Rethinking transport
27–30 April 2020

TRA 2020 HELSINKI

Proceedings of 8th Transport Research Arena TRA 2020, April 27-30, 2020, Helsinki, Finland

The Cyber Threat Preparedness in the Maritime Logistics Industry

Harri Pyykkö[a]*, Jarkko Kuusijärvi[b] Bilhanan Silverajan[c], Ville Hinkka[a]

[a] *VTT Technical Research Centre of Finland Ltd, Vuorimiehentie 3, FI-02150 Espoo, Finland*
[b] *VTT Technical Research Centre of Finland Ltd, Kaitoväylä 1, FI-90571 Oulu, Finland*
[c] *Tampere University, FI-33014 Tampere University, Tampere, Finland*

Abstract

This paper reflects the importance of preparedness regarding cybersecurity and cyber threat related factors in maritime logistics industry in present era when the digitalization combined with new emerging technologies i.e. Artificial Intelligence, Internet of Things, Blockchain and so forth are being utilized with accelerating speed in the maritime logistics among others. The future trend in the maritime logistics indicates that all the resources are connected with each other in order to form integrated autonomous operating systems based on IT-platforms. Therefore, there is a need also in the maritime logistics industry to attach cybersecurity related matters and cyber threat prevention more systematically to the existing procedures in every level of the organization and consider these aspects when new technologies are being implemented. Training the personnel from the non-technical to the technical experts in realistic exercises help to prepare and handle the cyber incidents and raise the overall level of cybersecurity preparedness.

Keywords: Cybersecurity, cyber threat, cyber exercise, maritime, logistics, port

* Corresponding author. Tel.: +358-40-158-9592;
E-mail address: harri.pyykko@vtt.fi

1. Introduction

Maritime transportation is one of the key elements for global trade and the EU economy as 80% of world trade and 74% of EU trade is carried by sea. (European Commission 2009; European Commission 2013). The global trade is dependent on maritime transportation which is an integral operational part of increasingly complex and large port systems. Maritime and port systems are more predisposed to various types of threats both physical and technological. There is an evolving demand to develop and apply methodologies and instruments in order to assess the overall risks occurring in the maritime logistics industry. (Pallis 2016) Due to the fact that ports are a part of critical infrastructure, an interruption to port operations can become highly expensive and the port security remains vitally important as threats towards ports effects not only the actors inside the physical port area but also causing severe financial damages on the existing supply chains. (Rantasila et. al, 2012) In addition to natural hazards, there are intentional and unintentional man-made risk sources that have a potential to cause financial losses or even physical harm to organisations or people. (Kaundinya et al. 2016).

As highlighted above the ports are a vital part of global supply chains and risks to ports affect not only the ports themselves despite they are in all-important role but also several other stakeholders and the whole supply chain from the manufacturer to the end-user of the cargo. There are various types of risks effecting ports which can in the worst case lead to the shutdown of a port such as breakdown in security systems, theft of cargo or data, smuggling of illicit material pass customs and financial losses. (Loh & Thai 2015.) Even a minor weakness in port systems or in critical databases creates a potential for cyber- or terrorism attacks which is a fact that can not be ignored by the stakeholders of maritime logistics industry (John et al. 2014; Polatidis et al. 2018). Due to growing digitalization trend effecting all supply chains, maritime information systems are increasingly vulnerable for cyber threats (Hebrard et al. 2017) and as maritime industry is increasingly depended on various ICT systems, the cybersecurity needs to be updated to an adequate level in order to meet the security requirements for future. (Fitton et al. 2014).

This is a position paper looking at the current state of cybersecurity readiness and ways to improve it. The emphasis is on maritime logistics in general and the motivation for this paper comes from increased digitalization which has also become integral part of current maritime logistics. Based on literature review and by utilizing the experience of multi-disciplinary researchers, this paper aims to summarize how the implementation of new digital technologies has effected cyber threats in maritime logistics industry and how the industry could prepare for these cyber threats.

