Journal of the Korean Society of Marine Engineering, Vol. 41, No. 8, pp. 738~745, 2017
J. Korean Soc. of Marine Engineering (JKOSME)
https://doi.org/10.5916/jkosme.2017.41.8.738

ISSN 2234-7925 (Print)
ISSN 2234-8352 (Online)
Original Paper

Improving cyber security awareness in maritime transport : A way forward

Young-Chan Lee[1] · Sang-Kyun Park[2] · Woo-Kun Lee[3] · Jun Kang†

(Received September28, 2017 ; Revised October18, 2017 ; Accepted October23, 2017)

Abstract: It is believed that maritime shipping trade has considerable impact on the global economy because 90% of international trade is carried out by maritime transportation. A merchant ship incident can not only cause casualties but also result in ports being shut down, shipping routes being blocked, other ships being damaged, and potential theft. Most ship equipment and systems are computer- and internet-based, and are susceptible to cyber threat by hackers. Cyber-attacks are increasingly common in present times; some examples are the NotPetya attack on A.P. Moller-Maersk, the infection of Australian customs service and immigration, and North Korea attacking GPS signals of vessels on the Korean coast. Unfortunately, seafarers are often unable to fathom the extent of damage that a cyber security attack can cause to a ship. The International Maritime Organization does not deal with cyber security. SOLAS, STCW, and ISPS provide security only against physical threats such as pirates. However, in accordance with resolution MSC.428 (98), the document of compliance of a shipping company requires a cyber threat management system to be included in the approved safety management system, from 1st of January, 2020. The concept of security in the maritime field is defined in SOLAS chapter XI-2, ISPS code (A/8.4, B/8, B/15), and a chapter of STCW convention, although at present it only addresses security threats related to piracy. This paper proposes a method to improve cyber security awareness in maritime transport by introducing the definition of cyber security into the ISPS code, to facilitate a change of security concepts for ships.

Keywords: Maritime transport, Cyber security, Merchant ship, International convention for the safety and life at sea (SOLAS), International convention on standards of training, certification and watchkeeping for seafarers (STCW)

1. Introduction

More than 90% of international trade is conducted via sea transportation, and hence the maritime freight-forwarding industry accounts for the largest portion of the shipping industry **[1]**. Most maritime navigation equipment and devices, including the engine machinery system mounted on a ship, is computerized. Such installations are mostly connected to the internet and tele-communication systems **[2]**. Merchant ships are used in a considerable proportion of the trade all over the world, and such vessels are designed and operated using computers and the Internet., making them vulnerable to cyber-attacks. If a ship faces a cyber-attack when it is in close proximity to a coastal area or in harbor, the attack can result in serious problems throughout the area **[3]**. As an example, ports on the US West Coast were shut down owing to a labor stoppage during January2015 **[4]**, which had a severe impact on the economy. A.P. Moller-Maersk, the world's largest shipping company, reported that the NotPetya wiper malware attacks of late June 2017 would cost it hundreds of millions of U.S. dollars in losses. In its 2/4 earnings report, Maersk executives predicted losses between $200 and $300 million USD. They commented that this lost revenue was due to "significant business interruption" because the company was forced to temporarily close critical systems infected with the malware **[5]**. Equipment and devices exposed to cyber threats on a ship are AIS, LRIT, internet-connected IT system, DSC, man-in waters beacons, information-sharing among USB devices, and interworking (lack of separation) between communication

