A Conceptual Model of Port Cybersecurity and Threats: Knowledge and Understanding

Hakan AKYILDIZ*
*Prof. Dr., Istanbul Technical University | akyildiz@itu.edu.tr

ABSTRACT

The use of risk analysis methods as decision support tools is getting more and more acceptance to analyze, recover or mitigate potential risks in engineering applications. Through the analysis to obtain more reliable and realistic solutions, level of understanding, quality of knowledge, uncertainty level of cybersecurity and threats, sensitivity levels of model parameters, are integrated to model parameters to analyze port cybersecurity and threats. In the port activities to increase their competitiveness, the digitalization of port operators with the integrated cyber technology becomes the major vulnerability for cybersecurity and threats. In order to investigate the cybersecurity measures, a risk perspective for the integrated risk management and decision making process conceptualized in terms of human, infrastructure, and procedure factors. Additionally, the relationships between port cybersecurity hygiene and cyber threats in terms of hacktivism, cyber criminality, cyber espionage, cyber terrorism, and cyber war are investigated. The results indicated that ports tended to encounter hacktivism when their human, infrastructure, and procedure factors were vulnerable. The weakness of the human factor could also lead to cyber terrorism, while the deficiency of the infrastructure factor could lead to cyber criminality. Moreover, ports were likely to be harmed by cyber espionage if their procedure factor was poorly implemented.

Keywords: Port cybersecurity and Threats, Cyber technology, Port digitalization, integrated risk assessment, uncertainty analysis

1. Introduction

The total amount of goods transported is continuously increasing as the world trade expands. Systems that offer convenience, speed, safety and low cost also evolve increasingly. Following the increasing demand for tonnage, the maritime industry moved to the development of bigger ships and the need for the creation of “economies of scale” resulted in the largest cargo ship sizes.

In the maritime industry, International Maritime Organization (IMO) implements the principles of risk management to assess risks and evaluate costs and benefits, support to decision making process. The use of risk analysis methods as decision support tools aims at enhancing maritime safety including protection of life, health, the marine environment and property. They also achieve a balance between the various technical and operational issues, including the human element, maritime safety, protection of the marine environment and costs.

To facilitate a more flexible and more representation of the real world decision making problems, it may be beneficial to adopt a more systematic risk perspective. To improve safety at sea and ports, risk factors need to be modelled and safety based decisions require to be made in a consistent and efficient way. Additionally, risk modeling and decision-making tools need to be developed and applied in a practical environment. As a result, integration of the techniques leads to acquire more reliable and realistic solutions in maritime domain.

The maritime industry is also becoming increasingly digitalized to modify their business model for customers (Shepherd, 2004). Most maritime operators have adopted digital technologies to comply with legal requirements and generate a competitive advantage (Barnes & Oloruntoba, 2005; Chao & Lin, 2009) by using digital navigation networks (ECDIS, GNSS, AIS, VDR and radar (International Chamber of Shipping, ICS, 2018)). They have supported access control to ensure physical security, in terms of administration of the ship, crew and communication (Tsai, 2006). They have also supported the loading, management and control of cargo (Yeo et al, 2013). At the same time, ports digitalize their operation and have the inevitable duty to integrate cyber technologies into port activities, such as process design (Lee & Whang, 2005), cargo handling and navigation, environment and pollution prevention, and risk management, and port safety and security taking

into consideration the international and national practices of the SOLAS Conventions (IMO, 2019a, 2019b, 2019c), the MARPOL Conventions and the ISPS Codes (Homeland Security, 2018; Pintong, 2010).
In the port efficiency and competitiveness, digitalization is of great importance considering automated vehicles, stacking cranes, gate automation, optical characters recognition, license plate recognition, automated teller machines, e-tracking services, and wireless devices (Chao & Lin, 2009). On the other hand, the vulnerabilities of these cyber technologies and digital systems can lead to cyber threats costing huge amounts of money for the business outage and system recovery. Unfortunately, a review of the literature shows the deficiency of knowledge and understanding regarding cyber threat and cybersecurity in preventing ports and shipping firms from malicious cyber actions. Therefore, port managers and policy makers are to understand how port cybersecurity is threatened by different cyber threats.
This study aimed to narrow the literature gap by creating a conceptual model demonstrating the integral elements of port cybersecurity hygiene and its relationship with five groups of cyber threats for cleaner and safer port operations. Additionally, the paper intends to investigate how the uncertainty parameters can be used for port cybersecurity to learn the effects on conceptual model parameters. The rest of this paper is organized as follows. Section 2 defines Knowledge and Understanding. In Section 3, the author reviews the literature on port cyber threat and cybersecurity hygiene to provide a theoretical background and considered concepts for developing the conceptual research model which was used as the reference for developing research hypotheses. This is followed by the discussions and recommendations in Section 5. Section 6 is the last part containing the conclusions.