2. Cyber threats as a risk for supply chains

In a supply chain management (SCM) viewpoint, cyber threats are part of the security threats. Security threats have been recognized in SCM literature, but until recently, they have received minor attention. Usually security threats are seen from a viewpoint of causing disorder as a primary aim such as in a form of terrorism. The viewpoint that terrorism could be used to e.g. to steal confidential information or just disturbing competitor's business is not specified. Rao and Goldsby (2009) mention terrorism as a source of social uncertainty risk, which is further included as one of the environmental risks for SCM. Xie et al. (2011) considers security threats in a viewpoint of their consequences. The most common consequence is disruption, and therefore Xie et al. (2011) include security threats as disruption risks for SCM. Kumar et al. (2010) instead mention terrorism as a part of external operational risks. Due to increased use of digital technologies in SCM, the viewpoint for security risks has enlarged and they have been recognized more in the literature. Recently based on the literature review of Birkel and Hartmann (2019), the most considered risks related to the use of Internet of Things (IoT) technologies in SCM are attack-related risks. Birkel and Hartmann (2019) also raise the security issues as further research directions in technological and environmental sectors of the use of IoT technologies.

Maritime industry is an integral part of the most of the supply chains as majority of the trade is carried by sea. Therefore, the problems in maritime transports will affect greatly for the management of the entire supply chain. However, it is challenging to construct a holistic model for a secure end-to-end supply chain for maritime logistics, as any of its individual parts can be subverted. In the absence of green field solutions, cyber practitioners, operators and cargo handlers have to presume a dirty network, and instead attempt at building trustworthy operations and systems out of untrustworthy parts. This is the philosophy behind much of the cybersecurity industry today: systems watching one another, looking for vulnerabilities and signs of attack. (Schneider 2019) In the near term, however, cyber risk management remains an important facet for cyber readiness, that should become an inherent

part of maritime logistics operations.

3. Cybersecurity and Maritime Logistics

The vulnerabilities in the maritime sector focuses especially on various types of operational risks and accidents, mishandling of hazardous cargo, labor strikes, and security violations. The digitalization has caused the ports to be involved in complex information flows that depend on different ICT systems interacting with each other, which means there is a potential threat for a possible entry point to an unauthorized access. The cyber threat can occur basically in every piece of data that is exchanged and saved in the existing ICT systems. (Kouwenhoven et al. 2016). The maritime business environment is very complex and can be divided various ways depending on the stakeholder's point of view however a clear division into the two main types remain: 1) the physical environment and 2) the cybernetic environment, as shown in Table 1. The physical environment involves various stakeholders such as authorities, maritime, terminal and insurance companies, labor, and facilities including the port infrastructure. The cybernetic environment in turn comprises the port infrastructure, ICT systems such as networks, ICT hardware, services, data, users and telecommunications systems. (Dellios & Papanikas 2014; Polemi 2018.)

Table 1. Physical and cybernetic environment of the maritime sector (Dellios & Papanikas 2014; Polemi 2018)

PHYSICAL ENVIRONMENT
Port infrastructure, facilities, gates, platform, data centres and marinas
Port authorities
Maritime and insurance companies
Shipping and cargo industry
Manufacturers and suppliers
Government ministries
Related transport infrastructure
Human resources

CYBERNETIC ENVIRONMENT
Infrastructure, such as buildings and ships
Platforms, such as servers and databases
Telecommunication systems, such as networking terminals and geographic information systems
Software and manuals, such as information and data
E-services, such as applications, frameworks, and test environments
Other equipment, such as fire alarm extinguisher systems, and surveillance systems
External users, such as port authorities and maritime companies
Internal users, such as administrators and personnel

As described in the Table 1, the operations of ports depend on the physical environment and infrastructures within the port areas, but also on a constant base of ICT systems and infrastructures (Papastergiou et al. 2015). Ports have large-scale and complex infrastructure and they are seen as part of the critical infrastructure and bottlenecks for transportation chains. Therefore if the operations in the ports would be disturbed or even interrupted this may have severe consequences on national health, security and safety, economy, and threating even the everyday life of the citizens. Since both of these physical and cyber systems include a large amount of critical and sensitive information and there are various interdependencies with other critical infrastructures, they are noticed to be susceptible, for example, to precarious accidents and cyberattacks. (Polemi & Papastergiou 2015; Polemi 2018; Ahokas 2019) Because of the significant transportation volumes involved in the maritime logistics, it has a vital role linking the global economies together. This fact makes the ICT system of maritime logistics especially attractive target for malicious actors. A possible cyberattack on any critical infrastructure can easily cause tremendous damages in various ways in a worst case effecting negatively the lives of large number of ordinary people and various businesses. (Kalogeraki et. al. 2018)