† Corresponding Author (ORCID: http://orcid.org/0000-0002-1797-4878): Division of Marine Engineering, Korea Maritimeand Ocean University, 727, Taejong-ro, Yeongdo-gu, Busan, 49112, Korea, E-mail: junkang@kmou.ac.kr, Tel: 051-410-4281
1 Division of Marine IT Engineering, Korea Maritime and Ocean University, E-mail: yclee@kmou.ac.kr, Tel: 051-410-4661
2 Division of Marine IT Engineering, Korea Maritime and Ocean University, E-mail: skpark@kmou.ac.kr, Tel: 051-410-4579
3 Future Policy Planning Team, Korea Institute of Maritime and Fisheries Technology, E-mail: lwk@seaman.or.kr, Tel: 051-620-5826

devices. Additionally, the equipment exposed to cyber threats in the port is AIS, VTS, industrial control system, and IT office equipment connected to the Internet. ECDIS, GNDSS, electronic charts, and eLoran can also be detected **[6]**. Cyber-hacking incidents occurred in the shipping cargo operation system operated by Australia customs service and immigration (2012) **[7]**. Drug traffickers hacked the Antwerp port of Belgium to control ship locations and movement of containers **[8]**. North Korea used the Lori-mounted device to block GPS signals on the Korean coast for 16 days in early 2012 causing 1016 aircraft and 254 vessels to be confused **[9]**. According to the survey implemented by IHS Market and BIMCO in July 2016, 65 respondents of the total 300 stakeholders in the maritime industry have experienced a cyber security threat. Among these, 77% were attacked with malware, 57% with phishing, 25% with a theft of credentials, and 23% with spear phishing **[10]**. Such cyber-attack incidents are possible owing to an increasing use of computer-based navigation equipment and devices in bridge, machinery in engine room, and ignorance of seafarers about cyber security. Taking into account the recent cyber-attack incidents, the International Maritime Organization recommends referring to the shipping-related cyber security guidelines developed by BIMCO in April, 2016 **[11]**. In order to act in accordance with national cyber security guidelines, the maritime safety committee agreed to develop a new circular, MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management, in place of MSC.1/Circ.1526, which was developed on the guideline of BIMCO **[12][13]**. The BIMCO guideline recommends three guidelines to address the technical aspects on cyber security such as IEC 61162-450:2011, Maritime navigation device and radio communication equipment and systems - Digital interfaces - Part 450: Multiple talkers and multiple listeners - Ethernet interconnection, ISO/IEC 27001: 2016 standard (Information technology security techniques) and framework for improving critical infrastructure cybersecurity of NIST **[11]**. Pursuant to resolution MSC.428 (98), the DOC of a shipping company requires a cyber threat management system to be in the approved safety management system in order for the approval of the DOC in all annual surveys conducted after 1st of January, 2020 **[14]**. The security in maritime field, however, deals with only pirates in SOLAS chapter XI-2, ISPS code (A/8.4, B/8, B/15), and the chapter of the STCW convention.

There are no requirements of competence of cyber security awareness for a seafarer and an employee of a shipping company in IMO provisions. This paper proposes to develop the competence of cyber security in the STCW convention.

2. International Maritime Organization's Position on Maritime Cyber security

While cyber threat is becoming a hot issue in the international maritime field, MSC 96 approved the interim guidelines on maritime cyber risk management (MSC.1/Circ.1526) and requested FAL 41 to review them **[13]**. In FAL 39, Canada proposed marine cyber security enforcement measures to be included in ISPS in the MSC regimes. However, the security review in terms of international trade promotion will be carried out by FAL **[15]**.

In MSC 94, the United States and Canada proposed strengthening cyber security in a variety of maritime sectors including ports, maritime facilities, and shipping logistics systems **[16]**.

In MSC 95, NGOs such as ICS and BIMCO introduced the development of the ship cyber security guideline in an urgent and industrially-oriented manner. Some countries (USA, Canada, and Korea, etc.) expressed opinions on the necessity of the integrated guideline on maritime security to be premature **[17]**.

In FAL 40, Canada and the United States submitted documents on the measures to address vessel-cyber-related threats (FAL 40/9) and submitted draft MSC 96/4 guidelines on shipboard risk management at MSC 96**[18]**. MSC 96 approved the interim guidelines on maritime risk management on the assumption that it could be modified at FAL 41, and MSC and FAL jointly issued guidance on security aspects of international trade facilitation at FAL 41 **[19]**.

