frontiers | Frontiers in Computer Science

TYPE Original Research
PUBLISHED 25 October 2023
DOI 10.3389/fcomp.2023.1154069

OPEN ACCESS

EDITED BY
A. J. Uhlmann,
NHL Stenden University of Applied Sciences, Netherlands

REVIEWED BY
Salih Biçakci,
Kadir Has University, Türkiye
Stephen James McCombie,
NHL Stenden University of Applied Sciences, Netherlands

*CORRESPONDENCE
Jouni Pöyhönen
jouni.a.poyhonen@jyu.fi

RECEIVED 30 January 2023
ACCEPTED 31 May 2023
PUBLISHED 25 October 2023

CITATION
Pöyhönen J and Lehto M (2023) Comprehensive cyber security for port and harbor ecosystems.
Front. Comput. Sci. 5:1154069.
doi: 10.3389/fcomp.2023.1154069

Comprehensive cyber security for port and harbor ecosystems

Jouni Pöyhönen* and Martti Lehto

Information Technology, University of Jyväskylä, Jyväskylä, Finland

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. In the coming years, digitalization and increased levels of autonomy in logistic transport chains are expected to take leaps forward. This development can help create safer, more efficient, more sustainable, and more reliable service chains to meet the requirements for a better quality of life and global prosperity. Port and harbor operations connect the maritime transport to other modes of transportation and enable multimodal transportation. Smart ports play a central role in future transport logistics and supply chains. Digitalization helps improve the efficiency of terminal systems in the processes of these ports. 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) as well as on industrial control systems (ICS) and operation technologies (OT). At the same time, the cyber security of maritime logistics also needs to be addressed. This article presents our findings related to the Sea4Value research goal on cyber security, which is a comprehensive cyber security architecture for port services at the system level. The article emphasizes the importance of a system of systems approach in terms of a comprehensive cyber security management process for port ecosystems. The description and recognition of management steps of every stakeholder are the key elements in this kind of process.

KEYWORDS

maritime logistics, port ecosystem, comprehensive cyber security management, cyber threat intelligence, risk management process

1. Introduction

The European Union Agency for Cybersecurity (ENISA) report "Port Cybersecurity" (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 a 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, more sustainable, and more reliable port services and operations that will play 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 cyber security, both in the Information Technologies (IT) and Operation Technologies (OT) worlds" (ENISA, 2019).

Digitalization makes it possible to create smart navigation, ports, and terminals by utilizing the latest Industry 4.0 technology (Beaumont, 2018; de la Peña Zarzueloa et al., 2020). A well-built digital maritime infrastructure is essential for optimizing operations and planning for future investment and maintenance needs.

Maritime digitalization means the development of solutions for information and communication technology (ICT), information technology (IT), and industrial control systems (ICS) or operation technologies (OT). Maritime transportation consists of a 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 article summarizes the research approach used in the Finnish maritime Sea4Value program to investigate cyber security aspects at the system level in various study cases. The article emphasizes the significance of adopting a system-of-systems approach to the cyber security investigation process, which helps in achieving comprehensive management elements for an organization to secure port and harbor ecosystems. The article highlights, as a conceptual model, the critical cyber security aspects of architecture, including current situation analysis, threat analysis process, risk assessment process, and holistic cyber security measures to ensure the resiliency of the organization of ecosystems in the complex cyber world.

2. The Sea4Value/SMARTER as a use case

The Sea4Value research program in Finland, operated by the DIMECC co-creation ecosystem, focuses on digitalizing fairways and ports. It concluded at the end of February 2023 and aimed to develop new digital solutions to benefit maritime transportation. The Fairway project involves experiments in smart fairway navigation and remote pilotage, while the smart port project (SMARTER) expands the program to include ports and harbors. SMARTER's mission is to create replicable models for digitalization, service innovation, and data usage in the harbor environment, with a focus on smart and autonomous maritime transportation. The project aims to reduce emissions, optimize operations, and improve cargo and people flows while enhancing stakeholder expertise. The Finnish One Sea vision aims to create the world's first autonomous maritime transport system by 2025, and SMARTER is a crucial step toward achieving this goal. The project focuses on developing ports and harbors to meet the needs of autonomous traffic and business through joint innovation between research organizations and Finnish companies. SMARTER seeks to have a wide societal impact by providing research-based recommendations on new business models, standardization, data usage, and sharing, as well as demonstrations and experiments to optimize traffic and improve people flow (DIMECC Oy, 2020a,b).

3. Using soft systems methodology for comprehensive cybersecurity research

Soft systems methodology (SSM) is a qualitative problem-solving and management approach developed by Peter Checkland in the 1970s, used to analyze complex and ill-defined situations that require multiple perspectives. SSM involves a seven-stage iterative process that includes identifying the problem situation and stakeholders, identifying relevant systems, building root definitions, developing conceptual models, comparing models with reality, and taking action to improve the situation. SSM is flexible and can be used in various situations, including organizational change, process improvement, and policy development, ensuring all stakeholders' perspectives are considered (Checkland, 1981).

SSM was developed to provide an organized and flexible process for thinking through problematic situations that require action to be taken. Social situations are complex, and SSM utilizes systems ideas to deal with their complexity, which focus on the interactions between parts of a whole. SSM involves four different kinds of activity, which include finding out about the initial situation, making purposeful activity models, using the models to question the real situation, and defining and taking action to improve the situation (Checkland and Poulter, 2010).

One area of research that utilizes SSM is cyber security research, specifically critical infrastructure protection against harmful attacks and unexpected behaviors. According to our experiences, SSM is well-suited to cyber security research projects that enhance comprehensive security, including people, processes, and technology, requiring a system of systems research attitude to understand the organization and processes as a whole system and inseparable parts of the critical infrastructure actor in the cyber world.