2. Knowledge and understanding

The paper focuses on to create and stimulate main aspects of uncertainty in port cybersecurity and threats. For this purpose, level of understanding, quality of knowledge, uncertainty level of cybersecurity and sensitivity levels of model parameters are used as uncertainty parameters the current study. Some related information is given the following sections.

2.1. Knowledge

Knowledge and understanding are fundamentally different. Knowledge is widely identified with propositional knowledge and is objective, so that the more you work in a field the more you know in it. To acquire knowledge about events, first the events need to exist in favour of expert knowledge (Baumberger, 2014). Therefore, the growth of knowledge is a cognitive advancement that satisfies the additional condition. On the other hand, the main goal of a cognitive process is not to acquire knowledge but to advance understanding (Montewka et al., 2014). "Real" understanding is dynamic and has nothing to do with knowledge.
Identification of risk factors is highly significant, together with the evaluation of their impact on cognitive process for the quantifying of risk and allows corrections and comparison of the results. There can be several relations between the risk assessment and the knowledge. One is how to improve the risk management process by using the knowledge. The other is how to identify and manage risks in the growth of knowledge, in order to obtain the best results in terms of the risk reduction. The growth of knowledge is the collection of people interactions, modern technology with a suitable sharing platform and structure of the risk management. It is also related to the class of information systems as creation of new knowledge, storage and retrieval, distribution and application. Therefore, it is of great importance for managing knowledge risks in terms of establishing a learning climate, mitigating knowledge loss, creating channels for knowledge flow and monitoring knowledge risks.
Risk factors may differ depending on many external and internal circumstances and specific characteristics. The selection of these factors should be done by monitoring the process and drawing on other experiences. The assessment of risk factors for achieving the growth of knowledge is crucial for making a good choice. The importance of knowledge could be aimed at analyzing various types of knowledge in order to check and correct the validation of the achieved results.

2.2. Understanding

The main goal of the growth of knowledge is to advance understanding. Besides knowing the important and relevant truths that belong to the comprehensive, "real" understanding is dynamic and has nothing to do with knowledge. It can be indicated that understanding is more ambitious. Therefore, argument and new questions should be carried out within the framework of the account that does not yet provide conclusive answers (see, Baumberger, 2011 and 2014, Elgin, 2006).

Knowledge and understanding are fundamentally different with different specific difficulties. Since understanding can be more or less accurate, it must answer to the facts by accommodating the evidence on the entire system. In complex systems, there are numerous causes which interact in complicated manners. Therefore, it is difficult to address all of the causes. Additionally, understanding admits degrees, meaning that with each step in the sequence we understand an analyzed phenomenon better than we did before. As a result, it can be concluded that understanding is not to be factive. As the risk is about future events and we do not possess facts about the future, our knowledge implies assumptions, which come from our understanding. This means that risk perspective inherently contains understanding in larger proportion than knowledge.

2.3. Scoring system

A scoring system is presented for the qualitative uncertainty assessment. The system consists of the level of knowledge, the quality of understanding and the joint effect on the uncertainty of a risk model. The main idea of the scoring system is to assign a qualitative description for the quality of knowledge and the level of understanding to each and every element of the model. Each element of the model and relations between the elements are evaluated with respect to the evidence, which is used to describe the element as follows:

• Considering the knowledge; data, models and theories are the factual elements that allow a decision-maker to formulate statements about the risk model.

• Considering the understanding; assumptions, judgments and the ability to assess the level of knowledge about the element are not necessarily the factual elements.

The presented classifiers are crude and can be case-specific and subject to judgment of the analyst.

The experts made judgments by expressing their opinions based on their experience, knowledge and expertise. The following category classification is applied for the qualitative uncertainty scoring in order to express the understanding and knowledge parameters of uncertainty system as follows:

Quality of knowledge:

High

1) Data is reliable and/or; 2) Risk model is accurate and/or ; 3) Theory is broadly accepted

Medium

Conditions between those characterizing quality of knowledge as High and Low

Low

1) Data is unreliable; 2) Risk model is a crude estimate; 3) Theory is contested

Level of understanding:

High

1) Assumption is broadly accepted among peers and/or; 2) Judgment is broadly accepted among peers and/or; 3) Assessor can well justify the ranking of quality of knowledge

Medium

Conditions between those characterizing quality of knowledge as High and Low.

Low

1) Assumption is contested among peers; 2) Judgment is contested among peers; 3) Assessor cannot properly justify the ranking of quality of knowledge

3. Port cybersecurity and Cyberthreats

3.1. Cyberthreats

Research papers regarding port security and threat have been published in the transportation sector. The infrastructure, port operators and sea carriers were the target of the terrorist and cybercrime and the safety of container cargo and security measure of seaport became the attractive issue in the global arena adopting automated technology (e.g. hijacking, migrant smuggling, nuclear terrorism, dangerous weapons, cargo thieves, drug smugglers etc.) (Choong-Hee, Soon-Tai, & Sang-Joon, 2019; Roach, 2004; McLay & Dreiding, 2012; Michel et al., 2014; McNicholas, 2016).

