SETSCI Conference Indexing System,
Volume 3 (2018), 246-251

ISAS 2018-Winter
2nd International Symposium on Innovative Approaches in Scientific Studies
November 30 – December 2, 2018, Samsun, Turkey

Cyber Terrorism Risk at Ports and Organizational Management Process in Application of Security Plan

Mehmet Sıtkı Saygılı[1*+], Ahmet Naci Ünal [2]

[1]Vocational School/Bahçeşehir University, İstanbul, Turkey
[2]Faculty of Engineering and Natural Sciences/Bahçeşehir University, İstanbul, Turkey
[*]Corresponding author: mehmet.saygili@vs.bau.edu.tr
[+]Speaker: mehmet.saygili@vs.bau.edu.tr
Presentation/Paper Type: Oral / Full Paper

Abstract **–** About 90% of world trade in transportation of goods is conducted via maritime transportation. An important operation area of maritime cargo transportation is ports. It is necessary to keep these ports secure where information and communication technologies are utilized widely. In terms of security, one of the security parameters is cyber space. Utilization of information and communication technologies at ports brings about various security flaws for cyber attacks. One of the risks led by the deficits is terrorist actions carried out by cyber attacks. Today, risk of cyber terrorism has been increasing gradually and companies which are aware of the threat work on necessary measures. In this study, cyber terrorism threat at ports is analyzed; also measures to be taken for prevention or decrease of risks, and application process in port organization structure are evaluated. In this study, literature review was conducted. Also, evaluations were conducted as a result of interviews with information technologies and security specialists of ports.

Keywords – Maritime Transportation, Port Management, Cyber Terrorism, Security, Risk Management

I. Introduction

Ports are international gates of a country that open up to the world. Today, ports are centers that are integrated with other modes of transportation, have logistic services like carriage, warehousing, custom, distribution and insurance as well as loading and unloading; they have infrastructure to give services to different types of ships and cargo and they utilize information and communication technologies intensely. A cyber attack to a port led by use of information and communication technologies for terror cause problems in economy of a country, destruction in infra- and/or super-structure, jeopardy in security, social chaos and negative effect on society's health.

After terrorist attacks on September 11th 2001 in United States of America conducted by vehicles, International Martime Organization (IMO) pioneered to take new measures regarding security of ships and port facilities in order to prevent all kinds of terrorist attacks at sea or from sea. In this way, the International Ship and Port Facility Security (ISPS) Code was constructed. ISPS Code defines responsibilities of the contracting states, obligations of the companies, measures regarding ship and port security and their scopes. Also, International Safety Management (ISM) Code was introduced for safe management of ships and prevention of sea pollution. ISM includes minimum standards that makes management of a ship possible without endangering life, property and environmental safety. Both applications were added to the 1974 dated International Convention for the Safety of Life at Sea (SOLAS) and have binding effects on contractor states [1]. Basic reason for measures is to increase security in maritime transportation. However, threat of cyber attacks continues to be a problem in maritime sector, as it is the case in all other sectors, even though measures that were taken increased physical security [2].

The present study considers possibility of terrorist actions at ports via cyber attacks. In the study, scope of cyber attacks and terrorism is defined firstly and then possible cyber terrorist attacks to ports are explored. Risk analysis for prevention of attacks and basic framework of related cyber security plan, and application of the plan within organizational structure of the port.

II. Cyber Attacks and Cyber Terrorism

Digital Information Warfare is a process of introducing malicious computer software into a system of information (which can be either a very large information network or personal computers) for civil, military, political, economic or personal purposes without the knowledge of the user. The attacker can be a security organization of any country, a terrorist organization, an international business or any other person. The field of activity of the digital information war is so wide and aims vary according to the damage to be given to the user. Therefore, according to the type of attacker, the purpose of digital information warfare can be grouped into three sub-headings. These are weakening, deception and disabling of the target information system. In order to achieve these objectives, individuals or organizations that apply the war of digital information generally follow the stages of infiltration, expansion, waiting to become active and becoming active [3]. In this context, the techniques used can be named as cyber attack.

