DEMONSTRATING THE CYBER VULNERABILITIES OF SIGNIFICANT MARITIME TECHNOLOGIES TO THE PORT FACILITIES AND ON BOARD OF VESSELS

Karim Mohamed Ali Aboul-Dahab

The Graduate School of Business (GSB), The Arab Academy for Science, Technology and Maritime Transport, Cairo, Egypt,

National Telecom Regulatory Authority, Smart Village, kmohamed@tra.gov.eg

Keywords: Cyber Risk Management, operational technology (OT), Cyber Security Onboard Ships, International Safety Management Code(ISM)

ABSTRACT: Ships are increasingly using systems that rely on digitization, digitalization, integration, and automation, which call for cyber risk management on board. As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together – and more frequently connected to the internet. In 2017, the International Maritime Organization (IMO) adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management System (SMS). The Resolution stated that an approved Safety Management System SMS should take into account cyber risk management in accordance with the objectives and functional requirements of the International Safety Management (ISM) CODE. The IMO encourages administrations to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021. This paper presents Guidelines on Cyber Security Onboard Ships that are aligned with IMO resolution MSC.428 to asses companies to identify risks arising from the use of IT and OT onboard ships and establish appropriate safeguards against cyber incidents, The aim of this study is to analyze cyber vulnerabilities of significant maritime technologies to the port facilities and on board of vessels , Evaluates the different frame works and guidelines on maritime cyber risk management to demonstrate the seriousness of maritime cyber threats for national security.

INTRODUCTION

The growth of digitalization and the connectedness produce pressure on the industry to be more and more connected. Nonetheless, the absolute dependency of systems and equipment regarding interconnectivity operations is creating more vulnerability and representing an increase in opportunities for the cyber-criminal (NEP&I, 2017), the world is relying more on technology than ever before. Numerous applications of technology have become a fundamental part of shipping, providing real information and effective communication around the world, instantaneously. Digital technology has advanced and increased exponentially in recent years; information technology (IT) and operational technology (OT) are more frequently connected to the world wide web than ever before, and the shipping industry cannot escape this reality (IMO, 2018). However, technology is also bringing along certain risks regarding safety and security of shipping operations that could possibly spill over to the economic domain, considering that both

information technology and operational technology are essential for the daily operation and the sustainability of the shipping industry [1]Cybersecurity introduces an additional element into the safety equation: security against deliberate actions intended to cause harm. Security has always been a concern with naval ships, and the military routinely exercise precautions to maintain the security of their ships and offshore assets. Commercial vessels routinely employ special security measures under certain circumstances to prevent theft, piracy, smuggling or stowaways. Those crimes are usually economically motivated, where destruction is not the goal. Acts of terror are usually politically motivated, and ships and offshore assets are prime targets because of their mobility and high potential for causing extensive damage to life, property, the environment, and the transportation and economic infrastructure[2]

IMO Facilitation Committee (FAL) and the Maritime Security Committee (MSC) defined IMO Guidelines on maritime cyber risk management in MSC-FAL.1/Circ.319. Both recognized the urgent need to raise awareness on cyber risk threats and vulnerabilities and to provide high-level recommendations on maritime cyber risk management from current and emerging cyber threats and vulnerabilities, including main areas that support effective cyber risk management (identify, protect, detect, respond and recover).
The shipping industry is moving into the world of digitalization. Big Data analytics, the Internet of things, Cloud computing, Machine learning, Artificial Intelligence are only some of the aspects that will transform the way vessels used to operate. Unmanned autonomous ships are already generating increasing interest in the industry but remote monitoring and control systems on board is already a reality for many companies around the world.

Cybersecurity is not just about preventing hackers gaining access to systems and information, potentially resulting in loss of confidentiality and/or control. It also addresses the maintenance of integrity and availability of information and systems, ensuring business continuity and the continuing utility of digital assets and systems. To achieve this, consideration needs to be given to not only protecting ship systems from physical attack, force majeure events, etc. but also ensuring the design of the systems and supporting processes that are resilient and applying reversionary modes to be available in case of disaster

Ships are increasingly using systems that rely on digitization, digitalization, integration, and automation, which call for cyber risk management on board. As technology continues to develop, information technology (IT) and operational technology (OT) onboard ships are being networked together – and more frequently connected to the internet.

