UNIVERSITY OF PIRAEUS

DEPARTMENT OF MARITIME STUDIES

POSTGRADUATE STUDIES

M.Sc. Course Shipping Management

CHALLENGES OF THE ISPS CODE IN THE GLOBAL SECURITY DOMAIN

Panagiotis Souliotis

MND18039

A Master's thesis presented

to the Department of Maritime Studies

in partial fulfillment of the requirements

for the Master's degree in Shipping Management

Piraeus

September 2019

Δήλωση Αυθεντικότητας / Copyright Declaration

Το άτομο το οποίο εκπονεί τη διπλωματική εργασία φέρει ολόκληρη την ευθύνη προσδιορισμού της δίκαιης χρήσης του υλικού, η οποία ορίζεται στη βάση των εξής παραγόντων: του σκοπού, του χαρακτήρα της χρήσης (εμπορικός, μη κερδοσκοπικός, ή εκπαιδευτικός), της φύσης του υλικού που χρησιμοποιεί (τμήμα του κειμένου, πίνακες, σχήματα, εικόνες ή χάρτες), του ποσοστού και της σημαντικότητας του τμήματος, που χρησιμοποιεί σε σχέση με άλλο κείμενο υπό copyright, και των πιθανών συνεπειών της χρήσης αυτής στην αγορά ή στη γενικότερη αξία του υπό copyright κειμένου.

I declare that this master's thesis has been composed by myself, that the work contained herein is my own except where explicitly stated otherwise in the text, and that this work has not been submitted for any other degree or professional qualification.

Σεπτέμβριος / September 2019

Τριμελής Εξεταστική Επιτροπή

Η παρούσα Διπλωματική Εργασία εγκρίθηκε ομόφωνα από την Τριμελή Εξεταστική Επιτροπή που ορίστηκε από το ΓΣΕΣ του Τμήματος Ναυτιλιακών Σπουδών του Πανεπιστημίου Πειραιώς σύμφωνα με τον Κανονισμό Λειτουργίας του Προγράμματος Μεταπτυχιακών Σπουδών στη Ναυτιλιακή Διοικητική.

Τα μέλη της Επιτροπής ήταν:

Ιωάννης Λαγούδης (Επιβλέπων)

Ιωάννης Θεοτοκάς

Μαρία Καρακασνάκη

Η έγκριση της Διπλωματικής Εργασίας από το Τμήμα Ναυτιλιακών Σπουδών του Πανεπιστημίου Πειραιώς δεν υποδηλώνει αποδοχή των γνωμών του συγγραφέα.

Acknowledgments

I would like to express my sincere appreciation to my supervisors who really helped me to prepare this thesis. Without their support, I would never have been able to finish it. First, I am grateful to my wise teachers for their support, advise and patience. I would also like to extend my sincere thanks to all those who provided me with invaluable data/information.

Special thanks are extended to my family for being patient, supportive and encouraging all along my research and preparation of this thesis. I am also grateful to the Hellenic Navy, for the experience and knowledge I gained during my soon-to-end career as a naval officer.

Last but not least, I must not omit to express my gratitude to my beloved mother who passed away recently so suddenly, sinking us all into grief, and take this opportunity to bid her my fondest farewell.

ABSTRACT

The sea is a vast space that has always been exposed to a wide range of threats. Even more so nowadays, with many terrorist, piratical and cyber-attacks taking place in the oceans, open seas and port facilities, which cannot adequately be prevented or addressed by conventional military/security forces or other means. Thus, mariners today are exposed to risks when operating at ports or on-board vessels. Against this background and with a view to enhancing security, the International Maritime Organization (IMO) has developed a comprehensive set of requirements and guidelines, the International Ship and Port Facility Code – ISPS Code.

The ISPS Code requires that flag states, ships and all organizations engaged in the maritime industry, tighten their security gates. While this certainly has positive effects, including higher security levels, efficiency, effectiveness and competitiveness, it also includes costs in terms of increased operational expenses, administrative work and staffing demands.