The cyber attack is an attempt to eliminate the privacy, integrity or accessibility of the information contained in cyberspace. There are many results ranging from propoganda to spying and interfering with services in order to damage

critical infrastructures (finance, production, communication, energy etc.) [4], [5]. Cyberspace, where cyber attacks take place is a complex environment that does not exist physically, which arises from the interaction of people, software and the services on the Internet through technological tools and their connected networks [6]. Cyberspace means more than internet. It includes all software, hardware and shared data, which can be linked to cyberspace. It is also a structure in which people and social interaction are involved.

Cyber attacks that result from the human factor in cyberspace as shown in Figure 1 are conducted by foreign intelligence services, disaffected employees, investigative journalists, extremist organizations, hactivists, organized crime goups [7], terrorists [8] and rebels [9].

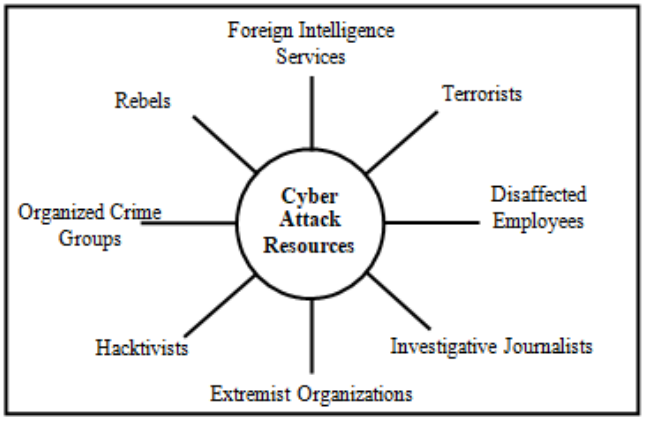

Fig. 1 Resources of cyber attacks

Terrorist actions can also be realized through cyber attacks. "The term 'terrorism' means premeditated, politically motivated violence perpetrated against non-combatant targets by sub-national groups or clandestine agents, usually intended to influence an audience [10]". Terrorism is also a kind of psychological warfare based on psychological manipulation. Terrorists aim to evoke fear and anxiety by attacking the weak and vulnerable sides of their targets. Terrorists use three main tools to increase their power. These are media, support networks and technology. Cyber terrorists similarly use the same tools to enhance the impact of their goals [11]-[13]. Because cyber space turned into a battlefield by terrorists, they no longer rely solely on military power; their strategy and tactics have become increasingly technology driven [14].

The concept of cyber terrorism is defined in various ways. According to Barry Collin who is one of the first users of the concept, cyber terrorism consists of intersection of physical and virtual concepts which are separate from each other [15]. According to another definition, cyber terrorism in the strict sense is defined as politically intended attacks targeting information systems that are not part of war; whereas in a broad sense, cyber terrorism refers to the use of all kinds of information and communication technologies of terrorists [16]. Cyber terrorism can also be defined as personally or politically motivated actions aim to disrupt or harm the balance of organizational or national interests through the use of electronic tools for information systems, computer programs or other communication transfer and storage tools [17]. There is also a reference to Dorothy E. Denning's paper for the definition of cyber terrorism [18]. According to this definition, cyber terrorism is the intersection of terrorism and cyberspace. They are attacks or threats against computers, networks, and information stored within them, or threats to suppress or intimidate a government or public for political and social purposes. Moreover, for an attack to be classified as cyber terrorism, it must contain violence against people or goods, or at least cause harm that evoke fear. Serious attacks against critical infrastructures can be an act of cyber terrorism when they adversely affect the social order if these structures fail to perform their functions. However, attacks that interrupt non-essential services or give intensely financial damage are not considered as cyber terrorism [19]. Although there are various differences in the scope of the definitions, the tools of attack are the information and communication technologies that have been increasing rapidly in people's daily life.

III. Maritime Transport and Cyber Terror Threats

Risk is the possibility that a different situation from expected one may arise in the future. The difference may be in favor of or against the company. However, the word risk is often used to mean the possibility of negative damage [20]. When it occurs, terrorist threat is a risk with devastating consequences.