The growing use of big data, smart ships and the "internet of things" will increase the amount of information available to cyber attackers and the potential attack surface to cyber criminals. This makes the need for robust approaches to cyber risk management important both now and in the future [5]

Maritime has fallen victim to multiple cyber-attacks which caused huge financial and operational losses. In 2017 Maersk experienced a destructive attack using the 'NotPetya' ransomware, not because of the nature of the business but because Maersk used specific Ukrainian accounting software targeted by the attackers [15]

In 2012, the major Saudi Arabian state owned oil and gas company, Saudi Aramco, which provides 10 % of the global oil suffered a cyber-attack during Ramadan month. An employee of the company opened a phishing mail with an infected link. According to Abdullah al-Saadan, vice president for corporate planning of Aramco, the primary intention behind this attack was to stop the flow of oil and gas to the international and national market (Reuter, 2012).

In April 2012, the Danish Maritime Authority was subjected to a cyber-attack. However, it was not until 2014 that the Administration discovered the attack. The attack was simply introduced by a Pdf document infected with a virus, and the virus was propagated from the Danish Maritime Authority to other government institutions before it was discovered in 2014 (Linton, 2016). Sensitive information from Danish shipping companies and merchant navy fell into the hands of hackers.

In August 2011,The Islamic Republic of Iran Shipping Lines (IRISL), an Iranian state-owned shipping company, fell victim to a cyber-attack.33 Lars Jenson, founder of CyberKeel ,reported, "The attacks damaged all the data related to rates, loading, cargo number, date and place … resulting in severe financial losses [8]

Despite of the increase of the cyber-attacks during the last few years, there is still a need for raising the awareness of the probable damaging that cyber-attacks could cause to the shipping companies, vessels, ports and maritime administrations and its further effect in the economic performance.

This paper is organized as follows, The first section gives a brief overview of the maritime cyber security, The second section analyze the different vulnerabilities to the cyber threats in the port Facilities and on the board of vessels, In the third section the paper presents the different Guidelines and frameworks on maritime cyber risk management, Our conclusions are drawn in the final section

Literature Review;

Maritime Cyber Security MCS is a combination of the two terms 'maritime security' and 'cyber security'. The first term; maritime security, has been argued to have no definite meaning, and subsequently relates to different concepts depending on the individuals attempting to make sense of it, or practice it.[10]

IMO Resolution MSC.428(98) identifies cyber risks as specific threats, which companies should try to address as far as possible in the same way as any other risk that may affect the safe operation of a ship and protection of the environment.

cyber security could be generally defined as "the measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack" .In other words, the objective of cybersecurity is a stable condition, where cyberspace is trusted and protected. At this point, there is also sufficient capacity to proactively control and sustain cyber threats[5]

Cyber risk management could be defined as "the process of identifying, analyzing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders [3]

Risk management is the ongoing process of identifying, assessing, and responding to risk. To manage risk organizations should understand the likelihood that an event will occur and the potential resulting impacts. With this information organizations can determine the acceptable level of risk for achieving their organizational objectives and can express this as their risk tolerance.[6]

Port facility: is a location where the ship/port interface takes place; this includes areas such as anchorages, awaiting berths and approaches from seaward, as appropriate, [Regulation(EC) No 725/2004].

Port: is a specified area of land and water, with boundaries defined by the Member State in which the port is situated, containing works and equipment designed to facilitate commercial maritime transport operations, [Directive2005/65/EC].

The topic of cybersecurity within the maritime industry is as dynamic as any other sector of business. The industry's global reach, large volume of capital transactions, extensive use of commercial services, and reliance on information technology create significant opportunities for exploitation through the cyber domain , Security threats have evolved from coastal piracy to complex smuggling operations, transnational organized crime, and terrorism. Safety risks have likewise evolved as merchant shipping progressed from sailing ships to ships driven by coal-fired steam boilers, to diesel engines and most recently to liquefied natural gas. Waterfront operations

evolved from break bulk cargo to containerization, with sophisticated systems now controlling the movement and tracking of containerized and liquid cargo

Nowadays, implemented security solutions within the ports areas aim to achieve the desired security levels through the implementation of a network of active sensors (high-resolution cameras, IR barriers, biometric fingerprint reader, microphone cable, etc.), subsystems functional (vehicular video, license plate reading and container codes units, video over IP, turnstiles, automatic barriers, metal detectors, baggage scanners, radar, etc.) and passive protection systems (metal fences, etc.) for control and protection of the different port areas (perimeter gates of vehicular / pedestrian access, cruise terminals, parking lots, docks, electrical substations, etc.). Although the above security network seems well structured, the use of modern technology is not enough. With regard to the ENISA report on cyber security challenges in the Maritime Sector seems evident that cyber threats are a growing menace, spreading to all industry sectors that are relying on ICT systems.[21]

Cyber Security on Port Facilities

Ports are extremely important to the government entities that operate them for three reasons: 1) ports are a major source of direct and indirect employment in their local economies; 2) the fees from port operations generate large direct and tax revenue streams for its owners; 3) population centers including the nation's largest cities have naturally formed around ports, ensuring their interest in keeping the ports' flow of commerce uninterrupted and ensuring the safety of these high population density areas.