4. Ecosystems of ports and harbors as a rich picture

To effectively use SSM for understanding and improving a real-life situation, the enquirer must approach the situation with an open mind and gather as much information as possible. Using a range of prompts focused on deployment of resources, operational processes, planning procedures, structures, and wider systems is recommended. Rich pictures are a better medium than linear

prose for showing multiple interacting relationships in complex human situations. These pictures evolve as inquiry proceeds and are useful for expressing crucial relationships and providing a basis for discussion. They can be presented to solicit feedback, allowing for corrections and omissions to be identified (Checkland and Poulter, 2010).

A modern seaport can include dozens of stakeholders interacting to run the port processes. A stakeholder organization together with others makes an ecosystem group for port processes and thus for essential maritime transportation activities. The case of a port in a maritime transportation system includes processes such as ship approaches 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 1 presents these processes (Simola and Pöyhönen, 2022).

The rich picture also needs to have key elements for the understanding of the research environment. From the cyber security ecosystem point of view, key elements associated with the operations and processes in ports need to be identified. These can be listed on the heading level as follows: activities, stakeholders, organizational relationships, security dimensions, security capabilities, and criteria. Figure 2 illustrates the cyber security elements of the port study. To cover all these, the result can be called the Port Cyber Security Management System (PortCSMS). The cyber security elements are explained after the figure.

4.1. Activities

The activities in this case are port processes according to Figure 1. All ports play an important role in maritime business processes and, by extension, in global logistics. From the cyber security point of view, business-related issues are the 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

Many stakeholders interact 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 security services. This means that, in an organization, cyber security management includes co-operation with organization leaders, managers, and employees as well as the use of the best partners in outsourcing, clustering, public–private partnerships (PPP), and international cooperation (Pöyhönen and Lehto, 2017).

4.3. Organizational relationships

Port processes and services include the relationships among organizations within the port and harbor as well as those outside of them. It is possible to have an organization's common situation awareness and to have the opportunity to learn about threats, often directly from the operating network or partners and as well as from national cyber security organizations. 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, at the same time, be challenging (Pöyhönen and Lehto, 2017).

4.4. Security dimensions

4.4.1. Main systems

The foundation of main systems is the main port process, including systems for transport and logistics, port service 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 complete system configuration is a complex system of systems environment. All these systems could face cyber threats in many ways.

4.4.2. Support systems

Based on our previous articles (Pöyhönen and 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 the 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 the 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 considered as part of any cyber security assessment.

4.4.3. Other dimensions

Other dimensions are process continuity, security awareness, and training. By ensuring process continuity, the actions are very much related to the systems of critical infrastructures, but also to the activities of the organization itself. Security awareness is part of efficient cyber security management in general and, in the case of port cases, requires close collaboration among port management, the situational awareness (SA) process, and communication. Training is the basis for the continuous improvement of activities in an organization and for the development of staff competence to enhance an organization's capability (Alcaidea and Llave, 2019).

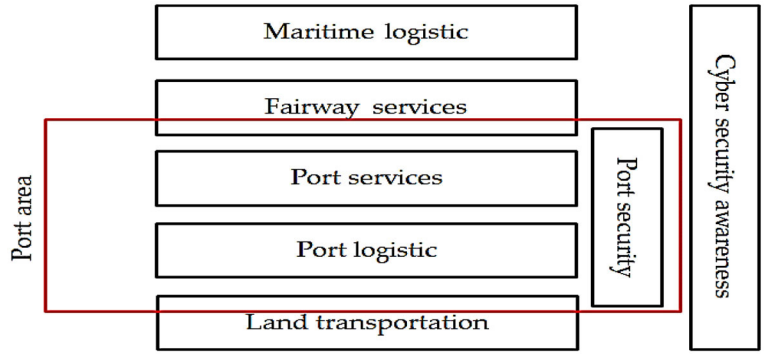

FIGURE 1
Port processes.