The maritime transport integrates the global trade and logistics network, and one of its main components is the ports [21]. The ports are delicate areas that spread the threat of terror over a wide area due to the size of their surface area, intermodal transport connections, busy and crowded trade centers. Also, because ports are critical infrastructures when the secrecy, integrity or accessibility of the information in the ports is impaired, it may cause loss of life, large-scale economic damage, national security deficits, or deterioration of public order [22]. For this reason, it is necessary to take protective measures in advance and eliminate the possibility of occurrence of the threat or minimize it within acceptable limits.

The basic objectives for a terrorist attack in a port can be summarized as follows in connection with Figure 2 [23].

A) Closing the harbor mouth to prevent entry from the sea to the port.

B) Sinking or damaging a ship in the port.

C) Damaging the terminal and / or terminal equipment.

D) Changing the contents of the load or damaging the load in the terminal.

E) Damaging the railway connection in the port area.

F) Damaging the highway connection in the port area.

G) Damaging the international highway.

H) Damaging inland waterway transport.

I) Sabotaging the pipeline and stopping the flow.

J) Armed attack on the facility from outside the port.

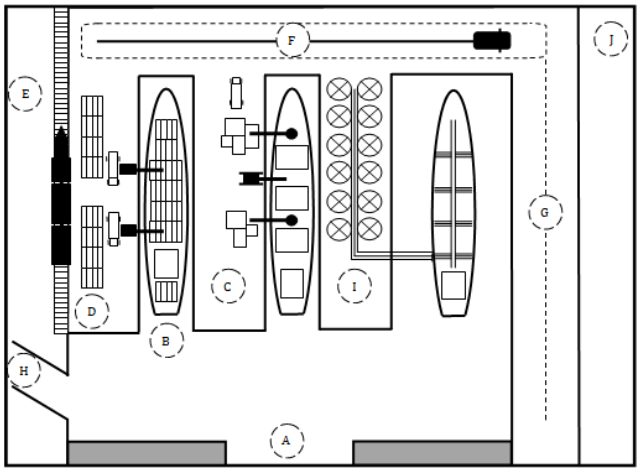

Fig. 2 Targets for terrorist attacks in ports

In general, a terrorist attack on a port targets, a portion of the cargo, transportation vehicles within the port and port environment. Cyber-attack elements can also be used in terrorist actions against these targets.

In international trade, in terms of security, it is difficult to monitor cargos produced in different parts of the world and transported by sea. For example, a container transport includes data transfer between different parties, such as shipping company, departure port, destination port, road transport company, purchaser, customs authorities, mediators and banks [24]. For security purposes, it is necessary to monitor all cargo movements and share information between the parties. Because of the cyber attacks, the system information in the ports can be changed and weapons and / or terrorists can be placed in containers. Chemical, biological, radiological and nuclear materials at the storage area in ports can be used for attacking [25]. Today, some terrorist groups use international communication tools to create international networks and thus increase their technical skills.

Today, many ships are driven by computers that control navigation, communication, fire prevention systems and engines; this situation creates vulnerability to cyber attacks in the maritime sector [26]. Automatic Identification System (AIS), which is developed to provide automatic information from ship to ship and from ship to shore authority, is used in international transports with over 300 gross tons and above vessels, and it is used on all passenger ships, regardless of the size of the cargoes carrying over 500 gross tons and above [27]. Researchers at Trend Micro have conducted an experiment to measure the sensitivity of the system to cyber attacks. By using a simple communication device, the internet provider has been manipulated and the system has been broken and the data changed. In this way details such as the position, route, load, flag and name of the ship could be changed and at the same time they were able to form a fake ship in any position [28]. Transport vehicles are the target of terrorist attacks, but are also used as weapons [29]. The Global Positioning System (GPS), which provides location information through the interaction of satellites emitting regular signal emitters on the earth, is affected by signal disturbers. In a study, the GPS, which directs the autopilot, was deceived by device that cost $3000 and the devide maneuvered the ship outside the control of the seaman [30]. The Vessel Traffic Services System (VTS), which is used to ensure safety in maritime traffic, may pose a danger by misleading ships as a result of cyber attacks. Here, ships can be targeted. At the same time the other danger is the possibility of attacking ports by using ships. The issue of cyber attack and terrorism is an important security risk for maritime transport considering all these events.