The growth of digitalization and the connectedness produce pressure on the industry to be more and more connected. shipping companies, vessels ,ports and terminals tend to install similar software to load ,unload and track cargo , the absolute dependency of systems and equipment regarding interconnectivity operations creates more vulnerability and representing an increase in opportunities for cyber-crimes ,so the vulnerability of a one single software installed could cause significant damages to other vessels, ports, terminals and shipping companies consequently.

The data handled by the Maritime Administration contains a large amount of detailed information, valuable to various maritime stakeholders. The system used by the maritime administration can be exposed to cyber espionage by other states, whose aim is to obtain access to sensitive data that can be used for their own purposes [1]

The port operation is very complex because of the nature of the services provided, the number of processes taking place in this infrastructure and the large number of workers involved in the operation which includes land, sea and economic activities. To ensure the smooth flow of the operation, it is necessary to enhance physical and cyber security measures. The International Ship Port Facility Security Code (ISPS) presents a clear legislation on implementation and maintenance of port security measures. It includes specific procedures and designates tasks and responsibilities, such Port Security Plan, Port Security Officer and Port Facility Security Officer, covering ship and port facility operations.[1]

Port facilities are becoming increasingly complex and dependent on the extensive use of information and communications technologies at all stages of their lifecycles. Some of this technology is embedded in the fixed and mobile assets used to operate the port; other elements may be remotely located such as the systems used to schedule vessel and cargo movements, Security threats have evolved from coastal piracy to complex smuggling operations, transnational organized crime, and terrorism. Safety risks have likewise evolved as merchant shipping progressed from sailing ships to ships driven by coal-fired steam boilers, to diesel engines and most recently to liquefied natural gas. Waterfront operations evolved from break bulk cargo to containerization, with sophisticated systems now controlling the movement and tracking of containerized and liquid cargo [15]

GPS technology, coupled with geographic information system (GIS) software, is a key to the efficient management and operation of automated container placement in the world's largest port facilities. GPS facilitates the automation of the pick-up, transfer, and placement process of containers by tracking them from port entry to exit. With millions of container shipments being placed in port terminals annually, GPS has greatly reduced the number of lost or misdirected containers and lowered associated operation costs, the most likely GPS maritime threat scenarios could be Jamming of a port or other congested waterway by an individual or small group of non-state actors using small, portable jammers

The most likely GPS maritime threat scenarios to consider include: Jamming of a port or other congested waterway by an individual or small group of non-state actors using small, portable jammers. Rapid movement of these individuals, coupled with intermittent use of the jammer(s) would make it very difficult for local law enforcement officials to track and arrest the per GPS is playing an increasingly important role in the management of maritime port facilities. [19]

According to the European Union Agency for Cybersecurity (ENISA) the main challenges currently facing the port facilities to implement cybersecurity measures are the following:

1-Lack of digital culture in the port ecosystem 2- Lack of awareness and training regarding cybersecurity: 3- Lack of time and budget allocated to cybersecurity: 4- Lack of human resources and qualified people regarding cybersecurity matters. Also the port facilities infrastructure should

be able to 1- Identify threats to assets and infrastructure in order to establish and prioritize security measures.2-Identifying ,selecting and prioritizing of measures and procedural changes and their level of acceptance in reducing vulnerability 3-Identifying the weaknesses including human factors, policies and procedures 4- Identifying of premier protection, access control and personal clearance requirements for access to restricted areas of the port 5-Identifying the port perimeter and the appropriate measures for access control 6-Identifying the nature of the expected traffic.[18]

Cyber Security on board of vessels

In 2007 The International Maritime Organization (IMO) issued a voluntary performance standard for Integrated Navigation Systems (INS) which recommended to include the following devices;