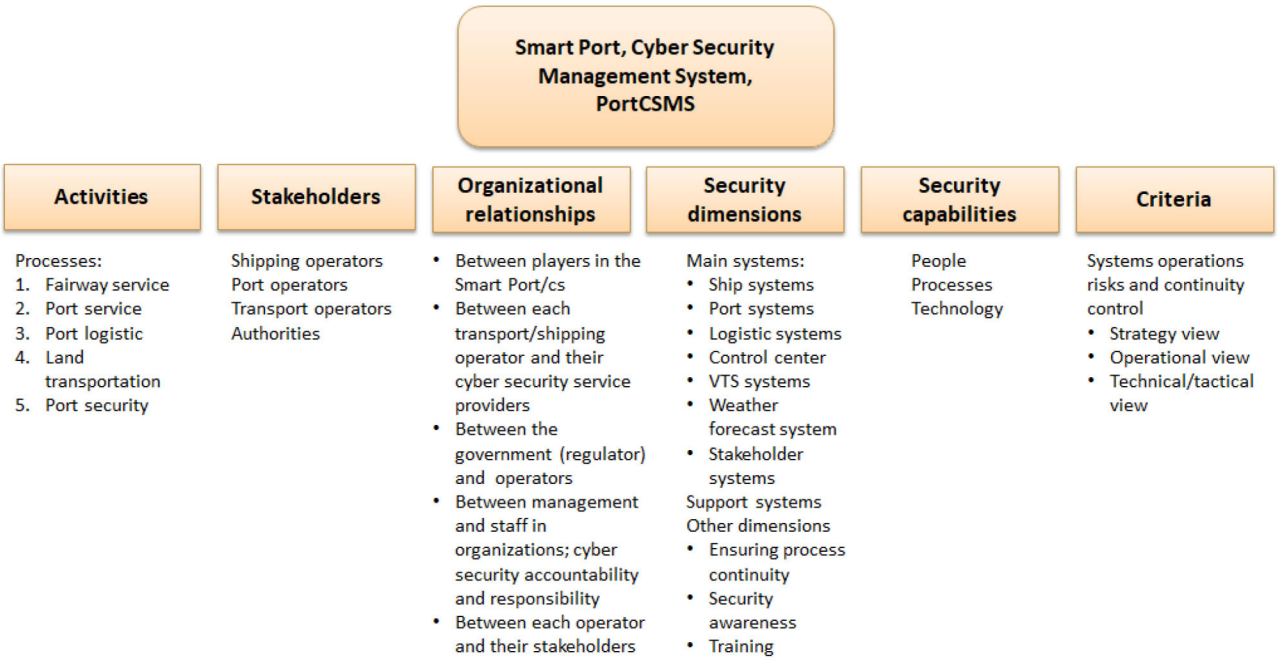

FIGURE 2
Elements of smart port cyber security management, PortCSMS.

4.5. Security capabilities

Different cyber security elements are related to various components, including people, processes, and technology. In their research and paper on the Maritime Security Management System (MSMS) framework, Thai and Grewal (2007) emphasize people, processes, and systems/technology as important elements. The human factor is always seen as the most important dimension and element 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.

Jacobs et al. (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."

4.6. Criteria

An organization's cyber security operations related to business continuity require comprehensive awareness on the system level. Appropriate 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 to 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 organization's 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 and Lehto, 2020).

5. An organization's cyber structure as a root definition

Libicki (2007) created a structure for the cyber world, the idea of which is based on the open systems interconnection reference model (OSI). The OSI model groups communication protocols into seven layers. Each layer serves the layer above it and is served by the layer below it. The Libicki (2007) cyber world model has the following four layers: physical, syntactic, semantic, and pragmatic. Martti Lehto, cyber security professor at the University of Jyväskylä, has updated Libicki's four-layer cyber world model by adding a fifth layer in order to consider an organization's networking needs. The structure is described in Figure 3 (modified from Lehto and Neittaanmäki, 2018).

The content of the structure of the five-layer model is as follows:

1. The physical layer contains the physical elements of the communications network.
2. The syntactic layer contains various system control and management programs and features which facilitate interaction between the devices connected to the network.
3. The semantic layer contains the information and datasets in the user's control systems and computer terminals as well as different datasets for user-administered functions.
4. The service layer contains network-based services and applications.
5. The cognitive layer portrays the user's information-awareness environment and where one's contextual understanding of information is created.

Organizations operate in very complex, interrelated cyber environments, in which new as well as long-used information technical system entities (e.g., system of systems) are utilized. Organizations are dependent on these systems and their apparatus in order to accomplish their missions. The management must recognize that clear, rational, and risk-based decisions are necessary from the point of view of business continuity. The management at best combines the best collective risk assessments of the organization's individuals and different groups related to strategic planning, alongside the operative and daily business management (Joint Task Force Transformation Initiative, 2011).

The Joint Task Force Transformation Initiative (2011) NIST 800-39 special publication "Managing Information Security Risk – Organization, Mission, and Information System View" recommends implementing the organization's cyber security management as a comprehensive operation, in which the actions are dealt with from the strategic to tactical levels. In that sense, the necessity of the organization's cyber security operations can be depicted as necessary for comprehensive awareness on the system level. The organizational and decision-maker awareness can be seen as system-level awareness arrangement. Thus, appropriate awareness supports the cyber security management and, more extensively, the evaluation of the organization's whole cyber capability. We have integrated the organization's three decision-making levels into a five-layer cyber structure in order to have a comprehensive system view and root definitions for the organization's cyber security environment. It is a systems-thinking approach to an organization's cyber security subject. The principle is described in Figure 4 (Pöyhönen and Lehto, 2020).

6. The holistic cyber security architecture process and conceptual model

The SSM work based on conceptual model from elements of stakeholder organization. According to Hoverstadt (2010), the conceptual model for viable organization is based on a set of axioms, principles, and laws that dictate the dynamic structure of an organization or organism. Its primary focus is on the adaptive connectivity of the organization's parts, enabling it to survive and thrive in a changing environment. The model serves as a benchmark for comparing actual organizations, identifying weaknesses, mismatches, or missing elements, and diagnosing problems. It also serves as a framework for organization design to solve problems and create new organizational enhancement.

In the case of SSM process, according to Checkland and Poulter (2010), purposeful activity models are not full descriptions of the real world, but rather intellectual "devices" that allow us to explore the real situation by asking relevant questions. By focusing on the differences between the model and situation, we can structure a discussion and debate about the real-world situation, different worldviews, and seek possible ways of changing the problematical situation for the better. In that sense, two criteria of findings are important: it is desirable given the outcomes of using the models to question the real situation, and it must be culturally feasible.

Adequate inquiry can be done by using relevant questions from holistic views of organizational cyber security.

Figure 5 illustrates the holistic architecture process that is needed to develop the comprehensive cyber security architecture of port and harbor security at the system level. For the stakeholder organizations, it includes four continuous investigation steps. These are an organization's current situation description (starting point), cyber threat intelligence phase, risk management process, and measures to be carried out based on previous steps. All this is surrounded by a system research and analysis approach, with the capability to understand a complex cyber environment, to continuously investigate cyber situation awareness, and to recognize the value of business continuity.