According to the literature review, the ransomware was the most frequently used cyber threat for disrupting the computer networks and servers, such as the attacks in Port of Barcelona (Aharoni, 2018) or COSCO Shipping Lines (Homeland Security, 2018). As an example for data destruction and cyber extortion, Maersk lines and its

terminals were attacked by malware in 2017 costing the firm lots of money and causing disrupted operations for many weeks (Ahokas et al., 2017; Fosen, 2019).

Shipping and port operators might be targeted by five categories of cyber threats, namely, ***hacktivism, cybercrime, cyber espionage, cyber terrorism, and cyber war*** (Ahokas et al. 2017)**.** The hacktivism means the operation in cyberspace using different hacking techniques to invade into web pages and on computers, and create pressure on a certain object. The aim for conducting hacktivism varies from gaining attention with his/her actions to disrupting business through the vulnerable gaps in the cyberspace. The cybercrime refers to criminal activities that are deemed injurious to the public welfare and are legally prohibited. The motivation to conduct cyber criminality is normally to exploit human or security vulnerabilities in order to steal passwords, data, or money directly, such as using bogus emails to ask for security information and personal details (National Crime Agency, 2017; Christou, 2016). The cyber espionage is the illegal access to secret and delicate information (e.g. company strategy, private information, or intellectual capital). However, the cyber espionage aims to gain competitive advantages rather than create pressure and business disruption (Ahokas et al., 2017). Thus, the consequences might be the loss of intellectual property, business profits and efficiency, and customer information, additional costs thanks to the interrupted business plan, and damage to company reputation (Platt, 2011). The cyber terrorism is a politically-motivated attack by cyberterrorist (e.g. international groups or secret agents) using various tools (e.g. computer viruses, computer worms, phishing, and other malicious software) to violate the information, computer systems, computer software, and databases of important organizations or global networks in order to accomplish the political or ideological gain. Thus, the cyber terrorism normally causes serious consequences, such as massive damage to government systems and national security programs, or loss of life or significant bodily harm (Limnéll, Majewski, Salminen, & Samani, 2015). Finally, the cyber war is a part of the modern information war between nations. In general, it is relevant to the military affair aiming to disable the military target by using malicious software, viruses, and other technologies (Lewis, 2002). Apart from the military, the cyber war might be done by the state-sponsored actor (e.g. terrorist groups, companies, political, or ideological extremist groups) to attack the opponent's computer networks (Green, 2015). In cyber war, the computers and satellites might be used to disturb the critical water, power, fuel, communications, and transportation infrastructure that leads to disastrous consequences.

This makes port infrastructure attractive for cyberattacks, especially the leading ports with a high degree of interconnection and lacking adequate cybersecurity (Lewis, 2002; Moerel & Dezeure, 2017; Tonn et al. 2019). This study gathered all cyberthreats exposed by port and other industries and classified them into five categories based on the approach of Ahokas et al. (2017), as presented in Table 1.

Table 1. Characteristics of Cyberthreats

Cyber threat category	Objective	Cyber threat
Hacktivism Moerel and Dezeure (2017), Homeland Security (2018),	To invade web pages and computers to create pressure	Hack by malware
		Hack by ransomware
		Credential theft
		Privacy violation
Cyber criminality Ahokas et al. (2017), Tonn et al. (2019)	To gain financial benefits	Revenge or bullying
	To inflict personally motivated harm	Criminal damage
		Robbery of cargo
		Identity theft Data breach
		Data damage
		Illicit gambling or spreading false information
		Copyright or brand violation
Cyber espionage Ahokas et al. (2017), Homeland Security (2018)	To gain competitive advantage and intellectual property of other business	Illegal access to secret and delicate information such as company strategy, private information or intellectual capital
	To interrupt business operations	Cyber extortion
	To damage company reputation	Information stealing
		Insiders gaining unauthorized access to information systems

		Intruder having direct physical access to systems and the network
		Cross contamination
		Cyber fraud
Cyber terrorism Moerel and Dezeure (2017), Tonn et al. (2019)	To politically attack information, computer systems, computer software and databases	Outage and information system failure
		Website defacement
		Subversion of security control Sabotage
Cyber war Ahokas et al. (2017), Moerel and Dezeure (2017)	To fight against opponent countries by damaging or disabling their rivals' computer networks, especially relevant to military affairs	Sabotage at national level
		Disruptive attacks by state actors

3.2. Port cybersecurity

The port authority has a responsibility to issue the regulations in question between terminal operators and their users (ISPS Code; IMO, 2019a, 2019b, 2019c). Therefore, port cybersecurity is off great importance for ensuring port safety and security by issuing the effective security procedures and communicating them to the shipping line and other relevant operators. The less sufficient the cybersecurity and the policy of the port, they are more vulnerable to protect their digital assets and infrastructure (Moerel & Dezeure, 2017). ISPS Code plays the most important role in port cybersecurity by standardizing the concept for regulating port and vessel cybersecurity implementing all security measures and exercise the Port Facility Security Plan (IMO, 2014, 2019a, 2019b, 2019c; SOLAS conventions, 1974/1988). The regulations focus on the procedure onboard the vessel and in port prior to docking with all requirements for security levels.