Lytle III & Thomas (2015) underlines the trend that the cyberattack methods are getting increasingly sophisticated and several types of threats in maritime ICT system have been recognized in recent years from advanced attacks which are focusing on a specific target to unintentional but damaging malware and simple technical failures. These type of failures can compromise vital safety, security and environmental functions or in a larger scale may lead to extensive trade interruptions effecting large geographical areas. It is important to recognize that merely by distracting or closing the ICT systems or electricity within a port or inside a ship, cyberattackers could jeopardize the functionality of emergency responses and rapidly cause diverse types of accidents. (Kouwenhoven et al. 2016; Polemi 2018). For instance, cyberattackers may gain access to a modern cargo ship's operating systems, shutting down a port or its terminal and gain access to delicate information. Due to the nature of maritime logistics where

large volumes are involved, even the smallest cyberattacks can lead to business losses of millions of dollars. (Caponi et al. 2014)

The maritime industry has generally not been involved in serious cyber incidents and it might have caused certain lack of focus on this particular topic. When the most significant cyberattack NotPetya occured in July 2017 against world's largest container carrier Maersk (Tinsley & Sorensen 2017), it made international maritime logistics industry to realize its exposure towards cyberattacks. It also emphasized to the maritime industry that there are no specific guidelines or standards in place to moderate or prevent a major cyberattack especially targeted on maritime logistics industry (Jensen 2017). The NotPetya cyberattack indicated a lot about the vulnerability level of the maritime sector to cyberattacks, given that the world's largest container carrier Maersk who had invested considerable amounts of money in digital safety protocols but was still successfully attacked by using very advanced cyberattack methods. (Nadkarni 2017; Kiiski 2018.) The lack of cyber security preparedness and awareness among maritime industry was also notable when Ahokas and Laakso (2017) published their findings based on empirical research from the Baltic Sea Region underlining the shortage of cyber threat preparedness and lack of regulation in ports. The empirical study indicated that there are multiple factors and actors that need to be studied and understood at a more common level and by using multidisciplinary approach in order to raise the awareness of cybersecurity even further. (Ahola 2019).

The important critical infrastructure sectors (energy, public health, etc.) have been progressing on cybersecurity matters greatly during the past years, partially because of the incentive for improvement due to cyber incidents in the world that have also received broad media coverage. The maritime logistics industry has the opportunity to take the lessons learned from the cybersecurity practices of the other critical infrastructure sectors in securing their part before facing the more devastating incidents. Nevertheless, it has not survived without major incidents completely either, as described earlier in this section, and other minor incidents reported (BIMCO, 2018). Starting from cyber risk management towards implementing the security controls, the current guidelines by IMO for shipping rely on the following functional elements to cover all the relevant cyber aspects: identify, protect, detect, respond, and recover (IMO, 2017). The IMO guidelines themselves are quite short and refer to other documents for actual implementation details. The more detailed steps and actions to implement each of the five elements can be found in other documents, such as the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST, 2018) and the BIMCO Guidelines on Cyber Security Onboard Ships (BIMCO, 2018). The BIMCO guidelines focus on the cybersecurity on ships and the connected stakeholders, giving more practical examples of the measures to be implemented, and even describe relevant cyber incidents that have occurred (BIMCO, 2018). The Cybersecurity Framework (NIST, 2018) gives references to other standards and guidelines as well (e.g., CIS Controls (CIS, 2019), ISO/IEC 27001 security standard, and NIST SP-800-53 Special Publication on security and privacy controls). To cover security controls, Centre for Internet Security (CIS, 2019) provides a list of 20 CIS Controls (with sub-controls for each) to implement.

The cybersecurity standards and frameworks are usually very large and complex to implement fully. One needs to select/combine and implement frameworks/standards/guidelines suitable for their domain and the specific system in question. The maritime logistics sector can utilize the same framework(s) available for the other critical infrastructures, adapting them according to the sector specific needs. First important step is to identify the assets (IT/OT devices, software, etc.) that are involved in the system(s) and implement the security controls to protect them, alongside the other elements (detect, respond, and recover) described to support the overall cyber risk management. Moving from the technological cybersecurity controls towards the users and their role, the CIS Control 17 (CIS, 2019) "Implement a Security Awareness and Training Program" is of particular interest in this paper, since raising the cybersecurity awareness in this sector is especially important.