6.1. Starting point

Figure 5 depicts an efficient cyber security architecture process. It requires good and real-time situation awareness of all ICT and ICS/OT assets and tight collaboration between an organization's leadership and management and internal communication at the

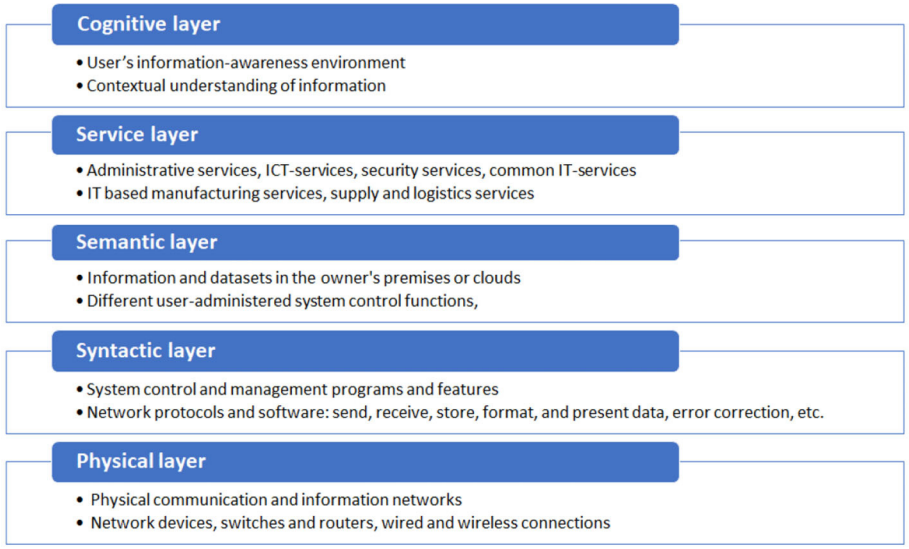

FIGURE 3
The five-layer structure for the cyber world.

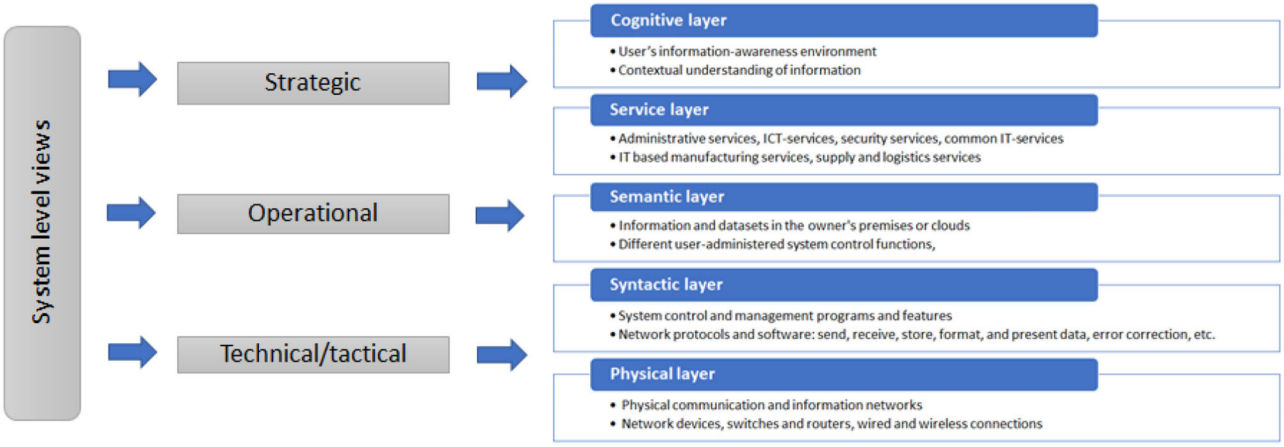

FIGURE 4
System-level view of organizational cyber security.

first phase of development work. The responsibilities could be as follows, as taken from Pöyhönen et al. (2021):

- The strategic choices of organization relate very much to the reputation of an organization. The leadership management must make concrete strategic choices and support and guide the performance of the chosen tasks through the whole organization. An important task of the management is to take care of the adequate resourcing for the cyber security operations and the chosen operations must be communicated extensively with the organization's personnel and other interest groups. At the starting point of an organization, it is important to have a cyber security assessment model for the needs of the uppermost management and for development investigation purposes. Using the model, an organization may evaluate its cyber security level and management efficiency and can become aware of the organization's strengths, weaknesses, opportunities, and threats for contingency planning. The cyber security operations require strategic level decisions from the organization's uppermost management (168).
- The organization's operational level cyber security operations are used to advance the strategic goals. The comprehensive operations require a comprehensive cyber security management. Its starting point must be the target's risk assessment, and the operation analyses carried out based on it. The operational level's concrete hands-on operations must be targeted at the confirmation of information security solutions and the composition of the organization's continuity and disaster recovery plans. The goal must be continuous