On the other hand, some regulations concentrate on the security facility, equipment onboard and on humans working onboard the vessel and in port considering a security alarm system and communicating system via satellite system. The ISPS Code highlights the port cybersecurity hygiene based on the factors of human, infrastructure, and procedure. These factors enable the relevant operators to prevent cyber infrastructure and asset loss from cyber threats (Kapalidis, 2018).

The human factor: Training courses should be provided to improve the knowledge and understanding, thereafter improve IT skill and cybersecurity. This is critical for the success of cybersecurity measures and could reduce the cyber risk. It is required to designate port security officers and top executives for dealing with malicious acts and cyber threat-awareness culture at all organizational levels (Ahokas et al., 2017; Moerel & Dezeure, 2017). In contrast, ports tend to encounter cyber threats when their human factor is vulnerable. Thus, Port operators with a high degree of interconnection and lacking adequate cybersecurity could encounter with ***hacktivism, cyber criminality, cyber espionage, cyber terrorism, and cyber war*** (Christou, 2016; Ahokas et al., 2017; Platt, 2011; Limnéll et al., 2015; Green, 2015; Lewis, 2002).

As a result, it is hypothesized that the lower the human factor, the higher the hacktivism, the cyber criminality, the cyber espionage, the cyber terrorism and the cyber war.

The infrastructure factor: Kapalidis (2018) considered that managers and policy makers should take into account the investment of infrastructure to maintain cybersecurity of the internet-based technologies that have been adopted by most modern companies. In the modern ports activities based on automatic and digital technologies (e.g. automated cargo handling equipment and vehicles, automated cargo container tracking system and traffic control system etc.), they could easily be harmed by cyber threats without security infrastructure (Boyes, Isbell, & Luck, 2016; Boiko et al, 2019; Moerel & Dezeure, 2017; Ahokas et al., 2017). In order to reduce the cyber risk, the investment in security infrastructure, such as firewalls, software encryption, virus detection, and system compartmentalization, is vital. In contrast, the deficiency of port cybersecurity infrastructure could increase the opportunity of hacktivism, cyber criminality, cyber espionage, cyber terrorism, and cyber war in ports.

As a result, it is hypothesized that the lower the infrastructure factor, the higher the hacktivism, the cyber criminality, the cyber espionage, the cyber terrorism and the cyber war.

The procedure factor: It enables the port activities to prevent, reduce or eliminate a cyberthreat. The procedure factor consists of the responsive measures that port managers could implement (e.g documentation, buying objectives, damage or disaster management, system design and operations etc.) (Boiko et al., 2019; Polatidis, Pavlidis, & Mouratidis, 2018; Windelberg, 2016; Tonn et al., 2019). It is well known that the risk management approach is the most preferable tool for port security enhancement. In this approach, port managers may identify all possible risks and thereafter select suitable measures more efficiently. On the other hand, the failure in implementing measures will lead ports to cyber threats because of insufficient knowledge and poorly understanding. This would disable ports to prepare the appropriate measures for mitigating cyber risks of hacktivism, cyber criminality, cyber espionage, cyber terrorism, and cyber war.
As a result, it is hypothesized that the lower the procedure factor, the higher the hacktivism, the cyber criminality, the cyber espionage, the cyber terrorism and the cyber war.

Table 2. Cyber Security Hygiene

Factors	**Objective**	**Attribute**
Human Ahokas et al. (2017), Moerel and Dezeure (2017), Kanalidis (2018), IMO (2019a, 2019b)	Training of workforce	
	Security awareness of workforce	
	Training of executives	
	Security awareness of executives	
	IT security staff and response team	
	Security culture of workers	
Infrastructure Vorakulpipat (2013) Boyes et al. (2016) Ahokas et al. (2017) IMO (2019a, 2019b) Moerel and Dezeure (2017) Kanalidis (2018) Boiko et al. (2019) IMO (2019a, 2019b) Tonn et al. (2019) IMO (2017) IMO (2019a, 2019b) Tonn et al. (2019)	Physical infrastructure and commodity	Office building
		Terminal operating center
		Cargo
	Vehicle and equipment	Vessels and long-haul trucks
		Cargo handling equipment
		Automated cargo handling equipment and vehicles
		Navigational support equipment
		Empty depot tools
		e-Desk tools
		Internet of Things devices (e.g. sensors and camera)
		Other machinery and equipment
	Port operation and control system	Port access control system
		Shore-based system for vessel operation and navigation
		Automated cargo container tracking system
		Internet-use control system
		Handling control system
		Traffic control system
		Building control system
		Warehouse access control system
		Internal working network
		External business collaboration network
		Customs information technology
	Information infrastructure to support port cyber security	Information security
		Application security
		Cyber threat protection
		Internet security
		Network security
Procedure Lee and Whang (2005) Ralston et al. (2007) Boyes et al. (2016)		Risk management
		Port risk governance
		Change management
		Information sharing
		Threat and vulnerability management

Cherdantseva et al. (2016) Kanalidis (2018) Polatidis et al. (2018) Boiko et al. (2019) IMO (2019a, 2019b)		Event and incident response Cyber and program management Resilience measure and system redundancy Damage management ISO 31000:2009 and ISO/IEC 27005:2011

Table 2 summarizes all factors influencing port cybersecurity hygiene, while Fig. 1 demonstrates the research model comprising cyber threats grouped into five latent factors and port cybersecurity hygiene grouped into three latent factors. Fig. 2 defines the structural model of cyber security hygiene and threat of port industry.