In MSC 97, Iran submitted a document stating that the cyber risk management guidelines should be submitted, but it has been decided to discuss the draft guidelines currently approved by MSC 96 after reviewing them at FAL 41**[19]**. The document provides functional elements (identification, protection, detection, response, and recovery) for managing maritime cyber risk and provides reference a document * for an advanced case such as guidelines on cyber security on-board ships by BIMCO, ISO/IEC 27001 standard, and NIST Framework. It emphasizes that cyber risk management should be initiated by the senior management and absorbed by all organizations, and this guidance should be a high-level recommendation and not a mandatory one. The FAL 41 committee confirmed that the MSC 96 and 97 already reviewed MSC.1/Circ.1526 on the maritime cyber risk management manual containing security-related aspects in terms of trade facilitation and agreed to inform the outcome of the meeting to MSC 98 **[19]**.

In MSC 98, a document was submitted to the Secretariat to request that the French Cyber Risk Management Manual be

added as a best practice to Chapter 4 (Best Practices for Implementing Cyber Risk Management) of the Interim Guidelines on Maritime Cyber Risk Management (MSC.1/Circ.1526). The United States proposed that the risk management of a ship's cyber risk should be included with the management of the whole cyber-related risks in the safety management system of the ISM code. The application and definition of risk assessment is quite broad in regulation 1.2.2.1 of the ISM code and it is appropriate to include the concept of cyber risk management in it. In the ISM code, the purpose of the safety management of the workplace is to define the evaluation and the security measures for all identified risks to the ship, personnel, and environment **[19]**. It is possible to assess whether cyber risk management has been carried out properly when business sites conduct internal and external evaluations of ISM code. To integrate the parts of safety management system of the ISM code and cyber-related risk management, a standardized guidance should be developed through evaluation by relevant experts, and necessary evaluation methods and strategies should be developed. As a result of the discussion, it has been decided to include maritime cyber risk management as a functional requirement of the Safety Management System (SMS) of the ISM Code **[20]**. The 98th MSC Committee agreed to include maritime cyber management in the ISM Code, but decided to include it in the form of a non-mandatory recommendation, and encouraged to reflect this in the Resolution (MSC Resolution). In the MSC resolution, it has been decided to write the implementation date of marine cyber risk management at the time of issuance of the Safety Management Certificate (SMC) from January 2021 onwards. However, it is a mandatory issue at 98 MSC **[20]**.

3. Vessel facilities Vulnerable by Cyber Attacks

When a cyber-attack occurs, it is necessary to prepare an action plan for emergency situations in order to recover and protect the ship information and stop it from spreading. Ways and procedures to mitigate cyber threats should be reflected on ship management system in accordance with ISM code. The procedures should be developed by the feedback circle as shown in **Figure 1**.

Figure 1 shows how cyber security should be maintained and operated as identification threats, identification vulnerabilities, assessment risk exposure, development of protection and detection means, establishment of contingency plan, and action to cyber security incidents **[11]**.