The primary objective of this paper is to demonstrate how the ISPS Code is dealing with the aforementioned threats, what sort of challenges the maritime security faces and how the physical and cyber security are affected. Moreover, focusing on cyber security in particular, the paper will attempt to identify any existing gaps and recommend necessary corrective and streamlining steps to address them.

From the discussion, it becomes evident that the ISPS Code has achieved more in the field of traditional threats, resulting in a significant decrease of piratical incidents in the so-called Horn of Africa. In this respect, the ISPS by its nature has proved to be an effective protective shield against any illegal actions related to security matters. On the other hand, the cyber security field seems to have emerged as a brand-new field in security assessment, planning and policy making, as numerous and diverse cyber threats render the maritime industry more vulnerable. In this regard, the ISPS Code, and not only, still seems to be in a premature (experimental) stage, with no solid and tangible results yet.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

ABS	American Bureau of Shipping
AIS	Automatic Identification System
APM	Automatic Performance Management
ARPA	Automatic Radar Plotting Aid
BIMCO	Baltic and International Maritime Council
BMP	Best Management Practice
CLIA	Cruise Lines International Association
dGPS	Differential GPS
DoS	Denial of Service
ECDIS	Electronic Chart Display and Information system
EU	European Union
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
HRA	High Risk Area
ICC	International Chamber of Commerce
ICS	International Chamber of Shipping
IG P&I Clubs	International Group
IMB	International Maritime Bureau
IMO	International Maritime Organization
INTERCARGO	International Association of Independent Cargo Owners

INTERTANKO	International Association of Independent Tanker Owners
ISM Code	International Safety Management Code
ISPS Code	International Ship Port Facility Security Code
IT	Information technology
IUMI	International Union of Marine Insurance
LPG	Liquefied Petroleum Gas
LRIT	Long-Range Identification and Tracking
NATO	North Atlantic Treaty Organization
OCIMF	Oil Companies International Marine Forum
OT	Operational technology
PCASP	Privately Contracted Armed Security Personnel
PRC	Piracy Reporting Center
RADAR	Radio Direction and Ranging
RCC	Rescue Co-ordination Centers
SMS	Safety Management System
SSA	Ship Security Assessment
SOLAS	Safety of Life at Sea
UK	United Kingdom
UN	United Nations
US	United States
USB	Universal Serial Bus
VDR	Voyage Data Recorder
VTC	Vessel Traffic Services

1. INTRODUCTION

1.1 BACKGROUND

Merchant shipping extends essential services to people by carrying the majority of goods and commodities all over the globe. In 2005, the shipping industry transported 7 billion tons of cargo between 160 countries. Ships, the industry's main assets, are physically mobile, and international flags allow shipping companies to choose their legal jurisdiction and with it their tax and financial environment (Stopford 2009, p. 48). However, merchant shipping often operates in an inhospitable environment, in which mariners are exposed to natural challenges such as extreme weather conditions, but also human-caused adversities, such as piracy, maritime terrorism and cyber-crime, which pose increasingly serious threats to maritime security, affecting crews, cargoes and vessels.

Maritime security is broadly conceived as a task beyond national boundaries. According to an official report by the UN Secretary General in 2008, international cooperation together with coordinated responses is of paramount importance. The same report underlines the need to share the burden of responsibility amongst nations and states and moreover highlights the emergence of the so-called "Collective Security" concept. NATO, the EU, the US and the UK similarly highlight in their strategic plans and policies the significance of multilateral/joint coordinated responses and efforts in this direction. There are several factors which certainly lead to this way of collective responding, including the transnational character of maritime security threats and maritime insecurity consequences. In this regard, we should always have in mind that pirates, for example, act across maritime territorial boundaries and that global shipping and trade is in its own nature transnational and complex, involving a wide variety of national actions and competences (Bueger 2014, p. 163).