IV. Risk Analysis and Cyber Security Plan for Cyber Terrorist Attacks in Ports

The risk analysis can be carried out correctly in order to prevent a cyber terror attack against a port. Security risk analysis consists of three main components: risk management, risk assessment and risk communication [31]. Risk management consists of establishing the basic principles of risk policy, determining the position of risk management within the organizational structure and determining the planning, coordination, information and control processes in order to support the senior management [32]. In the risk assessment, the scope of cyber terrorism risk that can be encountered in the port is identified and the types and consequences of the emergence are evaluated. Risk communication also focuses on how to share risk information among parties [33].

Once the risk has been analyzed, it is necessary to create a cyber security plan in order to prevent terrorist acts in ports from being carried out by cyber attacks. The plan determines the actions that will ensure the security of the systems used in all kinds of services, transactions and data provided in information technologies, prevent the realization of the risk or, if any, ensure that the effects are kept to a minimum and that the system will return to normal as soon as possible [34].

As in Figure 3, while creating the cyber security plan, it is necessary to create a network that works in coordination with each other, covering the minimum security requirements needed by port operation processes, ISPS security plan and ISM ship safety management.

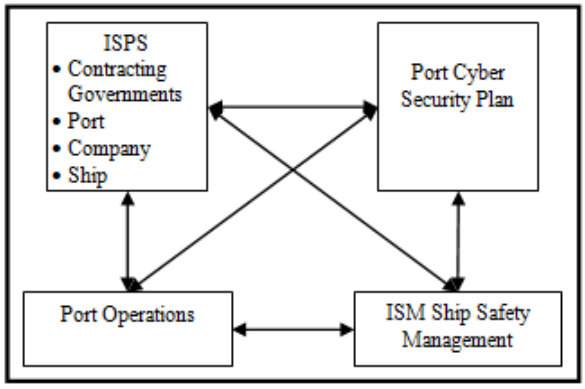

Fig. 3 Cyber security network in ports

Port operation processes mainly cover quay, yard and hinterland operations. Berth operations include guidance, tugboat, ship loading and unloading operations; quay operations include storage, documentation and handling of cargo, import, export and transit and hinterland operations cover the off-port distribution of cargoes [35]. Operational activities are performed within the framework of safety and security standards. With ISPS Code, it is aimed to detect and evaluate security threats and to take preventive measures against security threats affecting ships and port facilities used in international trade [36]. In order to meet ISM ship safety management requirements, safety and environmental protection policy, risk analysis and preventive measures are established. The authority and responsibility of the company,

the authorized personnel in the company, the responsibility of the captain and the resources are determined.

The issues to be considered when creating a port cyber security plan can be listed as follows [37].

- Making risk analysis of information communication technologies,
- Using preventive safety measures in ports and ships to reduce the risks in the IT systems to an acceptable level,
- Determining internet access security policy for ship operations,
- Determining the use policy of removable storage devices such as USB external memory, external disk, cd, dvd,
- Determining employees' wireless network connections and access policy,
- Setting a policy for maintenance and updating of information communication systems,
- Determining the limits of remote access authorization for system display and maintenance,
- Preparing a contingency plan for information communication technologies and systems,
- Determining cyber action management process like detecting, reporting, evaluation and decision, response, improvement, and lessons learned,
- Providing employees with awareness training on cyber security risks and controls.

The correct construction of the plan depends on the internal functioning of the port and its interaction with the external environment. It also depends on the integration of ISPS and ISM regulations and the coverage of security measures specific to cyber attacks, and the main determinant is the implementation of the cyber security plan.

V. Application of Cyber Security Plan in Port Operations

Ports are open systems. The systems that consist of various parts working together and in an environment, which interact with and within themselves, are defined as open systems [38]. At the same time, ports are organizations that have wide range of operations. An organization is a social structure with unique resources and characteristics that have certain purposes [39]. The organizational structure of a business is usually divided on the basis of its functions [40]. The organizational structure of the ports is generally divided into functional sections as in the example in Figure 4. Accordingly, the personnel or the unit responsible for port security may be included in the safety and security department.