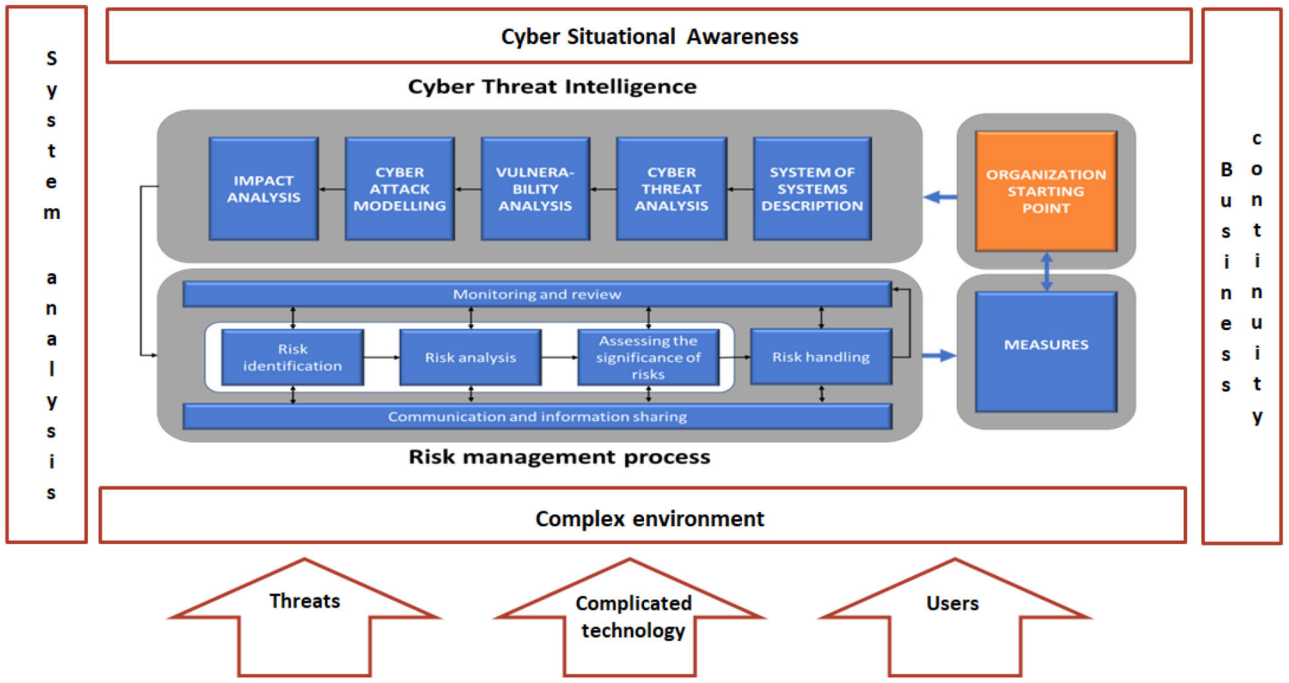

FIGURE 5
The holistic cyber security architecture process.

monitoring of the operational processes' usability, and the decision-making support in case of incidents that require analyzing and decisions (168, 169).

- At the tactical/technical level, the organization can consider real-time forming of the starting point of ICT systems and assets which is in accordance with the Information Technology Infrastructure Library (ITIL) service model. ICT systems and assets can be described with the tools of the control of the configuration. These tools help to analyze the properties of the ICT assets and to clarify the services which function in the ICT systems. The real-time situation information of the user experience of information processing systems and information reserves, which is in accordance with the ITIL service model, helps to form current situation awareness the organization's assets. Perhaps the most significant challenges of an organization's cyber security tasks deal with the observation of the structure and configuration from ICS/OT assets. In that sense, at the starting point, situation awareness creation should be acknowledged, and the organization needs to use industrial automation experts for that work (171).

6.2. Cyber threat intelligence

The system of systems description is related to the concept of national critical infrastructure with three layers of construction: electric network, data transmission, and, above these, services. All three layers are relevant in the case of port processes. In system-of-systems thinking, their digital structure and operational role should be identified as part of a port entity and part of reliable functioning in and between these layers. This also facilitates the identification of cyber dependencies within the layers so that the cyber threat intelligence can be carried out with the most efficient and practical measures (Pöyhönen and Lehto, 2017; Pöyhönen, 2022).

Understanding the motivation aspect of a potential attacker enables the risk of a cyberattack to be predicted in the case being investigated (Casey, 2015). Many cyberattacks are associated with social, political, economic, and cultural backgrounds. It is crucial for the defender to identify comprehensively different kinds of circumstances that might trigger an attacker archetype. Understanding the motivations and capabilities of different archetypes limits the number of scenarios and thus makes evaluation feasible for the defender.

A cyber threat intelligence model captures information about potential cyber threats against a system, a stakeholder, a system of systems, 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 cyber security requires a wide scope of analysis of a system of systems (or sub-system) against a set of threat events. It can be often impractical and, in that sense, the analysis of a system of systems 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 and McCollum, 2018).

The beginning of a broad cyber threat intelligence process should include cyber threat and vulnerability analyses phases. Then comes cyberattack modeling and, at the end of the process, there is

an impact analysis based on the information from previous phases. For this work, all available information is needed to have the most solid awareness of the cyber world. This includes information from the following sources:

- MITRE ATT&CK framework.
- Open source intelligence.
- Organizations' own cyber security network.
- National cyber security authorities.

Many cyber security companies have widely adopted MITRE's ATT&CK information source for the purposes of investigating cyber security incidents (FireEye, 2020). It is a framework and a database that provides information on adversary groups and their software, techniques, and tactics. The open source intelligence task covers all information sources, such as threat reports, webinars, blogs, and so on. An organization's cyber security information is in many cases built up in centralized monitoring rooms (security operations centers, SOC), the technical solutions of which can be under the organization's own control, or the service can be outsourced to the information security operator or based on other specific trust-based networks. National cyber security authorities monitor the operational reliability and security of communications networks and services and provide vulnerability database information (VDI).

6.3. Risk management process

The risk management process work should cover all three levels mentioned above in the five-layer cyber structure as well as in all of an organization's decision levels (Pöyhönen and Lehto, 2017; Pöyhönen, 2022). The risk assessment of each layer separately cannot address emerging threats associated with the interconnection of layers. Therefore, the risk process must consider a multi-dimensional model of target operations, such that all layers and elements of operations must be included. This multi-dimensional risk assessment process, according to our research, has been based on the following approach. The strategic level includes the situation of non-technical terminology. This means, for example, the discussion of the attacker's motivations by studying different types of adversaries. We have used six motivation scenarios: vandalism, cybercrime, espionage, terrorism, sabotage, and warfare operations (Kovanen et al., 2021). At the operational level, we have emphasized having a description of the situation with business continuity. This includes, for example, information on the attacker's capabilities to attack against business networks and systems. At the technical/tactical level (users and ICT/ICS/OT assets), there must be more technical information on the threat actor's tools, tactics, techniques, and procedures.

