assessment and what you deem an acceptable level of risks (Dutton 2017).

ISO/IEC 27001:2013 (ISO27001) is the international standard for information security that specifies an information security management system (ISMS). The ISMS assists organizations manage their information security by addressing the people, processes, and technology (International Organization for Standardization, (ISO) 2013). NIST produces a voluntary set of guidelines for organizations against cybersecurity risks. NIST Cybersecurity Frameworks (CSF) does not replace ISO security standards, but it supports all other essential guidelines and guidances. The five simple core functions of the framework are as follows a) Identify, b) Protect, c) Detect, d) Respond, e) Recover (NIST 2018). It is usable for the different kinds of maritime stakeholders. The crucial challenge is that actors and their procedures to tackle cyber threats vary significantly in the shipping environment. Others have invested a lot of resources to protect systems, working methods and procedures at strategic, operational, and tactical levels. Others have done almost nothing to protect their working environment.

Effective working environments require effective cyber threat prevention mechanisms, but in addition to this, physical threats must have to ability to eliminate. Hybrid threats form a combination of these.

5. Discussion

In the SMARTER research project, the main aim is to have future ports more efficient than they have been before. That will happen to develop the key areas of ship turnaround, truck traffic and passenger flow. The development of these three main port processes includes the collection, production, and processing of cyber situation

awareness information related to all services that are needed in port operations. Cyber security is an essential part of these services.

Firstly, this paper presents a research framework for the study of cyber security in a maritime smart port operations. It is a five-layer cyber structure of an organization (Figure 3) that includes people, services, data, and ICT and ICS systems of the SMARTER process. Other components of it are the system views decision-making levels from every stakeholder's organization, including strategic, operational and tactical/technical levels. The five-level cyber structure and decision-making levels are needed to obtain a comprehensive system view of the cyber security situation from the cyber environment of SMARTER. That makes it possible to provide an answer to the research question: Where can we direct the cyber security research to cover the whole system of systems entity in port operation? It is needed the system thinking approach to organization fife layer cyber structure. It makes it possible to have holistic cyber security architecture using the research framework mentioned earlier in this paper.

6. Conclusion

This paper provides the first research approach for investigating cyber security at the system level in a smart port process of autonomous activities development of maritime operations. It emphasizes the importation of cyber security awareness at all system systems levels at the beginning of the research. The paper emphasizes system thinking using a presented cyber security research framework.

Security elements like people, processes, and technology are the key capabilities in the cyber environment, but at the same time, these capabilities also include vulnerabilities. Vulnerabilities and threats can be divided into internal and external sources. Situation information from port processes, relevant stakeholders, and technologies behind systems, like port systems, port logistic systems and traffic systems, are needed to cover risk assessment of all port environments. Monitoring IT systems and sub-systems health is an essential part of this procedure. Therefore workable situation center or SOC that handles cyber-physical threats from the maritime ecosystem is needed in the port environment. Artificial Intelligence-based solutions will replace human capabilities shortly. Technological development will challenge traditional monitoring systems. It is not enough that humans follow the flow of information from simple screens; cyber situational awareness functionalities must ensure business continuity.

There is also a need to gather and analyze data from the environment and potential threats from outside the port. Cooperation between existing situation centers has to enhance and rationalized. The Finntraffic (VTS operator) and The Maritime Rescue Coordination Centre (MRCC) have a crucial information gathering, sharing and operational role in this environment, not forgetting Custom, Police and rescue services. Efficient threat information sharing is a crucial part of situational awareness that ensures business continuity management. It is also essential that shared information is understood in the same way between different actors.

There is a need for standardized models for digitalized systems and processes, procedures, data handling etc. In the near future, automated artificial intelligence solutions with multiagent systems constitute an opportunity but also threats. The risks of false alerts by AI surveillance systems must be minimized when programming new solutions for the port area. Efficient strategical, operational and tactical situational understanding needs maritime computer emergency response functionalities that cover all system enterprises that are in use. Threats and vulnerabilities have to tackle if the purpose is to reduce pollution and enhance the flow of passengers and goods traffic.