- The Electronic Position Fixing System (EPFS), providing the absolute position of the vessel (for example Global Positioning System (GPS)).
- Heading Control System (HCS), which enable the ship to keep a preset heading, known as autopilot.
- Speed and Distance Measurement Equipment (SDME), providing the speed of the vessel (and thus distance).
- The ECDIS, used for chart presentation and presentation of relevant information for the navigator.
- RADAR system, used as a mean for terrestrial positioning.
- AIS, automatic tracking system used on ships and by vessel traffic services (VTS).
- Echo sounding system (ESS), providing the depth measurements for the vessel.
- Conning application providing information about the engine and manoeuvring status.
- Information distribution on Local Area Networks (LAN) and presentation of information on Multi-Function Displays (MFDs).
- Use of Communication channels such as Global Maritime Distress Safety System (GMDSS), which uses for example the NAVTEX to receive navigational messages, or other communication channels for distributing data such as satellite communication (SATCOM) or mobile broadband.

Today's mariners rely heavily on networks, systems, and outside sources for navigation. Many significant cyber threats are the result of vulnerabilities in equipment carried and used by the maritime industry worldwide. Equipment vulnerable to cyberattacks includes navigation systems.[14]

The GMDSS (Global Maritime Distress and Safety System), and other advanced system used are rapidly increasing connectivity to the internet ,The connected devices include the navigational system(NAVTEX ,Inmarsat C), communication system (Inmarsat and Iridium satellite constellation), tracking system AIS (automatic identification system), Search and Rescue Radar Transponders (SART), The International Maritime Organization through The International Convention for the Safety of Life At Sea (SOLAS), Regulation V/19, 20 and 27 requires carrying onboard an AIS and ECDIS and requires having a receiver for a global navigation satellite system (GPS).

A cyber-attack on a GMDSS system devices could manipulate the ship information details such as cargo, position and speed or sending false warnings, alarms and distress signals, jamming or disruption on any of these essential navigation systems becomes a severe problem that can affect the maritime industry, Cyber-attack on vessels are very dynamic depending on cargo, geographic position, shipborne technology and competence of the crew.

The maritime vessels have become especially reliant on GNSS technology , The vast majority of vessels now rely on (GNSS) which could be spoofed or blocked causing disrupt of navigation, , GNSS signals could be vulnerable to the following threats ;Jamming and Interference by broadcasting a stronger signal that intentionally or unintentionally blocks or impacts a GNSS satellite signal. Spoofing by broadcasting a false GNSS signal, but at a slightly greater power which could deceives the GNSS receiver into locking onto the spoofed signal, Meaconing by causing intentional delay and rebroadcast of a GNSS signal intended to introduce error to receivers.

Vulnerabilities in the AIS system are widely known. For example, a study conducted by the Trend Micro Forward-looking Threat Team, a threat defense group that focuses on the technology sector, was able to recreate a VHF frequency on AIS that simulated a "ghost ship" in a harbor and alerted nearby vessels they were on a collision course with another vessel[13]

One of the most cost-effective counter measures to defend against the intentional or unintentional jamming of GNSS signals is crew training [19]

The continuous development on new GPS receivers that can identify non-GPS signals by their relative location (jamming and spoofing signals come from the terrestrial locations not satellites) and their strength (jamming and spoofing signals must by necessity be stronger than GPS satellite- generated signals). In addition to receiver signal strength alarms and specialized antennas, the effects of intentional jamming could be mitigated through the use of inertial navigation systems (INS) and radio frequency (RF) jamming detectors. However, at this point in time it is unclear when such equipment would be available to and employed by the commercial industry, or how much it will cost.[19]

The BIMCO's guidelines recommended the following Cyber risk management actions to act with resilience to cyber-attacks: 1- identify the roles and responsibilities of users, key personnel, and management both ashore and on board 2- identify the systems, assets, data and capabilities, which if disrupted, could pose risks to the ship's operations and safety 3- implement technical measures to protect against a cyber-incident and ensure continuity of operations. This may include configuration of networks, access control to networks and systems, communication and boundary defense and the use of protection and detection software 4-implement activities and plans (procedural protection measures) to provide resilience against cyber incidents. This may include training and awareness, software maintenance, remote and local access, access privileges, use of removable media and equipment disposal 5- implement activities to prepare for and respond to cyber incidents.

Cyber Security policy formulation

IMO has issued MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management The guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities and include functional elements that support effective cyber risk management.

The IMO identified five functional approaches as the basis for Cyber risk management;

1 Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations. .2 Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations. .3 Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner. .4 Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.