In risk assessment work, we would like to recommend the use of the Delphi method principle for conducting a holistic and relevant threat analysis and risk-level estimations for the system-of-systems entity. The members that could be involved in this analysis process have to be senior experts or well-educated researchers with appropriate research methods. According to Garson (2013), "The Delphi method is part of quantitative research to achieve an optimally reliable expert consensus." Garson states it could have three objectives:

1. Forecasting future events.
2. Achieving policy consensus on goals and objectives within organizations or groups.
3. Identifying diversity in and obtaining feedback from stakeholders in some policy outcome.

The paper "Dynamic Security Risk Management Using Bayesian Attack Graphs" (Poolsappasit et al., 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 ICT system asset from cyberattacks (Wang and Liu, 2014): "Attack trees (AT) technique plays an important role to investigate the threat analysis problem to known cyberattacks for risk assessment." An attack graph is based on a probabilistic metric model and can be used to quantify the cyber security issues of a system of systems environment. In the risk management process, we have used the Bayesian attack graph model.

In our work, an attack tree graph is used to represent the relationship between threat and defense actions in the Sea4Value research processes. It is more than a metric model way of thinking because there are many layers in the system-of-systems configuration. An exact probability calculation is therefore complicated, and results can be inaccurate. According to our experiences, the attack tree graph is a useful tool for risk assessment. The result of this represents the likelihood of an attack against the likelihood of defense against an attack. The final probability of success of defense measures vs. attacks will be estimated and the most serious attacks will be recognized and prioritized. This probability evaluation work is proposed to be done by cyber security experts by utilizing all relevant information that is available from the cyber security features of the system-of-systems entity as well as information from stakeholders' capabilities to engage in defense measures. From our point of view, we propose the use of the Delphi method principle to undertake relevant threat analysis and make risk-level estimations of the systems. It is a useful way of thinking about likelihood and probabilities at the system level of a process or an organization (Pöyhönen and Lehto, 2022).

6.4. Measures

The following standards can be used to support the creation of a holistic cyber security architecture framework based on a comprehensive system view of an organization's cyber world. The organization's cyber security measures must be carried out continuously on all levels in order to improve and maintain an organization's security. It should be based on the results of a cyber threat intelligence and risk management process.

The publication Joint Task Force Transformation Initiative (2011) places information security into the broader organizational

context of achieving mission/business success. The objectives are stated as follows:

- Ensure that senior leaders/executives recognize the importance of managing information security risks and establish appropriate governance structures for managing such risk;
- Ensure that the organization's risk management process is being effectively conducted across the three tiers of organization, mission/business processes, and information systems;
- Foster an organizational climate where information security risks are considered within the context of the design of mission/business processes, the definition of an overarching enterprise architecture, and system development life cycle processes; and
- Help individuals with responsibilities for information system implementation or operation better understand how information security risks associated with their systems translate into organization-wide risks that may ultimately affect the mission/business success.

The International Organization for Standardization (ISO) 9000 standard family of quality management systems helps organizations ensure stakeholders needs related to products or services are met. The main goal is customer satisfaction. The fundamentals of quality management systems, including the seven quality management principles (customer focus, leadership, the engagement of staff, a process approach, continuous improvement, evidence-based decision-making, and relationship management) are the basic principles of the family of standards (International Organization for Standardization, 2015).

The ISO 27000 family of standards provides recommendations for information security management systems (integrated elements of an organization to establish policies and objectives and https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en:term:3.54 processes to achieve those objectives), risk treatments, and controls (ISO/IEC 27000, 2018).

Figure 6 presents the integration of the measures in organizational cyber security and the system thinking approach to an organization's five-layer cyber structure (Pöyhönen and Lehto, 2020). This integration, in turn, enables the development of a holistic cyber security architecture framework. The content of the measures is derived from the organization-wide risk management standard NIST 800-39 (Joint Task Force Transformation Initiative, 2011) and perspectives from the ISO 9000 family of standards (seven quality management principles) and the ISO 27000 family of standards.

7. Discussion

The ENISA (2019) "Port Cybersecurity" identifies good practices for cyber security in the maritime sector, which is currently undergoing digital transformation in port operations and processes. In order to meet the emerging challenges, it is recommended to optimize existing processes and introduce new capabilities, such as automation and real-time monitoring of operations.

In practice, digital transformation trends require all parts of critical infrastructure to deal with new solutions with regards to information and communication technology (ICT) as well as industrial control systems (ICS) and operation technologies (OT). Recent cyber security research in the maritime sector, such as the 2019 ENISA report mentioned previously, has identified good practices for cyber security in the maritime sector, taking into account the ongoing digital transformation especially in port operations and processes. In order to meet emerging challenges, existing processes need to be optimized and new capabilities introduced, such as automation and the real-time monitoring of operations. The report highlights the need to have a high-level reference model based on research and information of the port structure.

Its objectives are to list, from a high-level perspective, the main port systems, data flows, and interactions with external systems.

In addition to the ENISA report, a paper by the Institution of Engineering and Technology, IET (2020), called "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 the efficiency of the port operations, the safety of operations, and the health and safety of staff and other people. In addition, the IMO (2017) "Guidelines on Maritime Cyber Risk Management" provide high-level recommendations for maritime cyber risk management as an essential measure to ensure the continuity of operations and processes in the maritime sector.

The aim of this article is to introduce our recent maritime cyber security studies, based on the comprehensive cyber security architecture processes of the maritime environment and, in this way, partially meet the needs of good practices for cyber security in the maritime sector.