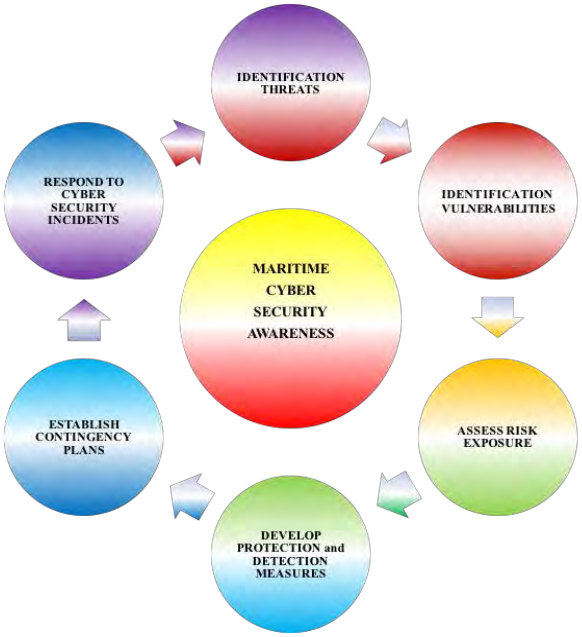

Figure 1: Whole Scheme of Maritime Cyber Security Awareness **[11]**

In the area of maritime transportation, cyber-attacks are of 5 categories such as safety navigation, radar, AIS, satellite, and cargo tracking system. Cyber technology threatened by hackers at sea consists of GPS spoofing, AIS and ECDIS.

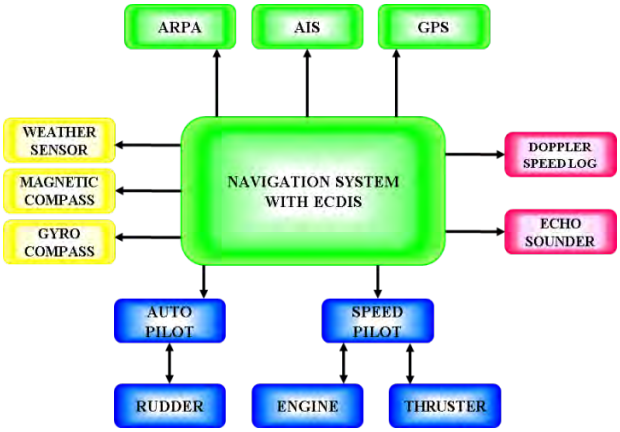

Figure 2: Block diagram showing the relationship between sensors, actuators, and the ECDIS on an integrated bridge system **[6]**

3.1 Attacks to Automatic Identification System

The AIS is a safety navigation equipment used for collision avoidance on-board a ship for communicating course, speed, ship type, cargo type, ship status either at-anchor or underway, and other necessary safety information at sea. The AIS installation allows marine officers to acquire useful navigation information of other ships.

Vulnerabilities in the AIS are widely known through a research, Trend Micro Forward-looking Threat Team. The team could recreate a frequency of VHF, which is a threat defense group that focuses on the technology sector. It was able to reproduce a VHF frequency on AIS.

Such technological experiments could newly generate a virtual ship in AIS with a false course, heading, speed, ship registration flag, vessel's name and wrong weather condition. Wrong weather influences the distress signal in ships to move to another place or change to other routes.

The press recognized the unlawful transportation of Iranian ship crude oil, subjected to navigating from Iran to East Asia in 2012.

The research team was aware that three Iranian ships with Tanzanian flag pretending to go to Syria attempted the avoidance of boarding and inspection of the containers for international legal sanctions. Iranian Oil Company falsified its AIS data and then, immigration officials denied Iranian vessels **[11]**.

3.2 GPS jamming and spoofing

GPS is an essential technology that provides valuable information related to safe navigation while sailing at sea. Spoofing is an attacking behavior that bypasses access control by accessing the system as if it were an authorized user, or by impersonating an authorized address on the network **[6][11]**.

Spoofing uses a medium consisting of a port, an access control address, an Internet Protocol (IP) address, and an e-mail (e-mail) address for disguising the identity purposely for intentional actions.

The Jamming is the act of disrupting or disturbing the communication system by detecting the propagation and frequency of the ship. In other words, it refers to electronic or mechanical interference that interferes with the display of radar and radio communications. The ship tracking system with autopilot equipment is shown in **Figure 3 [6]**.

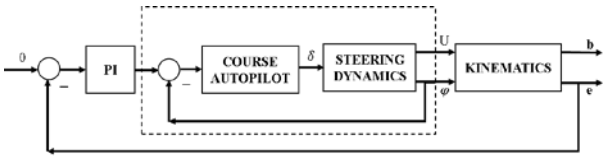

Figure 3: Ship tracking system with an autopilot system

Ship dynamics formulation is defined by NOMOTO model,

$$T\dot{r} + r = K\delta + rb \quad (1)$$

where T is the time constant of the ship, K is the rudder gain (1/s), δ is the rudder angle (rad), r is the ship's turning rate (rad/s), and rb is parameters of environment disturbances (rad/s).