As a recently much talked-about term within the maritime community, "maritime security" refers to the security of the maritime domain and can be further understood as a complete set of practices, policies and regulations, intended to secure this domain against all types of threats. Maritime security has long been one of the most significant concerns for the

international maritime community. Surprisingly, however, it was not until the beginning of the 2000s that the term "maritime security" became fairly common in any discussions and debates, despite the fact that particular incidents had already occurred, like that of the vessel "City of Poros" in the summer of 1988.

From 2002 onwards, academic and other references to maritime security have considerably increased in numbers (Fig. 1). There is of course an explanation for that, based on the combination of the following three major factors: (a) the 9/11 New York terrorist attacks, which raised awareness of security issues in general; (b) the undertaking of three high-visibility terrorist acts against ships (USS Cole in 2001, French tanker Limburg in 2002 and Filipino passenger ship Super-Ferry 14 in 2004); and (c) the significant increase of piratical incidents in the Malacca Straights at the outset of the century. Moreover, extensive academic debates were largely kindled after the surge of piracy at the Horn of Africa throughout the years between 2007 and 2012. These debates were standing beyond strictly strategic and security studies, engaging scholars, subject-matter experts and professionals from various sectors and disciplines, dwelling upon the social, cultural, legal, economic, military, energy, environmental and other dimensions of piracy and maritime security (Germont 2015, p. 54).

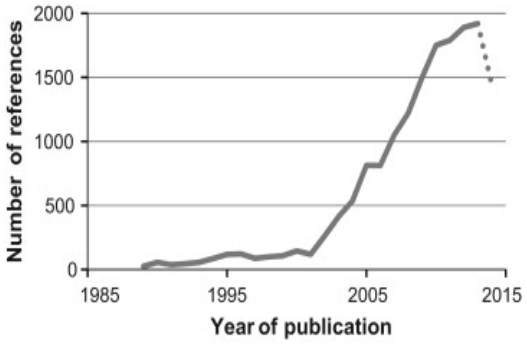

Fig. 1. Evolution between 1989 and 2014 of the number of academic publications mentioning 'maritime security', ***Source***: Google Scholars search

Maritime security has to deal with two completely different domains. The first one refers to the threats listed below, which arise from (illegal and disruptive) human activities in the maritime context, that is to say within a certain geographically limited space. Thus,

different states are differently impacted by maritime security threats, depending on their actual geographical location. For example, in the case of illegal immigration by sea, Greece is more directly impacted than (for instance) the Netherlands, because of its geographical location. This domain affects the physical security of the shipping industry. For the purpose of this thesis, even though some threats will be discussed next, we will focus mainly on piracy.

On the other hand, there is another "brand new" threat that has emerged globally and affects the shipping industry. It is not restricted by geographically borders or any other physical barriers. Undoubtedly, this sort of intangible threat is the cyber-threat, stemming from the ***Cyber-security*** domain.

In response to these developments and concerns, in December of 2002, the twenty-second session of the Assembly of the IMO agreed on the development of a new package of measures, relating to the security of ships and port facilities for adoption by a Conference of Contracting Governments to SOLAS (Safety of Life at Sea). In the second non-mandatory section (Part B) of the International Ship and Port Facility (ISPS) Code, a number of resolutions were adopted by the conference, aiming at streamlining specific amendments, enforcing the implementation of certain security measures on ships and harbor facilities not included in the Code and paving the way for more work on the subject in the future. The Code was published in 2003 and came into force on 1 July 2004 in a speedy manner.

In general terms, maritime security concerns in today's world encompass piracy and armed robbery against ships, maritime terrorism, stowaways, illegal immigration and smuggling at sea, as well as other security-related issues. The possible threats are adequately outlined in the ISPS Code, which extends far beyond the common perception that it is an anti-terrorism instrument. Part B, Paragraph 8.9 of the Code states the following:

"The SSA [ship security assessment, which is an essential and integral part of the process of developing and updating the ship security plan and includes for example identification of existing security measures and possible threats] should consider all possible threats, which may include the following types of security incidents::

- damage to, or destruction of, the ship or of a port facility, e.g. by explosive devices, arson, sabotage or vandalism;

- hijacking or seizure of the ship or of persons on board;
- tampering with cargo, essential ship equipment or system or ship's stores;
- unauthorized access or use, including presence of stowaways;
- smuggling weapons or equipment, including weapons of mass destruction;
- use of the ship to carry those intending to cause a security incident and/or their equipment;
- use of the ship itself as a weapon or as a means to cause damage or destruction;
- attacks from seaward whilst at berth or at anchor; and
- attacks whilst at sea."