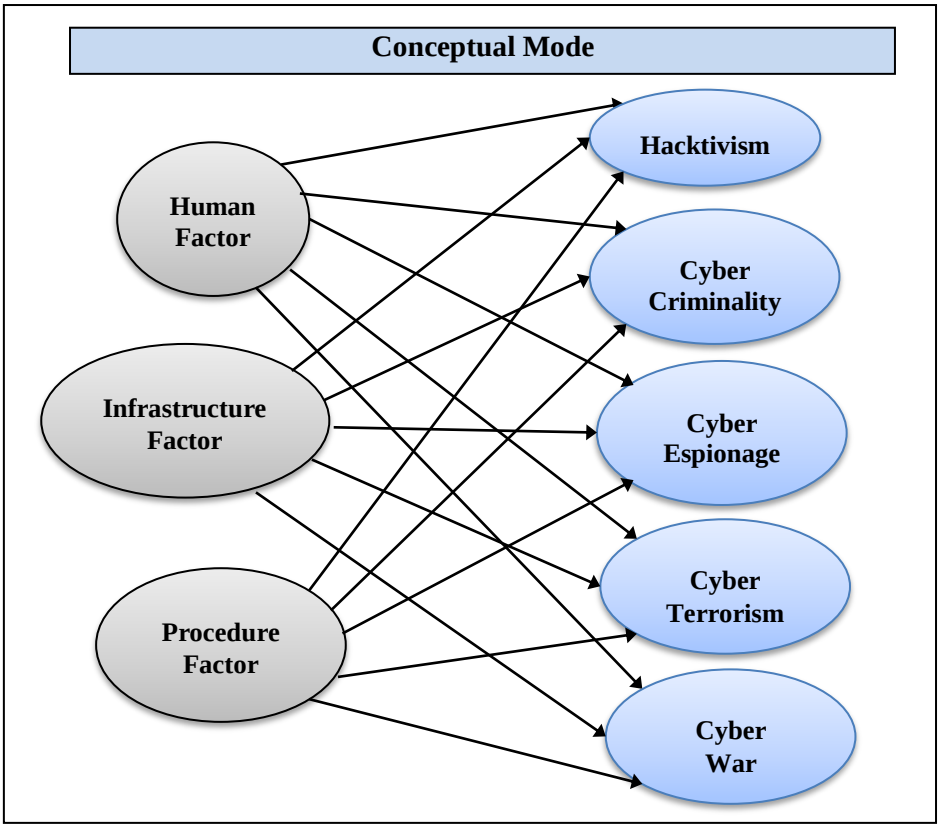

Fig. 1. Conceptual model.