The Maritime Safety Committee, at its 98th session in June 2017, also adopted Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems. The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

The National Institute of Standards and Technology (NIST) brings "NIST Framework" which is widely used as approach to cyber security assessment, as well as a step towards the fulfillment of cyber risk management. The advantage of "NIST framework" lies in its universality and

flexibility, which is why it can be employed in many industries, including the maritime one (National Institute of Standards and Technology NIST, 2018)

The National Institute of Standards and Technology (NIST) introduced the NIST Framework which has been used enormously as a cyber-security assessment also as a way of fulfillment of cyber risk management.

For the same purpose the Baltic and International Maritime Councils (BIMCO) in (BIMCO, 2017) rely on publications of NIST and IMO. The BIMCO's attitude is published as „Guidelines on Cyber Security Onboard Ships". BIMCO approaches to cyber risk problems through the following items: 1-identification of threats and vulnerabilities, 2-assesment of risk exposure, 3-development of protection and detection measures, 4-establishment of contingency plans to respond and recover upon a cyber- security incident[10]

Cyber Security Risk Assessment Models

Cybersecurity researchers have adopted the CIA model which defines three security objectives that describe the general trustworthiness of the data.

Confidentiality

Data confidentiality is the action of preserving authorized restrictions on information access. It is the property that personal privacy and proprietary information are not made available or disclosed to unauthorized individuals, entities, or processes. This goal of the CIA triad emphasizes the need for information protection.

Integrity

Data integrity is the property that defines whether data is correct, true and unaltered. In information security, securing the integrity of the data means preserving their accuracy and completeness during all stages of the production, communication, storage and retrieval of the data. A potential loss of integrity means unauthorized modification or destruction of information.

Availability

Data availability is the degree to which data is accessible when it is required. Typically this is a concern when an application is making use of communications or storage that is provided as a service outside the direct control of the application.[4]

The National Institute of Standards and Technology (NIST) developed the NIST Framework as a guidance for cyber-security assessment, the frame work was based on existing standards, guidelines, and practices, for critical infrastructure organizations to efficiently manage the cybersecurity risk , the frame work consists of five concurrent and continuous Functions:

1) Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
2) Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
3) Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
4) Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
5) Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event"

The guidelines on maritime cyber risk management" (MSC-FAL.1/Circ.3) introduced by the IMO accepted the NIST framework with the five key elements identification, protection, detection, response, and recovery
According to (Dennis Bothur et al ,2017) the cyber security policies should address and explain at least the following:

- Data recovery capability, backups, redundancy, business continuity and disaster recovery planning
- Administrator privileges, concepts of least privilege and the separation of duties
- Remote access control, use of encryption and Virtual Private Networks (VPN)
- Physical access, removable media controls, "Bring your own device" (BYOD)
- Acceptable personal use of IT systems
- Email, phishing, passwords rules
- Software upgrade, patch, and maintenance schedules
- Anti-virus/-malware software and signature updates
- White- or blacklisting and the use of third party software
- Onshore support and contingency planning
  Equipment disposal, and data destruction[20]

Victor Bolbot et al 2019 implemented a risk assessment for the navigation and propulsion systems of an inland autonomous vessel ,The study implemented the Cyber Preliminary Hazard Analysis (CPHA) method to an autonomous vessel , The CPHA better described the relevant hazardous scenarios by incorporating the potential attack type and the relevant hazardous Consequences, The CPHA also seems to be more realistic than the STRIDE and MaCRA methods cause it is not limited to certain types of attacks. [12]

Conclusions

This paper has investigated the cyber vulnerabilities of significant maritime technologies and evaluated the different frame works and guidelines on maritime cyber risk management.

Port facilities are becoming increasingly complex and dependent on the extensive use of information and communications technologies at all stages of their lifecycles, GPS technology, coupled with geographic information system (GIS) software, is key to the efficient management and operation of automated container placement in the world's largest port facilities. GPS facilitates the automation of the pick-up, transfer, and placement process of containers by tracking them from port entry to exit.

The main challenges currently facing the port facilities to implement cyber security measures are 1-Lack of digital culture in the port ecosystem 2- Lack of awareness and training regarding cyber security: 3- Lack of time and budget allocated to cyber security: 4- Lack of human resources and qualified people regarding cyber security matters:

The maritime vessels have become especially reliant on GNSS technology , The vast majority of vessels now rely on (GNSS) which could be spoofed or blocked causing disrupt of navigation, GNSS signals could be vulnerable to the following threats ;Jamming and Interference by broadcasting a stronger signal that intentionally or unintentionally blocks or impacts a GNSS satellite signal.
Addition of a safety system verifying the safety of the automatic navigation control system actions, Sanity checks and filter application for the GPS signals measurements, addition of anti-interference antennas, Encryption for the VHF signals is required .