8. Conclusion

In order to develop maritime digitalization and autonomy in Finland, the Sea4Value research program has been conducted since 2020. It has covered automated remote fairway pilotage features and smart port research phases. It means that stakeholders' ICT and ICS/OT systems together constitute a complex system of systems entity, characterized by a conglomeration of interconnected networks and operational dependencies. However, there will also be a continuing need for traditional engineering solutions for a long time to come. This development introduces the increased risks of a cyber adversary taking deliberate actions against the systems and processes. This article follows our Sea4Value research papers by summarizing the research approach for the investigation of cyber security aspects at the system level in the study cases. Using mainly previous research outcomes of smart port cases, a research framework has been established for examining the comprehensive cyber security architecture process in the maritime environment.

The framework helps to continue the process of organizations' cyber security work. It highlights the necessity to understand an organization's capabilities and assets at the starting point. Once

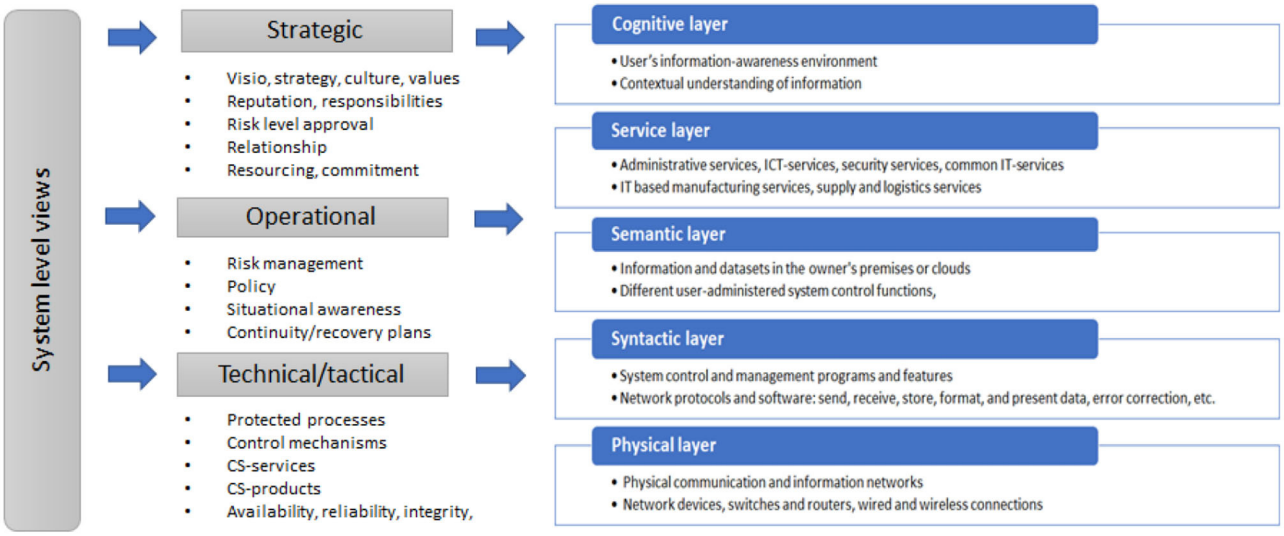

FIGURE 6
Measures for cyber security architecture framework.

this understanding is established, the cyber threat intelligence analysis and risk assessment process can be conducted in a holistic way. This work can be based on the evaluation of attack probabilities against the probabilities to defend against adversarial actions. In this evaluation, the Bayesian attack graph model and principles have been used together with cyber security actions such as identification, protection, detection, response, and recovery. Protecting the stakeholders' processes and systems against cyber threats implies measures taken based on the framework and thus they ensure confidentiality, integrity, and the availability of primarily digital information in the operating processes being examined. The measures should be highly significant for the overall availability of the systems that support the stakeholders' processes in the cyber environment. Operational availability plays a key role in achieving operational continuity and promoting the reliability of activities.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

All authors contributed to the research, conceptualization, writing, methodology, and read and agreed to the published version of the manuscript. This article is based on the Sea4Value research papers presented at different conferences as summaries of the research results.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Alcaidea, J. I., and 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. *Transp. Res. Proc.* 45, 547–554. doi: 10.1016/j.trpro.2020.03.058

Beaumont, P. (2018). "Cybersecurity risks and automated maritime container terminals in the age of 4IR [Fourth Industrial Revolution]," *Handbook of Research on Information and Cyber Security in the Fourth Industrial Revolution*, eds Z. Fields (Hershey, PA: IGI Global), 497–516. doi: 10.4018/978-1-5225-4763-1.ch017

Bodeu, D. J., and McCollum, C. D. (2018). *System-of-Systems Threat Model.* Bedford, MA: The Homeland Security Systems Engineering and Development Institute (HSSEDI) MITRE.

Casey, T. (2015). *Understanding Cyber Threat Motivations to Improve Defense*. Intel White Paper. Available online at: https://simplecore.intel.com/itpeernetwork/wp-content/uploads/sites/38/2016/10/wp-understanding-cyberthreat-motivations-to-improve-defense.pdf (Retrieved February, 2023).

Checkland, P. (1981). *Systems Thinking, Systems Practice*. Chichester: Wiley.

Checkland, P., and Poulter, J. (2010). "Soft systems methodology," in *Systems Approaches to Managing Change: A Practical Guide*, eds M. Reynolds, and S. Holwell (New York, NY: Springer), 191–242. e-ISBN 978-1-84882-809-4. doi: 10.1007/978-1-84882-809-4_5

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. *J. Ind. Inf. Integr.* 20, 100173. doi: 10.1016/j.jii.2020.100173

DIMECC Oy (2020a). *SEA FOR VALUE (S4V)*. 12.2.2020. Available online at: https://www.dimecc.com/dimecc-services/s4v/ (Retrieved February, 2023).