All the above threats could be considered as tangible, and more or less any liabilities arising by such incidents are covered by specific clauses in insurance policies (Pagonis and Pentheroudakis 2019, p. 118).

Taking a look at the latest EU and UK maritime security strategy official texts, we can see that the term "maritime security risks" is more commonly used instead of the term "maritime security threats", and some of the above threats are grouped together. For instance, the UK National Strategy for Maritime Security describes one of these risks as the "disruption to vital maritime trade routes as a result of war, criminality, piracy or changes in international norms" (UK National Strategy for Maritime Security 2014, p. 19). It also adds to this list by including "cyber-attacks against shipping or maritime infrastructure".

Lately, the IMO has recognized the urgent need to raise awareness on cyber risk threats and vulnerabilities in order to support safe and secure shipping, which is operationally resilient to cyber risks (MSC-FAL.1/Circ.3, 5 July 2017).

1.2 AIM

The aim of this paper is to demonstrate how the ISPS is dealing with the aforementioned threats, what challenges maritime security faces and how physical and cyber security are affected. Moreover, focusing on cyber security in particular, the paper will attempt to identify any existing gaps and recommend necessary corrective and streamlining steps to address them. To this end, we will gather, line up and assess all relevant and available

data with regard to particular security risks and challenges for the maritime industry. Then, appropriately using this data, we will compile a list of relevant cases in the past, followed by a critical analysis and assessment of the incumbent systems, means of entry and aiming at enhancing awareness and conducting Risk Analysis. By reviewing each case, we will attempt to adequately identify the level of exposure, the vulnerabilities and the entailed eventual consequences for safety, economic and environmental risk to the maritime sector. Moreover, with particular focus on cyber-security, we will outline the cyber-security measures currently in place in the maritime industry. As a wrap-up, a short discussion along with relevant conclusions will take place, utilizing specific expert views and ideas, in an attempt to highlight the importance of cyber-attacks as well as their impact on the maritime industry.

This information is also used to produce a timetable of past cases along with a critical evaluation and analysis of the systems involved, means of entry and consequences of each case, with the aim of increasing awareness and carrying out risk analysis. A theoretical and literature review demonstrates the exposure, vulnerabilities and possible consequences in terms of safety, environmental and economic risk to the maritime sector. Furthermore, the current framework of cyber-security measures introduced in the maritime industry is discussed.

1.3 OBJECTIVES

1.3.1 Create a list of recent cases with detailed information, through a collection of reports, mainly from open sources, such as electronic journals, magazines, reports and articles, related to security incidents in the maritime industry, showing the specific areas affected and the consequences of the attacks, in order to demonstrate the importance of the security measures to the shipping industry.

1.3.2 Collate and analyze data from security incidents so as to highlight any deficiencies and possible ways of enhancing the current framework. This will be accompanied by a critical analysis of the current action taken against threats, tangible or

intangible, showing the relevance of the security system for the maritime industry and the need for new regulations and effective implementation regarding cyber security policy.

1.4 SCOPE OF STUDY AND STRUCTURE

As a sector that includes many stakeholders involved in the development of different processes with regard to network and connectivity, the maritime industry has a wide range of activities. In this regard, the scope of this study is limited to shipping companies, port, maritime administration and ship systems and how the operation of all these is affected by cyber security challenges and direct and indirect security hazards. A general overview of the existing situation will be made, through an analysis of security incidents having taken place during the past few years. Recommendations will then follow, based on current guidance and shipping industry practice in order to adequately address the cyber security risks. The structure of this dissertation includes five chapters:

Chapter 1 provides the introduction with background information, aim, objectives, dissertation structure and scope of the study, as well as the various relevant definitions.