4. Cybersecurity training and awareness

It is evident that the growing level of digitization in the maritime logistics industry has had many positive effects in terms of increasing efficiency, safety and energy saving but this development has also shaped various forms of new cyber risks which need to be taken into serious consideration within the organizations. (Fruth & Teuteberg 2017) This can be eventually done when the maritime sector faces the fact that cybersecurity needs to be built-in to physical security and company strategies in addition to increase the general awareness on this topic throughout the whole organization. (Shah 2004; Skrlec et al. 2014). When considering security awareness in maritime, it is important to keep in mind the myriad stakeholders, upstream suppliers, competing providers as well as the complexity of interconnected, and sometimes, intersecting supply chains that feed into the logistics operations and

cargo handling in ports and shipping lines. Cybersecurity in the maritime industry is therefore closely coupled with physical security as well as safety. Cyber readiness is not just a technical problem. Other considerations such as operational practices and competing business interests factor heavily into the equation. Cyber incidents today arise from activities such as insecure practices (BBC 2018) as well as the usage of outdated and end-of-life systems. (Jones et. al. 2016) Incident sharing in the maritime sector, which can improve safety and security by learning from previous incidents, is poor. This was confirmed both by studies conducted to investigate how Finnish shipping companies engage in incident reporting (Lappalainen et. al. 2011), as well as from news reports detailing how similar ransomware attacks performed in different ports could have been prevented. (ZDNET 2018)

Training is needed for both the *professionals* (cybersecurity, ICT experts, etc.), and the *non-technical personnel* of ports, shipping operators, and so forth. Cyber threat awareness level and skills of the individuals can be improved by hands-on training with realistic cyber exercise scenarios that cover different levels of interactions and triggers/injects in the actual environment. An important aspect in cyber training is that the scenarios reflect to your normal day-to-day operations and the systems and tools you normally use. The exercises should also engage the users in the most recently discovered cyber threats/incidents, in order to keep up with the arms race between new techniques, technologies and tricks used to realize the threat. It is also important to instruct the users about all the possible ways a cyber threat can realize and the best way to learn and prepare to this is by experiencing it in an exercise at some level of detail. Cyber exercises should train and prepare the users to handle these cyber incidents from the start (the reconnaissance) all the way to the actual breach, data exfiltration, data destruction, or data encryption for ransom (as occurred in the Maersk case).

Conducting realistic exercises in the actual environment is difficult or even impossible, since the systems are in daily use and cannot be used in an exercise, where they will be compromised. Individual systems can be used in trainings separately, or specific cyber trainings can be organized, but in order to grasp the whole situation, an integrated and as operable as possible environment is needed. Cyber ranges can be used to conduct realistic cyber exercisers in IT as well as in OT (Operational Technology) environments, where PLCs (Programmable Logic Controller) and other IoT devices are attached and/or simulated in the cyber range. Cyber ranges can create a digital twin of the target environment and networks with the help of virtualization technologies, where it is safe and realistic to conduct exercises where cyber incidents occur in a controlled way. It is up to the actual personnel to handle the situations: prepare, block and/or mitigate against them, prepare and train how to recover the systems back online from previously secured backups, for instance. Trainings can therefore cover all aspects from normal day-to-day operations by operators down to the cybersecurity issues handled by the cybersecurity professionals.