The kinematics equation of the ship is defined as

$$\dot{\varphi} = r \quad (2)$$

$$\dot{x} = U\cos\varphi + d_x \quad (3)$$

$$\dot{y} = U\sin\varphi + d_y \quad (4)$$

where U is speed of ship against water velocity, x and y are the north and east directions respectively of the ship heading. d_x&d_y are environmental errors due to currents and wind (m/s), φ is radian of heading of the ship. The environment errors are defined as Gauss Markov process with the following formula,

$$\dot{d}_x = -\frac{1}{T_d} d_x + v_x \quad (5)$$

$$\dot{d}_y = -\frac{1}{T_d} d_y + v_y \quad (6)$$

where$T_d$is time constant of the environment error, v_x and v_y are additional white Gaussian noise.

Ship control law is given as

$$\delta(t) = K_i \int_0^t [\varphi_d - \varphi_{(\tau)}] d\tau + K_P[\varphi_d - \varphi_{(t)}] - K_d r(t) \quad (7)$$

K_p, K_i&$K_d$are P, I and D gains, respectively.

Spoofer control law is given by the following equations. Hackers can produce a new spoofing GPS signal (e_m with real position of the ship(e) by b and a. The spoofing error is described by e_s as,

$$e_s = e - e_m \quad (8)$$

The modulated velocity and acceleration of modulated error is shown by the following equations

$$|\dot{e}_m(t)| \le v_{max} \quad (9)$$

$$|\ddot{e}_m(t)| \le v_{max} \quad (10)$$

$\mathbf{e_m(t)}$is end up hacker's goal

$$\min_{u(t)} t_f \quad (11)$$

$$\ddot{e}_m(t) = u(t) \quad (12)$$

$$e_m(0) = 0, \dot{e}_m(0) = 0 \quad (13)$$

$$e_m(t_f) = \bar{e}, \dot{e}_m(t_f) = 0 \quad (14)$$

3.3 Invasion of Central network system of a ship

Central network system on-board a ship consists of many control systems. Signal generated in the vessel allow a marine officer to permit modulated data such as the information of engine propulsion, navigation data, and steering data.

The research team of Texas University invaded the network control system of a ship during its sailing at the Mediterranean in the year 2013. Prior to invasion of the ship, the team noted the ship's captain to take in control of the ship's condition. However, they did not notice when and where the hacking affected the ship. Ship personnel could not recognize the penetration of their automatic navigation system with serious vulnerabilities.

They had ability to drive the ship by rudder control. The hacker used the theory of ship dynamics law, ship control law, and spoofer control law as given by **Equation (1)~ Equation(14)**.

4. Training and Education of Global Maritime Institute on Maritime Cyber Security

4.1 BIMCO

According to The Navigator, magazine of the Nautical Institute, technical officer of BIMCO recommends to cover the maritime cyber security awareness course while designing the cyber training program of maritime institutes in the world as presented in **Table 1[11]**.

Table 1 : Recommended educational contents of BIMCO**[24]**

Steps	Contents
1	Emails dealing in a safe way
2	Use of Internet including social networks
3	Use of individual devices
4	Risk and hazards in installing and operating software
5	Poor security software and data security practices
6	Protection of shipboard personnel information, passwords and electronics-certificates
7	Physical presence of external personnel on equipment and devices without supervision
8	Recognition of suspicious behavior and activity as well as report way in cyber incident
9	Influence of cyber threat and accident.
10	Preventative measures to cyber attacks
11	Process of protecting ship systems

4.2 JWC International

JWC International provides maritime cyber security training program through E-learning. The Institute emphasizes computer-based environmental facilities in ships, specifically related to the bridge system and machineries in engine room. The training course is designed for ship-based and shore-based positions in vessel and shipping company, respectively. In addition, the education program includes assessments after completion. In doing so, seafarers possessing the certificate of cyber security competence are qualified. **Table 2** lists the contents of maritime cyber security training in JWC as follows **[21]**.