Chapter 2 establishes a theoretical and literature review, which focuses on historical background, exposure, vulnerability of systems supporting the maritime industry and possible consequences generally of attacks in terms of safety, environment and economy.

Chapter 3 demonstrates the investigation development, including the research methodology and risk analysis used in this research.

Chapter 4 presents the results coming from the above research.

Chapter 5 summarizes the findings, and presents the conclusions, thoughts and recommendations obtained via this research.

2. LITERATURE REVIEW

2.1 DEPICTION OF THE ISPS CODE

2.1.1 *OBJECTIVES OF THE CODE*

The International Ship and Port Facility (ISPS) code is aimed to establish an international framework for cooperation. In particular, the main objectives of the Code include:

- establishment of an international framework that fosters cooperation between Contracting Governments, Government agencies, local administrations and the shipping and port industries, in assessing and detecting potential security threats to ships or port facilities used for international trade, so as to implement preventive security measures against such threats;
- to determine the respective roles and responsibilities of all parties concerned with safeguarding maritime security in ports and on-board ships, at the national, regional and international levels;
- to ensure that there is early and efficient collation and exchange of maritime security-related information, at national, regional and international levels;
- to provide a methodology for ship and port security assessments, which facilitates the development of ship, company and port facility security plans and procedures, which must be utilized to respond to ships' or ports' varying security levels; and
- to ensure that adequate and proportionate maritime security measures are in place on board ships and in ports.

2.1.2 *IMPLEMENTATION– REQUIREMENTS*

In order to achieve the above objectives, SOLAS contracting governments, port authorities and shipping companies are required, under the ISPS Code, to designate appropriate security officers and personnel, on each ship, port facility and shipping company. These security officers, designated Port Facility Security Officers (PFSOs), Ship Security Officers (SSOs) and Company Security Officers (CSOs), are charged with the duties of assessing, as well as preparing and implementing effective security plans that are able to manage any potential security threat. IMO is able to provide support to Member States in need of assistance in implementing the Code, by way of national and regional workshops, seminars, needs assessment missions, etc.

Inevitably, the requirement of the freedom of sea lines of communication has risen high not only on the international community agenda, but also within the shipping industry. Most of the times the response of the international community to maritime security challenges includes deployment of Naval forces tasked to secure the freedom of navigation, even if sometimes needs time to be implemented. As far as the maritime industry is concerned, the International Maritime Organization (IMO) at the highest level when it comes to maritime security issues provides support, assistance, and guidance to Member Governments through the implementation of conventions/resolutions, codes, and protocols" (http://www.imo.org/en/ourwork/security/guide_to_maritime_security/pages/solas).

According to the Code, the Company Security Officer (CSO) is responsible for ensuring that a Ship Security Assessment (SSA) is carried out for each ship of the Company's fleet under his responsibility which is subject to the provisions of chapter XI-2 and part A of the Code. The Ship Security Assessment should consider all possible threats, as described above, such as smuggling weapons or equipment, damage or destruction of the ship or of a port facility, e.g. by explosive devices, arson, sabotage or vandalism, hijacking or seizure of the ship or of individuals on board, attacks from seaward whilst at berth or at anchor, and attacks whilst at sea" (ISPS presentation by the Department of Maritime Studies, University of Piraeus).