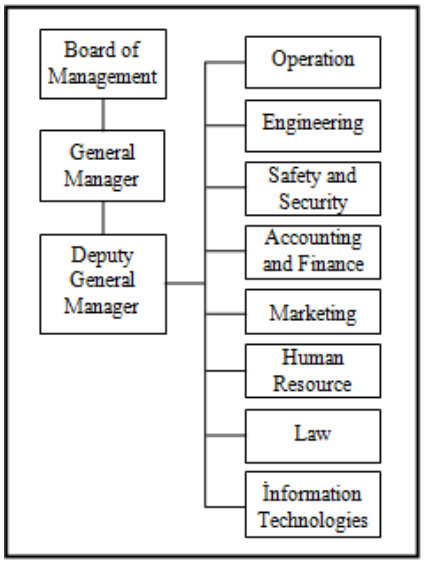

Fig. 4 Example of a port organization chart

Operation planning requires a systematic and comprehensive approach [41], [42]. The personnel in the port operation department follow up the business processes with support from software programs. According to the information provided by the IT and security experts working in the ports, the ship file and work order are created for each ship in these software programs and stored on a server. The ship file is accessible to all parties involved in the operation of the work orders. In such a case, a cyber attack can be made to the network, the data in the files that are open to share can be deleted or altered, etc. and it will cause erroneous work orders to be sent to hand terminals. If the attack is noticed, operations are paused until the system is fixed. However, in cases where the attack is noticed but the system will take a long time to recover, the operations are carried out manually by the employees. Communication between the center and the field is provided by radio communication and every work order is done on paper. Switching to a manual operation as a result of a cyber attack can make the port vulnerable to terrorist attacks. Especially at night, fog, rainfall and so on. Terrorist operations in the port area may not be noticed during the operations performed in weather conditions.

Due to all possible hazards, the cyber security network needs to be managed correctly in order to be functional. This management process is carried out by the safety and security department at the port. The port security department carries out its security-related business processes in coordination with other parts of the port, third parties engaged in port and public institutions, and organizations. First of all, safety standards and plans are determined according to ISPS. Possible threats are identified; countermeasures are taken; infrastructure and superstructure elements as well as vehicles and equipment in the harbor are secured. All loading and unloading operations related to the ship are inspected. Preventive measures are taken for software and hardware that may create cyber security threats. The computers used for this purpose are encrypted and / or anti-virus programs are used. Stored and used data is backed up at regular intervals. The database is backed up both on the server and on machines that do not have an internet connection, or on disks that are not sharable.

The security of the information infrastructure can be ensured by applying ISO 27001 Information Security

Management System which is regulated by International Standards Organization (ISO). In addition, daily work processes are carried out in a structure with protective security measures. The port entries of the personnel are made with the entry card defined for them and the entry of unauthorized persons is prevented. Safety and security training is provided to the employees of the port personnel and the third party enterprises in the port. Continuous and accurate communication between all departments is vital. The content and operation of the plan are checked at specific intervals and the content is updated if necessary.

VI. CONCLUSION

Intensive use of cyber technologies in business processes also brings about new security problems. Terrorist forces in particular also benefit from information and communication technologies. For this reason, the possibility of terrorist attacks against ports can be realized through cyber attacks. In order to prevent cyber attacks and related terrorist acts in ports, firstly risk analysis is needed and a cyber security plan specific to the functioning of the port is needed according to results of the analysis.

Considering the software-supported virtual environments provided by today's technology, there is no inconvenience to bring the "cyber" prefix in front of all of these security initiatives. With this prefix, the concept of war, which could only target soldiers and military facilities in the past, has spread to all units of society, and it is common to continue cyber activities even in peace conditions.

The sources of cyber threats consist of people with software knowledge and people are targets again. These threats try to affect individuals via attacks on social networks and personal web pages. Also, cyber threats target society with state structures that have smart infrastructure such as corporate web pages, e-government, e-bank and e-health. This effect covers all components of port security and at different levels. This situation, naturally; it concerns all structures of maritime transport in general and port security in particular.