In Finland, Official operators as Vessel Traffic Services have to follow, e.g., the Vessel Traffic Service Act (The Finnish Parliament 2005). The act obligates to inform authorities in all abnormal threat situations. Before organizational changes and artificial automation, Port Facilities need to organize precise and common guidelines on preparing and preventing cyber and physical threats. The combination of system of systems has to control with the same principles. This does not necessarily mean unifying systems into a single system. It has to be possible to disconnect the infected functionalities from the system chain and the system recovery must be capable. Optimizing harbor operations and improving cargo and people flow are essential purposes of the SMARTER project. System-level thinking cannot be separated from each other level. Strategical and operational level understanding about the ecosystem has to support tactical level purposes and vice versa. Horizontal and vertical situational awareness must be at the same level of understanding.

All these parts should be covered in order to have comprehensive situation awareness to relevant threats, vulnerabilities, risks and cyber security measures. After this, the work will continue towards answering the main research question of the SMART project: How can a comprehensive cyber security architecture for smart port terminal be developed?

References

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

DIMECC Oy, (2020a) SEA FOR VALUE (S4V). 12.2.2020. Available on 3 December 2021: https://www.dimecc.com/dimecc-services/s4v/

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

Dutton, J. (2017) *Three pillars of cyber security.* -09-26T10:00:51+00:00, [viewed Jan 12, 2022]. Available from: https://www.itgovernance.co.uk/blog/three-pillars-of-cyber-security.

European Maritime Security Agency (2022) *This is EMSA.* Available from: http://www.emsa.europa.eu/about.html.

European Union Agency for Cybersecurity ENISA (2019) PORT CYBERSECURITY. Good practices for cybersecurity in the maritime sector. NOVEMBER 2019

Finnish Parliament (2005) Vessel Traffic Service Act 623/2005. Ministry of Transport and Communications

Finnish Standards Association SFS (2016) Johdanto laadunhallinnan ISO 9000 -standardeihin. Available on 3 December 2021: slideplayer.fi/slide/11133323/

The first International Maritime Cyber Centre of Excellence (2018) -10-17T09:00:20+00:00 [viewed Jan 12, 2022]. Available from: https://container-news.com/iinternational-maritime-cyber-centre-excellence/

International Organization for Standardization, (ISO) (2013) *ISO/IEC 27002:2013 Security techniques — Code of practice for information security controls.* ISO. Available from: https://www.iso.org/standard/54533.html.

Lehto, M. & Neittaanmäki, P. (2018) The modern strategies in the cyber warfare. Cyber Security: Cyber power and technology. Berlin: Springer.

Libicki, M. C. (2007) Conquest in Cyberspace – National Security and Information Warfare, Cambridge University Press, New York 2007.

Maritime Safety Committee (2017) *Maritime Cyber Risk Management in Safety Management System Resolution MSC.428(98)* , 16 June.

NIST (2018) *The Five Functions.* -04-12T13:27-04:00, [viewed Jan 7, 2022]. Available from: https://www.nist.gov/cyberframework/online-learning/five-functions

Pöyhönen J., Kovanen T. & Lehto M. (2021) Basic Elements of Cyber Security for an Automated Remote Piloting Fairway System. The proceedings of the 16th International Conference on Cyber Warfare and Security ICCWS2021, 25 - 26 February 2021, A Virtual Conference, Tennessee Tech University and the Oak Ridge National Laboratory, USA, pages 299-308

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

Simola, J. and J. Rajamäki (2018) Improving Cyber Situational Awareness in Maritime Surveillance.JOSANG, A., ed. *the 17th European Conference on Cyber Warfare and Security ECCWS 2018*. Oslo, Norway,.

Stouffer K., Falco J., Scarfone K. (2011) NIST Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security. Recommendations of the National Institute of Standards and Technology. U.S. Department of Commerce. Available on 3 December 2021: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

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.

Yin, R.K. (2014) *Case Study Research, Design and Methods.* 5th ed. Thousand Oaks: Sage Publications.