2.2 *TANGIBLE/TRADITIONAL THREATS*

2.2.1 PIRACY AND ARMED ROBBERY AGAINST SHIPS

Piracy has existed almost as long as shipping and maritime trade. Piracy came to be seen as an interesting historical problem, associated with the skull and crossbones flag, galleons of gold and villains carrying cutlasses with a dash of excitement and even romance. In ancient Greece, piracy seems to have been widespread and widely regarded as an entirely honorable way of making a living, and even during Roman times parts of the Mediterranean were infested with pirates, provoking several naval campaigns to suppress them (Møller 2009, p. 4). It seemed that, by the end of the 19th century, it had already been put under control. The fact that piracy was always a crime, often vicious and usually murderous, was

seemingly forgotten or ignored by people. But piracy had not disappeared. During the 1970s and 1980s, attacks on merchant ships began to increase and became a problem that soon could no longer be ignored (Li 2013). In the years 1999-2002, the International Maritime Bureau of the International Chamber of Commerce (ICC/IMB or IMB) registered a record number of attacks against vessels (Mazaheri and Ekwall 2009, pp. 326-342). Targets of these attacks included most classes of vessels: bulk/general cargo vessels, tankers, container carriers and chemical and LPG carriers. The attacks were concentrated in several distinct geographical areas including the Malacca straits, Indonesian and Malaysian waters, the coasts of Bangladesh and India, the Red Sea/Horn of Africa area and mainly the west coast of Africa. Piratical attacks occur today with an alarming frequency in many parts of the world. Attacks range from incidents in which the pirates have simply taken money and valuables from the crew and ship's safe to cases where the entire cargo has been stolen and in some cases the ship as well. Reports of incidents show that apart from the danger to the crews who are the victims of an attack, the navigational and environmental dangers in cases where the crews have been tied up and the ships have been left to steam at full power with nobody in control while the robbers make their escape can scarcely be exaggerated, especially in areas where there is heavy traffic (Suppiah 2009, pp. 57-72).

2.2.2 TRAFFICKING

Trafficking is one out of everyday crimes found in seaports and maritime domain. It includes trafficking or smuggling of persons, money, drugs, weapons, or other contraband goods. Some smugglers use the proceeds from the trafficking or smuggling to support terrorism. Trafficking is usually connected to piracy and is a criminal activity. As it happens in West-Africa currently and as it also happened some years ago with Somali pirates, hijacking of commercial ships as well as cargo ships and tankers take place, releasing the vessels only after millions of dollars are paid (Kusi 2015, p. 21).

2.2.3 CARGO THEFT

Cargo theft is well paid and occurs day in day out, throughout the world. It was reported in 2010 that the loss as a result of cargo theft in the US was nearly 171 million dollars. Despite the fact that there are no reliable crime statistics on cargo theft locally, even approximately, it was indicated that West Africa countries have the uppermost risk of cargo theft on the entire continent of Africa. Globally, the theft of goods in transit is expected to reach 50 billion dollars a year or more. According to law enforcement agencies, half of the cargo theft cases have not been reported, and if reported, the figure may even exceed 100 billion dollars annually. Sometimes robbery forms part of the tactics used in cargo theft - particularly cargo hijackings (Suppiah 2009).

2.2.4 MARITIME TERRORISM

Terrorism in the maritime environment is not a new phenomenon and arguably not a dramatically growing one. It is one of the oldest of all professions. It is not a matter of concern to one country or a group of countries - it is a global issue. Maritime terrorism has been an adjunct to political and quasi-military campaigns for more than a century now. Maritime terrorism since the end of World War II displays most characteristics common to other areas of terrorism in the period. The fact is still that maritime terrorism precisely mirrors other forms of terrorism in that about 85% of incidents involved bombs or other explosives. The number of reported incidents demonstrates some growth from decade to decade, not all of which can be accounted for by better reporting and analysis. Although terrorist hijacking is not particularly common, it often receives the majority of media speculation and anti-terrorist planning.

The events of “9/11” have jolted the United States and the world to the recognition of how vulnerable the international systems of transportation and trade are to those who would do harm to the world. An event similar to these attacks would have a very serious and long-lasting negative impact on the maritime sector, affecting both to the international systems of trade and the economies as a whole. The economic impact of terrorist attacks against maritime transport could be extremely fearsome. The disruption of oil trade for example, as a result of a terrorist attack, will have significant implications for economies worldwide. It is

noteworthy that following the 2019 attacks on tankers in the Persian Gulf and the attack on Aramco's refinery in Saudi Arabia, Brent's prices rose sharply.