Therefore, it is assessed that following are needed:

- Structuring a strategy and action planning in a highly flexible manner with serious foresight studies.
- Establishing an organization to prevent cyber-threatening activities with a supranational organization and defining responsibilities on a sub-component basis very clearly.
- Ensuring that the necessary legislations are structured and updated on a national and international level in a manner that will not create any vacancy and that also protects the rights and freedoms of the people.
- Designing all necessary software, primarily critical software, using national resources and software discipline.
- Designing various levels of trainings in order to increase cyber security awareness in both the institutional and individual levels and creating cyber security awareness.

REFERENCES

[1] Z. Ş. Öğüz, "Güvenli yönetim sisteminin donatanın yükle ilgililere karşı sorumsuz olduğu haller üzerindeki etkisi," *İstanbul Üniversitesi Hukuk Fakültesi Mecmuası*, vol. LXI, pp. 327-337, 2003.

[2] S., Clarke. (2015) Risk Insights Ports and Terminals: The Growing Threat of Cyber Risks. [Online]. Available: https://www.millerinsurance.com/~/media/Files/Publications/Risk%20Insights%20for%20Ports%20and%20Terminal%20owners/M03413%20MTL%20Newsletter%200415%20v4.ashx

[3] A. N. Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, İstanbul, Turkey: Nobel, 2015.

[4] D. C. Alexander, "Cyber threats against the north atlantic treaty organization (NATO) and selected responses," *İGÜ Sosyal Bilimler Dergisi*, Vol 1, pp. 1-36, Oct. 2014.

[5] K. Geers, *Strategic Cyber Security*, Tallin, Estonia: CCD-COE, 2011.

[6] *Information technology - Security techniques - Guidelines for cybersecurity*, ISO/IEC 27032:2012(E), 2012.

[7] F. Wamala, "The ITU National Cyber Security Strategy Guide," International Telecommunication Union, Geneva, 2012.

[8] S. Ruffle and T. Evan, "Cyber terrorism: assessment of the threat to insurance," Univ. of Cambridge, Cambridge, UK, 2017.

[9] D. Bieda and L. Halawi, "Cyberspace avenue for terrorism," *Issues in Information Systems*, vol. 16 (3), pp. 33-42, 2015.

[10] M. Convay, "Cyberterrorism: the story so far," *Journal of Information Warfare*, vol. 2 (2), pp. 33-42, 2003.

[11] G. Weimann, *Terror on the Internet: The New Arena, the New Challenges*, Washington, DC: United States Institute of Peace Press, 2006.

[12] J. White, *Terrorism: An Introduction*, Pacific Grove, CA: Brooks/Cole, 1991.

[13] S. Goodman, J. C. Kirk, M. H. Kirk, "Cyberspace as a medium for terrorists," *Technological Forecasting & Social Change*, vol. 74 (2), pp. 193-210, Feb. 2007.

[14] M. Zerzri, "The Threat of Cyber Terrorism and Recommendations for Countermeasures," Center for Applied Policy Research (CAP) Perspectives on Tunisia, No. 04-2017, 2017.

[15] B. Collin, "The future of cyberterrorism: the physical and virtual worlds converge," *Crime & Justice International*, vol. 13 (2), pp. 15-18, Mach 1997.

[16] P.W. Brunst, *A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications: Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet*, M. Wade and A. Maljevic, Ed., London, UK: Springer, 2009.

[17] K. C. Desouza and T. Hensgen, "Semiotic emergent framework to address the reality of cyberterrorism," *Technological Forecasting and Social Change*, vol. *70* (4), pp. 385-396, May 2003.

[18] S. Gordon and R. Ford, "Cyberterrorism," *Computer & Security*, vol. 21 (7), pp. 636-647, Nov. 2002.

[19] D. E. Denning, "Cyberterrorism," *Global Dialog*, vol. 2 (4), pp. 29-37, Autumn 2000.

[20] Ali Polat, *Uluslararası Ticarette Risk Yönetimi*, İstanbul, Türkiye: İTO Yayınları, 2008.