DIMECC Oy (2020b). *Sea4Value - Smart Terminals*. FINAL REPORT 1/2023. Available online at: https://www.dimecc.com/wp-content/uploads/2023/09/DIMECC-123_Smarter_lowr.pdf (Retrieved September, 2023).

ENISA (2017). *Threat Landscape Report 2016, 15 Top Cyber-Threats and Trends*. Available online at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016 (Retrieved February, 2023).

ENISA (2019). *PORT CYBERSECURITY. Good Practices for Cybersecurity in the Maritime Sector*. Available online at: https://www.enisa.europa.eu/publications/portcybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector (Retrieved February, 2023).

FireEye (2020). *"M-Trends 2020". FireEye Mandiant Services, Special Report*. Available online at: https://services.google.com/fh/files/misc/m-trends-report-2020-en.pdf Retrieved (Retrieved February, 2023).

Garson, G. D. (2013). *The Delphi Method in Quantitative Research*. Asheboro, NC: Statistical Associates Publishers.

Hoverstadt, P. (2010). "The viable system model," in *Systems Approaches to Managing Change: A Practical Guide*, eds M. Reynolds, and S. Holwell (New York, NY: Springer), 87–133. e-ISBN 978-1-84882809-4. doi: 10.1007/978-1-84882-809-4_3

IET (2020). *Good Practice Guide. Cyber Security for Ports and Port Systems*. London: The Institution of Engineering and Technology.

IMO (2017). *Guidelines on Maritime Cyber Risk Management*. MSC-FAL.1/Circ.3. London: International Maritime Organization.

International Organization for Standardization (2015). *Quality Management Principles*. Available online at: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100080.pdf (Retrieved February, 2023).

ISO/IEC 27000 (2018). *International Organization for Standardization. Information Technology. Security Techniques. Information Security Management Systems. Overview and vocabulary*. Available online at: https://www.iso.org/standard/73906.html (Retrieved February, 2023).

Jacobs, P. C., von Solms, S. H., and Grobler, M. M. (2016). "Towards a framework for the development of business cybersecurity capabilities," in *International Conference on Business and Cyber Security (ICBCS)*, Vol. 7 (London: The Business and Management Review), 51–61.

Joint Task Force Transformation Initiative (2011). *NIST Special Publication 800-39: Managing Information Security Risk - Organization, Mission, and Information System View*. Gaithersburg: National Institute of Standards and Technology.

Kovanen, T., Pöyhönen, J., and Lehto, M. (2021). "Cyber threat analysis in the remote pilotage system," in *Proceeding of the 20th European Conference on Cyber Warfare and Security ECCWS 2021*. Published by Academic Conferences International Limited Reading, UK (University of Chester UK), 221–229.

Lehto, M., and Neittaanmäki, P. (2018). *The Modern Strategies in the Cyber Warfare. Cyber Security: Cyber Power and Technology*. Berlin: Springer. doi: 10.1007/978-3-319-75307-2

Libicki, M. C. (2007). *Conquest in Cyberspace – National Security and Information Warfare*. New York, NY: Cambridge University Press. doi: 10.7249/CB407

Poolsappasit, N., Dewri, R., and Ray, I. (2012). Dynamic security risk management using bayesian attack graphs. *IEEE Trans. Dependable Secure Comput.* 9, 61–74. doi: 10.1109/TDSC.2011.34

Pöyhönen, J. (2022). "Cyber security of an electric power system in critical infrastructure. cyber security, critical infrastructure protection," in *Computational Methods in Applied Sciences*, Volume 56, eds M. Lehto, and P. Neittaanmäki (New York, NY: Springer), 217–254. ISSN 1871-3033. ISBN 978-3-030-91292-5. ISBN 978-3-030-91293-2 (eBook). doi: 10.1007/978-3-030-91293-2_9

Pöyhönen, J., and Lehto, M. (2017). "Cyber security creation as part of the management of an energy company," in *Proceedings of the 16th European Conference on Cyber Warfare and Security ECCWS2017, 29–30 June 2017, Dublin, Ireland* (Reading: Academic Conferences and Publishing International Limited), 332–340.

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

Pöyhönen, J., and Lehto, M. (2022). "Assessment of cyber security risks - maritime automated piloting process," in *Proceedings of the 17th International Conference on Information Warfare and Security, ICCWS 2022*. Published by Academic Conferences International Limited (Reading; New York, NY: State University of New York at Albany), 262−271. doi: 10.34190/iccws.17.1.18

Pöyhönen, J., Rajamäki, J., Nuojua, V., and Lehto, M. (2021). "Cyber situational awareness in critical infrastructure organizations," in *Digital Transformation, Cyber Security and Resilience of Modern Societies* (New York, NY: Springer), 161–178. Studies in Big Data, 84. doi: 10.1007/978-3-030-65722-2_10

Simola, J., and Pöyhönen, J. (2022). "Emerging cyber risk challenges in maritime transportation," in *Proceedings of the 17th International Conference on Information Warfare and Security ICCWS2022, 17–18. March 2022, Albany, New York, USA* (Reading: Academic Conferences and Publishing International Limited), 306–314. doi: 10.34190/iccws.17.1.46

Thai, V. V., and Grewal, D. (2007). The maritime security management system: perceptions of the international shipping community. *Mar. Econ. Logist.* 9, 119–137. doi: 10.1057/palgrave.mel.9100175

Wang, P., and Liu, J. C. (2014). Threat analysis of cyber-attacks with attack tree+. *J. Inform. Hiding Multimed. Sign. Process.* 5, 778–788.