Guidelines for cybersecurity risk management already exist for ship-board systems (BIMCO 2019), but they are equally relevant to maritime logistics. This is depicted in the risk management approach as shown in the Fig. 1. below:

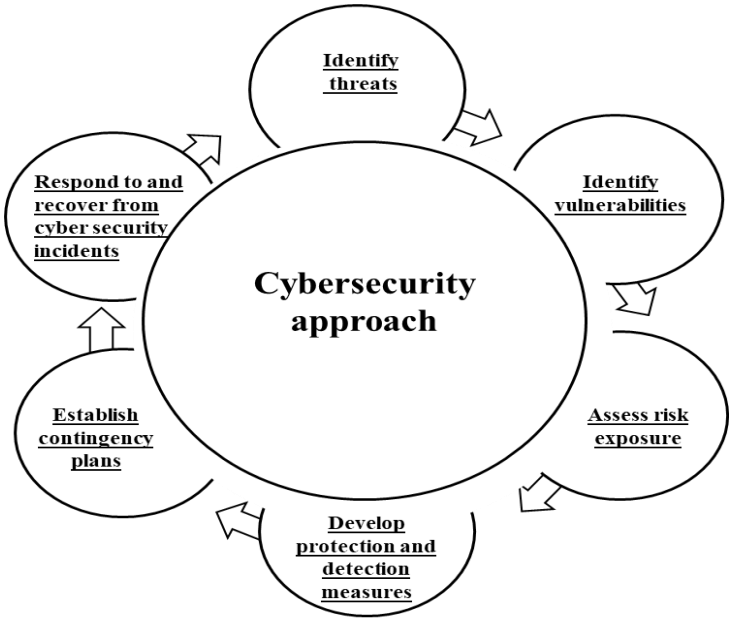

Fig. 1. Cyber risk management for ships (BIMCO 2019)

These guidelines, when adapted towards cyber risk management for maritime logistics should include the following activities:

1. Identification of the roles and responsibilities of users, key personnel and management of stakeholders and operators of the relevant supply chains
2. Identification of the systems, assets, data and capabilities, which if disrupted, could pose risks to the logistics operations and safety
3. Implementation of technical and procedural measures as well as alternatives, to protect against a cyber incident to ensure continuity of operations
4. Implementation of activities to prepare for and respond to cyber incidents.

5. Concluding Remarks

This paper reflects the importance of preparedness regarding cybersecurity and cyber threat related factors in maritime logistics industry in the present era when the digitalization combined with new emerging technologies are being utilized with accelerating speed. The future trend in the maritime logistics indicates that the next-generation smart shipping is rapidly embracing advanced technologies such as autonomously operating systems, machine learning and artificial intelligence, that perform decision making without human intervention and indeed inspect systems faster and more thoroughly than humans do. Solutions based on these can mitigate against increasingly sophisticated cyberattacks. However, the advantage today still lies with the attacker. Cyber readiness and risk management for maritime logistics is an area that needs substantial research. Compared to several other industries, cyber awareness remains very low in the maritime sector. In a leading transport survey published by international law firm Norton Rose Fulbright in 2017, 87 percent of respondents from the shipping industry believed cyberattacks would increase over the next five years - a level that was higher than counterparts in the aviation, rail and logistics industries (Saul, 2017).

The safety related issues have always played a major role in the maritime sector as even a minor accident might have serious effects to the people and environment due to the large cargo volumes involved which are often including hazardous materials in addition to the potential financial losses. However, based on several indicators, there is a general need among maritime sector to target the interest more closely towards improving the cybersecurity matters and increasing the cyber awareness by training the entire personnel whoever has access to the ICT-systems to be aware of techniques to prevent cyber threats in their daily work. To raise the topic in a larger scale, Miron & Muita (2014) highlighted the fact that cybersecurity is actually a global matter as ports form a significant part of the critical infrastructure, which is important for every nation in the world. In terms of improving research on this subject, it appears that the majority of the cybersecurity research have been done with the focus of technical approach while there is a lack of more specific cross-functional research on cybersecurity in the context of maritime logistics especially. Bringing cyber exercises and cyber range capabilities into the context of the maritime sector can greatly improve the preparedness of the different users of this specific area and therefore improve the overall cybersecurity preparedness as a result.

It is hard to envision a future scenario where the maritime sector, a sector where some of the world's oldest fleets and ports compete with some of the world's most modern in terms of price and performance for shipping and cargo handling, can be solved purely with technical solutions, without detailed rules and guidance from regulatory authorities regarding IT and OT infrastructure used. Data governance rules must be put in place to facilitate industry-wide incident exchange and response systems. Incentives, such as reduced insurance costs or increased coverage, can be provided to modernize logistics and shipping operations to reduce fraudulent activity, increase accountability and promote transparency. This is not just for the present but for the future, to cater for autonomous vessels and land-based vehicles. EU/NIS Directive (pl, art.3) concludes that "Cybersecurity is not only a technological, but also a strategic and political issue which affects every physical or legal entity and which everyone for their part is responsible for."