2.3 *INTANGIBLE THREATS (CYBER)*

While the IMO has given specific guidance to shipowners and operators to incorporate cyber risk into ships' safety management systems by the year 2021, cyber criminals are already at work. Attacks of this nature are by no means limited to land. Opportunities for cyber criminals to cause chaos are expanding as vessels become increasingly connected. Cybersecurity vulnerabilities, exploits, and threats are on the rise across all critical infrastructure sectors, particularly transportation. There are many analogues between the aviation and maritime transportation sectors; whereas aviation has airport operations, air traffic control, airline operations, aircraft operations, and unmanned aircraft systems, maritime transportation has port operations, vessel traffic services (VTS), shipping line operations, vessel operations, and unmanned maritime systems, respectively. Both sectors have manufacturing, cargo and passenger transport, and hand-offs of passengers and cargo to other modes of transportation. Both have a broad variety of users, including commercial, military, individual, corporate, and public sector craft. And both are subject to attack by a variety of Cyber actors, ranging from criminals and hacktivists to spies, terrorists, and information warriors. Indeed, there are similarities to other transportation sectors (e.g., trucking and railroads), as well as other critical infrastructure sectors.

Numerous maritime-specific communications systems are used for navigation, ship-to-ship and ship-to-shore information exchange, vessel management and control, cargo scheduling and management, passenger entertainment, and safety.

Most of these systems were created without cyber-security in mind and well before the widespread cyber-attacks that are now so common on the Internet.

From maritime automated navigation systems and the Automatic Identification System (AIS) to Global Navigation Satellite Systems (GNSS) and the Long-Range Identification and Tracking (LRIT) network, it is clear that it is important to design, deploy, and maintain critical maritime systems with appropriate adversarial models, risk frameworks, and

resiliency plans" (Kessler and Craiger 2019, p. 429). The global shipping industry – much like air, road and rail transportation – is undergoing a technological revolution. Shipping industry has partnered with the engineering group to promote and to launch automated/unmanned vessels.

Shipping has all become more and more dependent on technology. Many younger mariners do not recall a day at sea without radar, GPS, AIS, ECDIS, and the other myriad data, communication, and navigation systems aboard today's large vessels. Indeed, the U.S. Navy stopped teaching celestial navigation in 1996 due to the prevalence of GPS; they brought it back 20 years later most likely due to the susceptibility of cyber threats against GPS (ibid, p. 435).

In accordance with chapter 8 of the ISPS Code, the ship must be subject to a security assessment, which should include all operations that are important to protect. The assessment should address radio and telecommunication systems, including computer systems and networks (part B, paragraph 8.3 of the ISPS Code). This calls for controlling and monitoring "the ship to shore" path of the internet connection, which is important owing to the fast adoption of sophisticated and digitized onboard systems that in many cases have not been designed to be cyber resilient. The objective of the company's Safety Management System (SMS) is to provide a safe working environment by establishing appropriate safe practices and procedures based on an assessment of all identified risks to the ship, onboard personnel and the environment. In the context of ship operations, cyber incidents are anticipated to result in physical effects and potential safety and/or pollution incidents. This means that the company needs to assess risks arising from the use of cyber technology on board ships and establish appropriate safeguards against cyber incidents. Prior to the ISPS code, the SOLAS primarily focused on the safety of the ship at sea.

The current maritime security measures do not tackle non-seaborne or pier-side vulnerabilities related to information system and technology. Computers and communications system are the strength of modern-day businesses. Many activities in the international maritime commerce could not be successfully done without efficient computer and communication networks. Thus, any attempt to ignore it, when safeguarding international maritime commerce, will make the maritime business vulnerable to exploitation

by criminals or terrorists. For example, terrorists may use a port's computer information systems to locate hazardous cargoes for their subsequent destruction.