Table 2: Contents of maritime cyber security training in JWC **[21]**

Steps	Contents
1	Malware awareness
2	Phishing & social engineering
3	Passwords
4	The 'Insider Threat'
5	Securing mobile devices & removable media
6	Responsible web surfing & social media habits
7	10 Essential steps to maritime cyber security
8	Real life case studies

4.3 ASPIDA

Table 3 lists the contents of the course in maritime cyber security training provided by ASPIDA, designed for ship personnel, shipping company employees, superintendents, and relevant workers. It focuses on the dangers of cyber security and how they protect and maintain the computer based and communication based facilities as well as more important things such as recognition and reaction to contingency situations caused due to cyber threats. The seafarer would be aware of the existence of threat and vulnerabilities in cyber security on-board a ship through some cases **[22]**.

Table 3: Education Program provided by ASPIDA **[22]**

Steps	Contents
1	General cyber security terminology and categorization
2	Malware, viruses and spyware
3	Identification of theft and compromise of classified data
4	Phishing
5	Dangers associated with emails (dangerous attachments, hoaxes, etc.)
6	Risks regarding removable media
7	USB stick dangers
8	File sharing and copyright issues
9	Dangers related to mobile devices
10	Dangers of unsecured wireless networks
11	Desktop security
12	Social engineering and other human aspects
13	Risks of social networking
14	Unauthorized system access and characteristics of a strong password
15	Risks associated with information, communication, navigation and automation systems on board
16	Case studies & Best Practices
17	Incident response procedures

4.4 CBS

Maritime cyber security course delivered by maritime business and IT managers deals with how hackers infect computer and telecommunication systems, by using case studies and various examples in maritime business and entire work processes. Trainees would be qualified in cyber defenses. The maritime cyber security training course of CBS is presented in **Table 4 [23]**.

Table 4: Contents of maritime cyber security training in CBS **[23]**

Steps	Contents
1	How is “cyber” relevant to the maritime sector?
2	Social engineering
3	Risks from out-of-the-box tools
4	A simulated attack scenario workshop
5	Employees: the first line of defenses
6	Defensive IT
7	Balancing cyber security against business requirements
8	Contingency planning

Under the assumption that the cyber-attacks can happen on any ordinary day, the course participants firstly study their behavioral character in dealing with the cyber security device and facility, as well as the Internet use including opening of an e-mail. The first day of the course focuses on how the cyber hacker works, and stress the strategic defense by understanding the behavior of the attacker. Second day delivers defensive strategies between easy working in facilitation aspect and burden of cyber security, by taking into account emergencies. Second day’s training program does not require any IT technical and academic knowledge and provides actual instances of cyber threats.

The participants would be made aware of cyber risks and threats in maritime field, method of improvement of cyber security through easy technical knowledge, quick awareness of cyber-attacks, identifying ability in emergencies, and the skill of dealing between cyber security and business facilitation.

5. Analysis of Cyber Security in International Maritime Provisions

5.1 SOLAS convention and other related code

When taking into account legislation and evolvement background of security related law and regulation with the 9/11 disaster, the definition “Security incident” in Reg.1 of Chapter XI-2 of the SOLAS convention does not include meaning of cyber risk and hazard. Therefore, before discussing cyber security issue with amendment of the STCW convention, the terminology should be amended with inclusion of cyber risk and hazard. With due respect to ISPS code, the instrument needs to impart proper training to ship security officers in accordance with the B code. Also, all crew assigning security duties should receive appropriate training for ship security responsibilities and duties. The provisions require establishing and maintaining a ship security plan. The contents of cyber security should reflect on ISPS and cyber security training should provide on **[24][25]**, because the ship personnel encounter cyber-attacks.