Acknowledgements

The authors want to thank EU Commission's Horizon 2020 Cyber-MAR (Cyber preparedness actions for a holistic approach and awareness raising in the MARitime logistics supply chain) project (grant agreement No. 833389) project and COREALIS (Capacity with a pOsitive enviRonmEntal and societAL footprInt: portS in the future era) project (grant agreement No. 768994) for funding the writing of this paper. However, the content reflects only the authors' view and EU is not responsible for any use of the information it contains.

References

Ahokas, I. (2019) *The Finnish Maritime Sector and Cybersecurity*. Publications of the HAZARD Project. https://blogit.utu.fi/hazard, retrieved 2.5.2019.

Ahokas, I., Laakso, K. (2017) *Delphi study on safety and security in the Baltic Sea Region ports.* Publications of the HAZARD Project. https://blogit.utu.fi/hazard, retrieved 6.5.2019.

BBC (2018): *Ship hack 'risks chaos in English Channel'*, https://www.bbc.com/news/technology-44397872 [Accessed 15 September 2019]

BIMCO (2018). The Baltic and International Maritime Council (BIMCO), *The Guidelines on Cyber Security Onboard Ships*, Version 3, 2018.

BIMCO, (2019), *The guidelines on cybersecurity onboard ships*,
https://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelineson-cyber-security-onboard-ships.pdf [Accessed 15 September 2019].

Birkel, H. S., & Hartmann, E. (2019). Impact of IoT challenges and risks for SCM. *Supply Chain Management: An International Journal*, 24 (1), 39-61

Caponi, S., Belmont K. (2014) *Maritime Cybersecurity: A Growing Threat Goes Unanswered*. Published 22.10.2015.

CIS (2019). Center for Internet Security (CIS), *CIS Controls*. https://www.cisecurity.org/controls/cis-controls-list/, retrieved October 8, 2019.

Dellios, K, Papanikas, D., (2014), *Deploying a Maritime Cloud*, IT Professional, Vol 16 (5), 56-61.

European Commission, 2009, *Communication from the Commission to the EU Parlament, Strategic goals and recommendations for the EU's maritime transport policy until 2018*. COM2009/008 final.

European Commission, 2013. 'Ports: an engine for growth'. COM/2013/0295, 23.05.2013, Brussels.

Fitton, O., Prince, D., Germond, B., Lacy, M. (2014) *The Future of Maritime CyberSecurity. Lancaster University*, 15th April 2014.

Fruth, M. – Teuteberg, F. (2017) Digitization in maritime logistics – What is there and what is missing?
Cogent Business & Management, Vol 4.

Hebrard, P., Lacoste,F. (2017), *Maritime Cybersecurity*, White Paper, ECSO.

IMO (2017). The International Maritime Organisation (IMO) MSC-FAL.1/Circ.3, *Guidelines on Maritime Cyber Risk Management*.

Jensen, L. (2017) *The Threat hidden in the depths*. Harbours Review - Cyber security and risk management, No. 4/2017.

John, A., Paraskevadakis, D., Bury, A., Yang, Z., Riahi, R., Wang, J. (2014): *An integrated fuzzy risk assessment for seaport operations*, *Safety Science*, 68(1), pp. 180–194.

Jones, K., Tam, T., Papadaki, M.(2016). *Threats and impacts in maritime cybersecurity*. Journal of Engineering & Technology Reference, Published 22/04/2016

Kaundinya, I. Nisancioglu, S, Kammerer, H, Oliva, R. (2016): *All-hazard Guide for Transport Infrastructure*, Transportation Research Procedia, 14(1), pp. 1325–1334.

Kalogeraki, E., Papastergiou, S., Haralambos, M., Polemi, N. (2018): *A Novel Risk Assessment Methodology for SCADA Maritime Logistics Environments*, Applied Sciences Journal, 2018: 8 (9).

Kiiski, T. (2018) *Major Maritime Cyber Incidents: A review*. PTI Journal, Vol 77, 129-130.