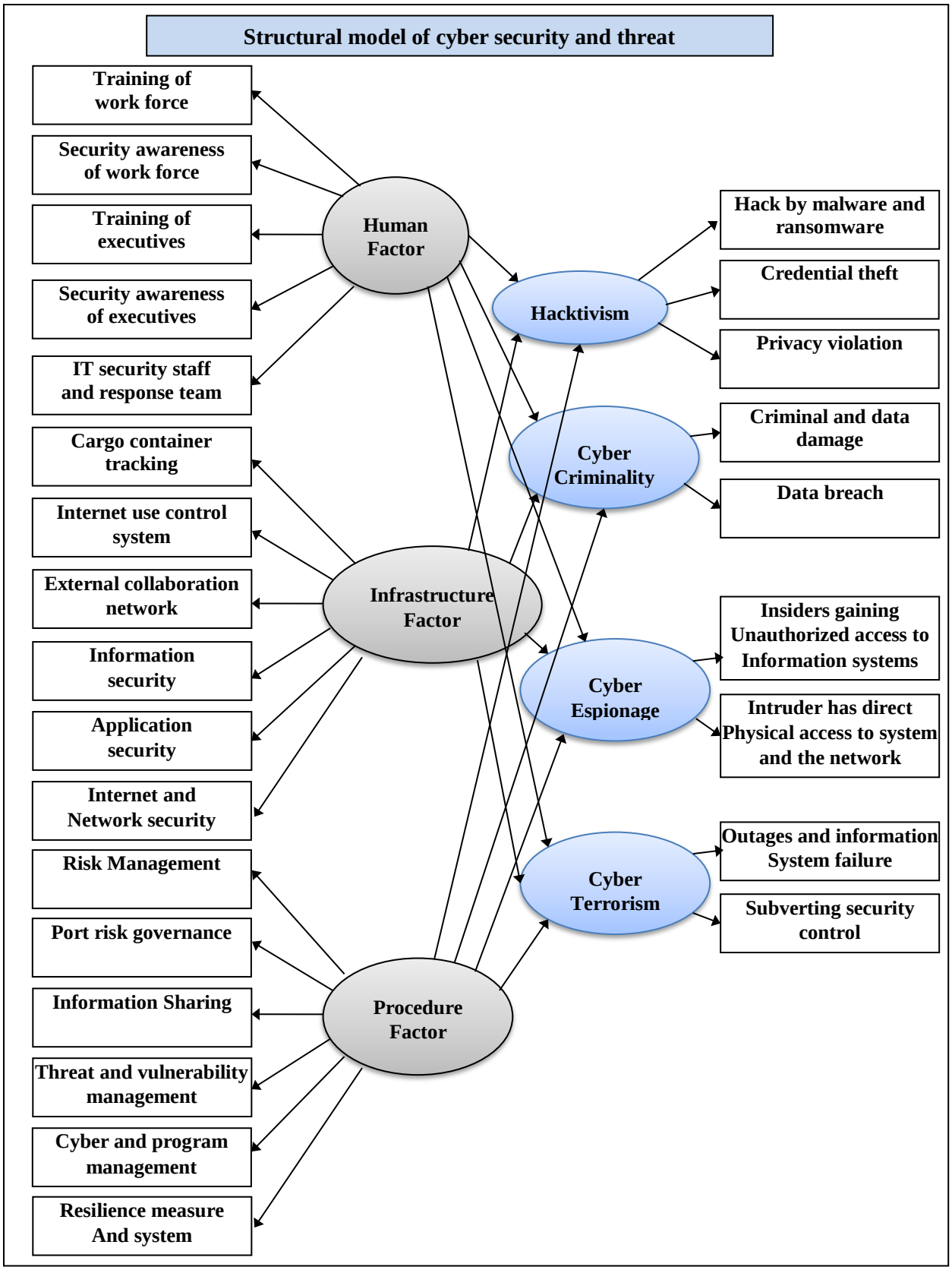

Fig. 2. Structural model of cyber security hygiene and threat of port industry.

4. Discussions and Recommendations

The human, infrastructure and procedure factors constitute port cybersecurity hygiene and they depend on each other. Port managers and policymakers should prepare the cultivated and skillful manpower (the human factor). Therefore, provision of training and education to port workers is required for human factor who will implement the preventive measures (the procedure factor) to secure port digital assets, technology and networks. It is also important to secure port facilities (the infrastructure factor) against cyber threats. A shortfall in the knowledge and understanding to enforce cybersecurity measures would possibly cause failure in developing successful port cybersecurity hygiene. Training should include port managers and supervisors to raise their awareness for the effective cybersecurity measures.

To monitor cyber threats in a port that can gradually establish an active environment, cyber risk assessment and cybersecurity measures are implemented and emphasized at all organizational levels. This helps not only the port to identify possible cyber threats and their impacts on port digital infrastructure and security, but assists in the selection of suitable preventive measures to reduce cyber risk or address the impact of malicious actions.

In the port cybersecurity procedures, the implementation of the cybersecurity systems and policies at ports should be developed by the firms (International Ship and Port Facility Security Code (ISPS) and the International Safety Management Code (ISMC) and IMO, 2017). All team members can understand and implement the procedures as well as monitor and review the results for further improvement (IMO, 2017). It is a key success factor of port cybersecurity that all stakeholders are suggested to be involved in port cybersecurity development and good collaboration should be continuously ensured.

On the other hand, any weakness in the port infrastructure will be critical regarding hacktivism and cyber criminality. Therefore, investment in port infrastructure and facility is also essential for ports. Port managers should use a secured container tracking, traffic control system and monitor to keep important information secure, prevent unauthorized access for the risk of cyber threats. The infrastructure is also important for a port to secure its computer network from intruders (network security), keep software and devices free of threats (application security) and protect the privacy of data, both in storage and in transit (information security) (Tonn et al., 2019). Hacktivism and cyber espionage depends on how the information is shared between port operators and other stakeholders. Therefore, the procedure factors, preventive measures and other security procedures should be considered and implemented. The port manager should control all digital networks and systems by changing default passwords in order to avoid external attackers in the port. Ensuring security in the data exchange process and storage throughout the infrastructure is off great importance in terms of cybersecurity measures. Thus, control of internet use and the communication network by employees, checklists for cyber hazard identification, provision of training, and regular testing to ensure adequate levels of knowledge and skills of port employees should be enforced strictly without compromise.

The effectiveness of cyber risk management is a continuous operation and constantly evaluated through effective feedback mechanisms for all organizational levels including government authorities, business partners, academic and civil society (Pallis, 2017).