5.2 STCW convention and its model course

Not only Section A-Ⅵ/5 of STCW convention describes the proficiency of a ship security officer, Section A-Ⅵ/6 of STCW convention also requires qualifying ship personnel in security-related training such as security-related familiarization training, security-awareness training, and training for designated security duties. These training programs do not contain any cyber security contents and just provide training in physical security in relation to attacks by pirates. This can lead to a cyber threat to a ship, ship personnel, ship to ship, and ship to port. With such STCW convention, cyber security related model course for competence of seafarer in IMO analyzed on model course 3.19 ship security officer, 3.20 company security officer, 3.26 security training for seafarers with designated security duties, 3.27 security awareness training for all seafarers. Accordingly, after the chapter A-Ⅵ/6 of STCW convention was first amended in term of cyber security, a 4-model course should be modified **[26]**.

6. Proposals

This paper is only regarding the competence of cyber security for seafarers on-board a ship and does not deal with cyber risk management with a focus on training program. Hence, in order to implement cyber related regulations, the definition of cyber security is included in regulation 2.1.4.1 of 2 definition of Part A of ISPS code. This definition says: “Cybersecurity” is one of the tool, practices, policy, safety concept, technologies, and process designing for protecting network system, computers, programs and its data from intended or unintended attack, damage, contaminated program, or unauthorized use, access, or modulation **[27]**.

This paper proposes the competence of cyber security for all seafarers as familiarization training in Section A-Ⅵ/6 of STCW convention. Seafarers should be sufficiently qualified in their capacity on board ship for cyber security before assigning the duties.

The following contents should be included in,

1. Type and principle of cyber threat
2. Kind of a cyber attack
3. Technology of target system, networks and equipment
4. Assessment of a cyber risk
5. Way to reduce a cyber risk
6. Development of contingency plan: and
7. Best practices with actual accident

7. Conclusion

Considering that most international trade is conducted via maritime transportation, maritime shipping trade has a significant impact on the global economy. There is a saying that transport is meat and drink to cyber criminals. That means it is very vulnerable to cyber-attack. Seafarers are unable to fathom the extent of damage that a cyber security attack can cause to a ship. Currently, the International Maritime Organization does not consider measures for cyber security. SOLAS, STCW, and ISPS provide guidelines only for physical security threats such as pirates. However, in accordance with resolution MSC.428 (98), the DOC of a shipping company requires cyber threat management systems to be included in the approved safety management system from 1st of January, 2020. As of now, security in the maritime field is defined only in terms of security measures for dealing with pirates, as given in SOLAS chapter XI-2, ISPS code (A/8.4, B/8, B/15), and a chapter of STCW convention.

In section 3, this paper described essential cyber security measures that should be undertaken on a ship. It explored how a ship navigation facility interconnects, and, as an example of a cyber threat, how hackers fabricate GPS signals.

In addition, this paper reviewed contemporary maritime cyber security training courses, referred to development of cyber security programs, and proposed a way forward to improve cyber security awareness in maritime transport with an introduction of the definition of cyber security into the ISPS code for changes in security concepts on-board ship, as described in section 6.

References

[1] Overview of the International Shipping Industry, http://www.pfri.uniri.hr/~bopri/documents/01c_Shipping_and_world_trade.pdf, Accessed June 22, 2017.

[2] What Marine Communication Systems Are Used in the Maritime Industry, https://www.marineinsight.com/marine-navigation/marine-communication-systems-used-in-the-maritime-industry/, Accessed May 05, 2017

[3] Elias. Bou-Harb, E. I Kaisar, and M Austin, “On the impact of empirical attack models targeting Marine transportation,” 5th IEEE International Conference on Models and Technologies for Intelligent Transportation System(MT-ITS), pp. 200-205, 2017.