Konecny, J., Jankova, M., Dvorak, J., 2017, *Modelling of Processes of Logistics in Cyberspace Security*, MATEC Web of Conferences 134, 134. LOGI 2017.

Kouwenhoven, N., Borrett, M., Wakankar, M. (2016) *The Implications and Threats of Cyber Security for Ports*. PTI Journal, Vol 72, 58-60.

Kumar, S. K., Tiwari, M. K., & Babiceanu, R. F. (2010). Minimisation of supply chain cost with embedded risk using computational intelligence approaches. *International Journal of Production Research*, 48(13), 3717-3739.Lytle III, M., Thomas, P., (2015), *Assistant Commandants' Perspective*. Proceeding of the Marine - WIN 2015, The Marine Safety & Security Council of US Coast Guard.

Lappalainen, J,, Vepsäläinen, A., Salmi, K., Tapaninen, U., (2011), *Incidentreporting in finnish shipping companies*,WMU Journal of MaritimeAffairs, vol. 10, no. 2, p. 167, 2011

Loh, H., Thai, V. (2015) *Assessing the risk of cyber terrorism, cyber war and other cyber threats.* Centre of Strategic & Internation Studies (CSIS).

Miron, W., Muita, K. (2014), *Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure.* Technology Innovation Management Review. Vol 4 (10), 33-39.

Nadkarni, N. (2017) *Fighting the faceless criminal*. Port & Harbours, September/October 2017, 22-23.

NIS (2016), *The Directive on security of network and information systems*, p1, art. 3., Directive (EU) 2016/1148 of the European Parliament and of the Council.

NIST (2018), National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*. Available: https://doi.org/10.6028/NIST.CSWP.04162018

Pallis, P.,L, 2016, *Port Risk Management in Container Terminals*, WCTR 2016, Shanghai 10-15 July 2016.

Papastergiou. S., Polemi, N., Karantijas, A., (2015) CYSM: *An Innovative Phisical/Cyber Security Management System for Ports*. HAS 2015: Human Aspects of Information Security, Privacy and Trust. 219-230.

Polatidis, N, Pavlidis, M, Mouratidis, H. (2018): *Cyber-attack path discovery in a dynamic supply chain maritime risk management system*, Computer Standards & Interfaces, 56(1), pp. 74–82.

Polemi, N. (2018) *Port Cybersecurity - Securing Critical Information Infrastructures and Supply Chains*. Elsevier.

Polemi, N., Papastergiou,S, (2015), *Current efforts in Ports and Supply Chain Risk Assessment.* The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015), London, UK, December 14-16, 2015.

Rantasila, K., Pilli-Sihvola, E., Permala, A., (2012), *Technologies enabling efficient transport monitoring*, 5th European conference on ICT for Transport Logistics, November 2012, Gothenburg, Sweden.

Rao, S., & Goldsby, T. J. (2009). Supply chain risks: a review and typology. *The International Journal of Logistics Management*, Vol 20 (1), 97-123.

Saul, J. (2017). RPT-Global shipping feels fallout from Maersk cyber attack, *Reuters*, June 30, 2017.

Shneider, B., (2019), *Supply-Chain Security and Trust*,
https://www.schneier.com/crypto-gram/archives/2019/1015.html#cg13 [Accessed 15 September 2019]

Shah, S.K. (2004) *The Evolving Landscape of Maritime Cybersecurity*. Review of Business, St. John's University, Vol 25 (3), 30-36.

Skrlec, Z., Bicanic, Z. (2014) *Maritime Cyber Defence*. 6th IMSC Conference, Book of Proceedings, April 28-29, 2014, Croatia.

Tinsley, P., Sorensen, A.F., (2017), *Port and Ship Cyber Security after NotPetya*, PTI Journal, Vol 75, 96-97.

Xie, C., Anumba, C. J., Lee, T. R., Tummala, R., & Schoenherr, T. (2011). Assessing and managing risks using the supply chain risk management process (SCRMP). *Supply Chain Management: An International Journal*. Vol. 16 No. 6, pp. 474-483.

ZDNET, (2018), *Port of San Diego suffers cyber-attack, second port in a week after Barcelona*,
https://www.zdnet.com/article/port-of-san-diego-suffers-cyber-attack-second-port-in-a-week-after-barcelona/
[Accessed 15 September 2019]