It is indicated that the port industry becoming increasingly digitalized in every country tends to be the target of cyber threats (Ahokas et al. (2017). Therefore, government agencies should

(1) invest in national and regional cybersecurity,
(2) develop a holistic strategy and policy,
(3) update the national regulations in order to sustainably reduce the risk of cyber malicious acts in not only the port industry, but also other critical industries associated with chemicals, commercial activities, communications, manufacturing, dams, energy financial services, and food and agriculture.

5. Conclusions

In this study, to obtain more reliable and realistic solutions, level of understanding, quality of knowledge, uncertainty level of cybersecurity and threats, sensitivity levels of model parameters, are integrated to model parameters to analyze port cybersecurity and threats. Furthermore, the goals of the framework are to utilize the systematic and transparent risk management by identifying and evaluating aspects of uncertainty on the process of risk model development, uncertainty analysis and selection of risk measures. Therefore, knowledge and understanding are the most important inherent parts of risk description and are of great importance to take preventive measures to recover or mitigate the impacts of the model parameter.

It is indicated that there is the positive relationship between cyber threats and port cybersecurity factors which are subject to different cyber threats depending on its vulnerability in terms of the human, procedure, and infrastructure factors. Ports are an attractive target for the hacktivist, snooper, criminal, and terrorist impacting on not only the port industry but on the entire national economy. This includes accessibility to state-of-the-art technologies and innovative policies that potentially help increase government capability to secure the critical infrastructures.

This study presents a structural model illustrating the association between port cybersecurity hygiene and cyber threats to increase the cybersecurity performance of ports taking into account port operators, shipping lines, and ship agents in maritime transportation generally. Some theoretical findings can be used by port practitioners in the port risk assessment. Additionally, this model can be used as a reference for developing multi-hazard matrices and hazard models.

Most national ports have become integral parts of digitized supply chains, innovation districts, and smart cities projects increasing the variety and risk of cyber threats. Thus, it is required to extend the scope of the study and to consider the impact of external factors from other organizations on port security performance and competitiveness. Developing new risk assessment methods to quantify the risk of each cyber threat is also recommended for making better decisions.

References

[1] Aharoni, E. (2018). Cybercriminals are industrious when hacking industries.. Retrieved from https://blog.cymulate.com/cybercriminals-are-industrious-whenhacking-industries

[2] Ahokas, J., Kiiski, T., Malmsten, J., & Ojala, L. (2017). Cybersecurity in ports: A conceptual approach. Hamburg International Conference of Logistics, 23.

[3] Barnes, P., & Oloruntoba, R. (2005). Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management. Journal of International Management, 11(4), 519–540.

[4] Baumberger, C., 2011. Understanding and its Relation to Knowledge. 34th International Wittgenstein Symposium, 16–18, Kirchberg am Wechsel.

[5] Baumberger, C, 2014. Art and understanding. In defence of aesthetic cognitivism. In: Wagner, C., Greenlee, M., Hammwöhner, R., Körber, B., Wolff, C., editors. Bilder sehen. Perspektiven der Bildwissenschaft. Regensburg: SchnellþSteiner.

[6] Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: Uncertainties, risks and cyber security. Procedia Computer Science, 149, 65–70.

[7] Boyes, H., Isbell, R., & Luck, A. (2016). Code of practice cyber security for ports. London: Institution of Engineering and Technology.

[8] Chao, S.-L., & Lin, P.-S. (2009). Critical factors affecting the adoption of container security service: The shippers' perspective. International Journal of Production Economics, 122(1), 67–77.

[9] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. Computers & Security, 56, 1–27.

[10] Choong-Hee, H., Soon-Tai, P., & Sang-Joon, L. (2019). The Enhanced Security Control model for critical infrastructures with the blocking prioritization process to cyber threats in power system. International Journal of Critical Infrastructure Protection, 26, 103–112.

[11] Christou, G. (2016). Cybersecurity in the European Union. London: Palgrave Macmillan.

[12] Elgin, C., 2006. Understanding and the facts. Philosophical Studies, 132(1), 33–42.

[13] Fosen, J. (2019). Cyber security awareness in the maritime industry.. Retrieved from http://www.gard.no/Content/25634225/Cyber%20Security resentation%20(ID%201418279).pdf

[14] Green, J. A. (2015). Cyber warfare: A multidisciplinary analysis. Abington: Routledge.

[15] Homeland Security. (2018). Examining physical security and cybersecurity at our nation's ports. Washington: U.S. Government Publishing Office.