[4] The National Impact of a West Coast Port Stoppage, https://nrf.com/sites/default/files/Port%20Closure%20Full%20Report.pdf, Accessed September 11, 2017.

[5] Maersk Shipping Reports $300M Loss Stemming from NotPetya Attack, https://threatpost.com/maersk-shipping-reports-300m-loss-stemming-from-notpetya-attack/127477/, Accessed July 10, 2017.

[6] J. Bhatti and T. E. Humphreys, “Covert control of surface vessels via counterfeitcivil GPS signals,” Semanticscholar, pp. 1-10, 2015. [Online] Available:https://pdfs.semanticscholar.org/6f20/450b32b71f2454e63292acb632d3619ee8ef.pdf.

[7] Maritime Industry is Easy Meat for Cyber Criminals, https://www.kaspersky.com/blog/maritime-cyber-security/8796/, Accessed May 17, 2017.

[8] Police Warning after Drug Traffickers' Cyber-attack, http://www.bbc.com/news/world-europe-24539417, Accessed July 5, 2017.

[9] North Korea interfering with GPS signals in South Korea as China relations deteriorate , http://www.telegraph.co.uk/news/2016/04/01/north-korea-interfering-with-gps-signals-in-south-korea-as-china/, Accessed September 13, 2017.

[10] 2016 cyber security survey in association with BIMCO, https://cybersail.org/wp-content/uploads/2017/02/IHS-BIMCO-Survey-Findings.pdf, Accessed July 5, 2012.

[11] The Guidelines on Cyber security onboard ships, http://www.liscr.com/sites/default/files/online_library/Guidelines_on_cyber_security_onboard_ships_version_1-1_Feb2016%283%29.pdf, Accessed August15, 2012.

[12] International Maritime Organization (IMO), MSC-FAL.1/Circ.3, “GUIDELINES ON MARITIME CYBER RISK MANAGEMENT,” 2017.

[13] International Maritime Organization (IMO), MSC.1/Circ.1526, “INTERIM GUIDELINES ON MARITIME CYBER RISK MANAGEMENT,” 2016.

[14] International Maritime Organization (IMO), MSC.428(98), “MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS,” 2017.

[15] International Maritime Organization (IMO), FAL 39/7,

"Measures toward enhancing maritime cybersecurity," 2014

[16] International Maritime Organization (IMO), MSC 94/21, "REPORT OF THE MARITIME SAFETY COMMITTEE ON ITS NINETY-FOURTH SESSION,"2014.

[17] International Maritime Organization (IMO), MSC 94/22, "REPORT OF THE MARITIME SAFETY COMMITTEE ON ITS NINETY-FITTH SESSION," 2015.

[18] International Maritime Organization (IMO), FAL 40/9, "GUIDELINES ON THE FACILITATION ASPECTS OF PROTECTING THE MARITIME TRANSPORT NETWORK FROM CYBERTHREATS," 2016.

[19] International Maritime Organization (IMO), FAL 41/17, "REPORT OF THE FACILITATION COMMITTEE ON ITS FORTY-FIRST SESSION," 2017.

[20] International Maritime Organization (IMO), MSC 98/23, "REPORT OF THE MARITIME SAFETY COMMITTEE ON ITS NINETY-EIGHTH SESSION," 2017.

[21] JWC International, https://www.becyberawareatsea.com/resources, Accessed August 9, 2017.

[22] Aspida Cyber security, https://www.becyberawareatsea.com/resources, Accessed August 9, 2017.

[23] Maritime Cyber Security and Big Data, https://cbs-executive.dk/en/programme/maritime-cyber-security-and-big-data/, Accessed August 9, 2017.

[24] International Maritime Organization (IMO), MSC 96/WP.9, "Report of the Working Group," 2017.

[25] International Maritime Organization (IMO), SOLAS Convention, 2017.

[26] IMO, STCW Convention & Codes, Manila Amendments 2011 / STCW Code Part A, 2015.

[27] International Maritime Organization (IMO), ISPS Code, 2017.