[21] M. Yorulmaz and S. Birgün, "Lojistik yetenekler üzerine literatür araştırması ve deniz ulaştırma lojistiği hizmet yeteneklerinin belirlenmesi," *The Journal of Academic Social Science*, vol. 4 (25), pp. 313-331, March 2016.

[22] UBAK. (2013) Ulaştırma Denizcilik ve Haberleşme Bakanlığı Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. [Online]. Available:https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FSayfalar%2FBTDNewFolder%2FSiber+G%C3%BCvenlik%2F2_1_Strateji+Eylem+Plan%C4%B1+2013-2014.pdf

[23] W. Price, "Reducing the risk of terror events at seaports," *Review of Policy Research*, vol. 21 (3), pp. 329-349, 2004.

[24] P. Burnson, "Defining threats finding solutions for cyber attacks," *Logistics Management*, vol. 54 (7), pp. 46-50, June 2015.

[25] A. Ekşi, "KBRN terörizminde risk değerlendirmesi ve yönetimi," *Uluslararası Sosyal Araştırmalar Dergisi*, vol. 9 (42), pp. 1489-1498, Feb. 2016.

[26] P. T. Leach. (2015) Marine insurers worry about their ability to meet obligations if catastrophe strikes a mega vessel. [Online]. Available: https://jocdigital.uberflip.com

[27] IMO. (2002) Guidelines for the Onboard Operational Use of Shipborne Automatic Identification System. [Online]. Available: https://www.navcen.uscg.gov/pdf/AIS/IMO_A_917(22)_AIS_OPS_Guidelines.pdf

[28] M. Dwyer, "Cybercrime - is it a threat to Australia's marine industry," *Austmarine Magazine*, vol. 37 (7), p. 22, June 2015.

[29] J. S. Szyliowicz, "International transportation security," *Review of Policy Research*, vol. 21 (3), pp. 351-368, May 2004.

[30] D. Walsh, "Maritime Cyber Security: Shoal Water Ahead," U.S. *Naval Institute Proceedings Magazine*, vol. 141 (7), p. 88, 2105.

[31] M. G. Burns, *Logistics and Transportation Security A Strategic Tactical and Operational Guide to Resilience*, Boca Raton, FL: CRC Press, 2016.

[32] Ş. Aydeniz, *İşletmelerde Gelecek ve Opsiyon Sözleşmeleri ile Risk Yönetimi*, İstanbul, Turkey: Arıkan, 2008.
[33] J. Arvai and L. Rivers, *Effective Risk Communication*, New York, NY: Routledge, 2014.
[34] UBAK. (2015) 2016-2019 Ulusal Siber Güvenlik Stratejisi. [Online]. Available:http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf
[35] J. Luo, Y. Wu and A. B. Mendes, "Modelling of integrated vehicle scheduling and container storage problems in unloading process at an automated container terminal," *Elsevier Computers and Industrial Engineering*, vol. 94, pp. 32-44, 2016.
[36] IMO, *ISPS Code 2003 Edition*, London, UK: IMO Publications, 2003.
[37] A. G. Bermejo. (2015) Maritime cyber security using ISPS and ISM codes. [Online]. Available:http://www.he-alert.org/en/utilities/search .cfm
[38] İ. Akat, G. Budak and G. Budak, *İşletme Yönetimi*, İzmir, Turkey: Barış, 1999.
[39] T. Koçel, *İşletme Yöneticiliği*, 16th ed., İstanbul, Turkey: Beta, 2015.
[40] C. Çetin and L. Arslan, *Temel İşletmecilik*, 6th ed., İstanbul, Turkey: Beta, 2016.
[41] H. Kişi, R. Fışkın, E. Uçan, C. Şakar, E. Çakır, A. Y. Kaya and T. A. Gülcan, "Limanlarda operasyonel planlama: Türk limanlarının mevcut durumu üzerine bir çalışma," *Journal of ETA Maritime Science*, vol. 3 (1), pp. 37-46, 2015.
[42] B.J.Thomas, *UNCTAD Monographs on Port Management*, Cardiff, Galler: United Nations, 1985.