The guidelines on maritime cyber risk management" (MSC-FAL.1/Circ.3) introduced by the IMO accepted the NIST framework with the five key elements identification, protection, detection, response, and recovery

The Baltic and International Maritime Councils (BIMCO) in 2017 published a "Guidelines on Cyber Security Onboard Ships". BIMCO approaches to cyber risk problems through the following items: 1-identification of threats and vulnerabilities, 2-assesment of risk exposure, 3-development of protection and detection measures, 4-establishment of contingency plans to respond and recover upon a cyber- security incident.

REFERENCES

1. David Miranda Silgado, "Cyber-attacks: a digital threat reality affecting the maritime industry, world maritime university, Malmo Sweden , 2018.
2. ABS Cyber Safety, "cybersecurity implementations for the marine and offshore industries ," American Bureau of Shipping Incorporated by Act of Legislature of the State of New York 1862, September, 2016 .

3 Hugh Boyes, Roy Isbell and Alexandra Luck, "Code of Practice Cyber Security for Ports and Port Systems,"

4 The Institution of Engineering and Technology, 2016. Sotiria Lagouvardou., Maritime Cyber Security concepts, problems and models, 3rd ed., technical university of Denmark , Master thesis, 2018.

5." BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL " The guidelines on cyber security onboard ships, Version 3.0

6." Jenna Ahokas1, Tuomas Kiiski1, Jarmo Malmsten1, Lauri Ojala1 " Cyber security in Ports: a Conceptual Approach, 2017.

7.National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity", April 16, 2018.

8.Christopher R. Hayes, NAVAL POSTGRADUATE SCHOOL MONTEREY, CALIFORNIA, June 2016, "Maritime Cyber Security :The future of national security", June, 2016.

9.MDR Cyber, "Stormy seas ahead Cyber-security guidance for the maritime industry"

10.Ivan Mraković, Ranko Vojinović, "Maritime Cyber Security Analysis – How to Reduce Threats?", June, 2019.

11.Odd Sveinung Hareide, Øyvind Jøsok, Mass Soldal Lund ,Runar Ostnes and Kirsi Helkala, "Enhancing Navigator Competence by Demonstrating Maritime Cyber Security", Journal of Navigation April, 2018.

12.Victor Bolbot, Gerasimos Theotokatos, Evangelos Boulougouris and Dracos Vassalos "Safety related cyber-attacks identification and assessment for autonomous inland ships", Maritime Safety Research Centre, University of Strathclyde UK, 2019.

13.Operational Analysis Division "CONSEQUENCES TO SEAPORT OPERATIONS FROM MALICIOUS CYBER ACTIVITY", National Protection and Programs Directorate Office of Cyber and Infrastructure Analysis ,USA, 2016.

14.Christopher R. Hayes , NAVAL POSTGRADUATE SCHOOL MONTEREY ,MARITIME CYBERSECURITY: THE FUTURE OF NATIONAL Security, , CALIFORNIA, June 2016

15.MDR Cyber, "Stormy seas ahead Cyber-security guidance for the maritime industry

16.The U.S. Government Publishing Office (GPO),EXAMINING PHYSICAL SECURITY AND CYBERSECURITY AT OUR NATION'S PORTS,2017

17. European Union Agency for Cybersecurity (ENISA), PORT CYBERSECURITY Good practices for cybersecurity in the maritime sector, November 2019

18. Fivos Andritsos , European Commission, Joint Research Centre and Institute for the Protection & Security of the Citizen ,"Port Security & Access Control A systemic approach", July 2013
19. Dr. Joe DiRenzo III, Dr. Nicole K. Drumhiller, Dr. Fred S. Roberts "ISSUES IN MARITIME CYBER SECURITY",July-2017
20. Dennis Bothur, Guanglou Zheng, Craig Valli,A CRITICAL ANALYSIS OF SECURITY VULNERABILITIES AND COUNTERMEASURES IN A SMART SHIP SYSTEM, 2017
21- Andrea Chiappetta ,Critical Infrastructure Protection Beyond The Hybrid Port And Airport Firmware Security ,Cyber Security Applications On Transport , Conference: 2017 5th IEEE International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS), DOI: 10.1109/MTITS.2017.8005666