[16] International Chamber of Shipping (2018). The Guidelines on Cyber Security Onboard Ships.. Retrieved from https://www.ics-shipping.org/docs/default-source/ resources/safety-security-and-operations/guidelines-on-cyber-securityonboard-ships.pdf?sfvrsn=20

[17] International Maritime Organization (IMO). (2014). Maritime (ISPS Code) Regulations 2014. Retrieved from http://extwprlegs1.fao.org/docs/pdf/fij152587.pdf

[18] International Maritime Organization (IMO). (2014). Guidelines on maritime cyber risk management. Retrieved from http://www.imo.org/en/OurWork/ Security/Guide to Maritime Security/Documents/MSC-FAL.1-Circ.3%20%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20 (Secretariat).pdf

[19] IMO (2019a). Air pollution, energy efficiency and greenhouse gas emissions.. Retrieved from http://www.imo.org/en/OurWork/Environment/PollutionPrevention/AirPollution/Pages/Default.aspx

[20] IMO (2019b). AIS transponders. Retrieved from http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx

[21] IMO (2019c). SOLAS XI-2 and the ISPS code.. Retrieved from The International Ship and Port Facility (ISPS) Code: http://www.imo.org/en/OurWork/Security/Guide to Maritime Security/ Pages/SOLAS-XI-2%20ISPS%20Code.aspx

[22] Kapalidis, C. (2018, November 27). Port Cyber Security: Maersk, Cosco, Barcelona, San Diego. Who is next? Retrieved from http://www.boussiasconferences.gr/files/ boussias conferences content/presentations/portdevelopment/2018/chronis kapalidis portdevelopment 18.pdf

[23] Lee, H. L., & Whang, S. (2005). Higher supply chain security with lower cost: Lessons from total quality management. International Journal of Production Economics, 96(3), 289–300.

[24] Lewis, J. A. (2002, November 1). Assessing the risks of cyber terrorism, cyber war and other cyber threats.. Retrieved from https://www.csis.org/analysis/assessingrisks-cyber-terrorism-cyber-war-and-other-cyber-threats

[25] Limnéll, J., Majewski, K., Salminen, M., & Samani, R. (2015). Cyber security for decision makers. Aalborg: Docendo.

[26] McLay, L. A., & Dreiding, R. (2012). Multilevel, threshold-based policies for cargo container security screening systems. European Journal of Operational Research, 220(2), 522–529.

[27] McNicholas, M. A. (2016). Vulnerabilities in the cargo supply chain. Maritime Security, 137–168.

[28] Michel, S., Mendes, M., Ruiter, J. C., Koomen, G. C., & Schwaninger, A. (2014). Increasing X-ray image interpretation competency of cargo security screeners. International Journal of Industrial Ergonomics, (44), 551–560.

[29] Moerel, L., & Dezeure, F. (2017). Cyber security in port: Business as usual?
[30] Retrieved from http://www.vndelta.eu/files/3215/1125/0649/Cyber Security in Ports Whitepaper VND vonference november 2017.pdf

[31] Montewka, J., Ehlers, S., Goerlandt, F., Hinz, T., Tabri, K., Kujala, P., 2014. A framework for risk assessment for maritime transportation systems – A case study for open sea collisions involving RoPax vessels. Reliability Engineering and System Safety, 124, 142–57.

[32] National Crime Agency. (2017). Cyber crime.. Retrieved from https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime

[33] Pallis, P. L. (2017). Port risk management in container terminals. Transportation Research Procedia, 25, 4411–4421.

[34] Pintong, W. (2010). GMS trade facilitation enhancement thailands contributions..
Retrieved from https://www.nesdb.go.th/ewt dl link.php?nid=3358

[35] Platt, V. (2011). Still the fire-proof house? An analysis of Canada's cyber security strategy. International Journal: Canada's Journal of Global Policy Analysis, 67(1), 155–167.

[36] Polatidis, N., Pavlidis, M., & Mouratidis, H. (2018). Cyber-attack path discovery in a dynamic supply chain maritime risk management system. Computer Standards & Interfaces, 56, 74–82.

[37] Ralston, P., Graham, J. H., & Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. ISA Transactions, 46(4), 583–594.

[38] Shepherd, J. (2004). What is the digital era? Social and Economic Transformation in the Digital Era, 18.

[39] Tonn, G., Kesan, J. P., Zhang, L., & Czajkowski, J. (2019). Cyber risk and insurance for transportation infrastructure. Transport Policy, 79, 103–114.

[40] Tsai, M.-C. (2006). Constructing a logistics tracking system for preventing smuggling risk of transit containers. Transportation Research Part A: Policy and Practice, 40(6), 526–536.

[41] Vorakulpipat, C. (2013). Good practices and challenges in Cyber Security Thailand.. Retrieved from www.connect2sea.eu/news-and-events/news/details/EU-SEA-Workshop-International-Cooperation-on-Cyber-Security-Towards-the-NewAvenues-organised-in-Hanoi-Vietnam.html%3Ffile%3Dfiles/connect2sea/files/Workshops/Good%2520Practices%2520and%2520Challenges%2520in

[42] Windelberg, M. (2016). Objectives for managing cyber supply chain risk. International Journal of Critical Infrastructure Protection, 12, 4–11.

[43] Yeo, G.-T., Pak, J.-Y., & Yang, Z. (2013). Analysis of dynamic effects on seaports adopting port security policy. Transportation Research Part A: Policy and Practice, 49, 285–301.