According to Michael Edgerton (2013), as cited by Kusi (2015), the ISPS Code is a "reasonably effective initial step in establishing low-low base line security in global shipping. It is because of the drastic differences in size, technological development, and resources available to ports, administrations and shipping companies around the world." Many are of the view that the U.S government has performed well in harmonizing the need for improved supply chain security, and the concerns of the industry's business (Kusi 2015, p. 14).

2.3.1 TYPES OF CYBER-ATTACKS/TOOLS

There are two categories of cyber-attacks, which may affect companies, ports and ships. (The distinction between information technology (IT) and operational technology (OT) systems should be considered. Information technology systems may be thought of as focusing on the use of data as information. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes. Furthermore, the protection of information and data exchange within these systems should also be considered) (MSC-FAL.1/Circ.3 Annex, 5 July 2017, p. 2):

• ***untargeted attacks***, where a company, port or a ship's systems and data are one of many potential targets

• ***targeted attacks***, where a company, port or a ship's systems and data are the intended target.

Untargeted attacks are likely to use tools and techniques available on the internet which can be used to locate, discover and exploit widespread vulnerabilities which may also exist in a company and onboard a ship. Examples of some tools and techniques that may be used in these circumstances include:

• Malware: Malicious software which is designed to access or damage a computer without the knowledge of the owner. There are various types of malware including Trojans, ransomware, spyware, viruses, and worms. Ransomware encrypts data on systems until a ransom has been paid. Malware may also exploit known deficiencies and problems in outdated/unpatched business software. The term exploit usually refers to the use of a software

or code, which is designed to take advantage and manipulate a problem in another computer software or hardware. This problem can, for example, be a code bug, system vulnerability, improper design, hardware malfunction, and error in protocol implementation. These vulnerabilities may be exploited remotely or triggered locally.

Locally, a piece of malicious code may often be executed by the user, sometimes via links distributed in email attachments or through malicious websites.

• Social engineering: A non-technical technique used by potential cyber attackers to manipulate insider individuals into breaking security procedures, normally, but not exclusively, through interaction via social media.

• Phishing: Sending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information. Such an email may also request that a person visits a fake website using a hyperlink included in the email.

• Water holing: Establishing a fake website or compromising a genuine website to exploit visitors.

• Scanning: Attacking large portions of the internet at random.

Targeted attacks may be more sophisticated and use tools and techniques specifically created for targeting a company or ship. Examples of tools and techniques which may be used in these circumstances include:

• Brute force: An attack trying many passwords with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords until the correct one is found.

• Denial of service (DoS): prevents legitimate and authorized users from accessing information, usually by flooding a network with data. A distributed denial of service (DdoS) attack takes control of multiple computers and/or servers to implement a DoS attack.

• Spear-phishing: Like phishing but the individuals are targeted with personal emails, often containing malicious software or links that automatically download malicious software.

• Subverting the supply chain: Attacking a company or ship by compromising equipment, software or supporting services being delivered to the company or ship (The Guidelines on Cyber Security Onboard Ships Version 3.0).

2.3.2 EXPOSURE/VULNERABILITY OF SYSTEMS

The increased use of Computer Network Systems from navigation to container inspection has enhanced mariners' and vessels' safety at sea. However, the more we leverage on internet for these activities, the more vulnerable we become. Vessels are now vulnerable to Cyber Attacks, as those systems were designed to meet the needs of the 20th century rather than the threats of the 21st. Important exposed/vulnerable systems with high risk such as (Fig.2):

A. Bridge systems such as:

(1) E-navigation and integrated Automatic Identification Systems (AIS) to supplement marine radar, the main method of vessel detection, positioning and collision avoidance

(2) GPS/dGPS, ECDIS (Electronic Chart Display and Information Systems) that are often integrated with company's AIS;

B. Cargo handling and management systems;

C. Propulsion and machinery management and power control systems;

D. Access control systems;

E. Passenger servicing and management systems;

F. Passenger facing public networks;

G. Administrative and crew welfare systems; and

H. Communication systems (MSC-FAL.1/Circ.3 Annex, p. 1).

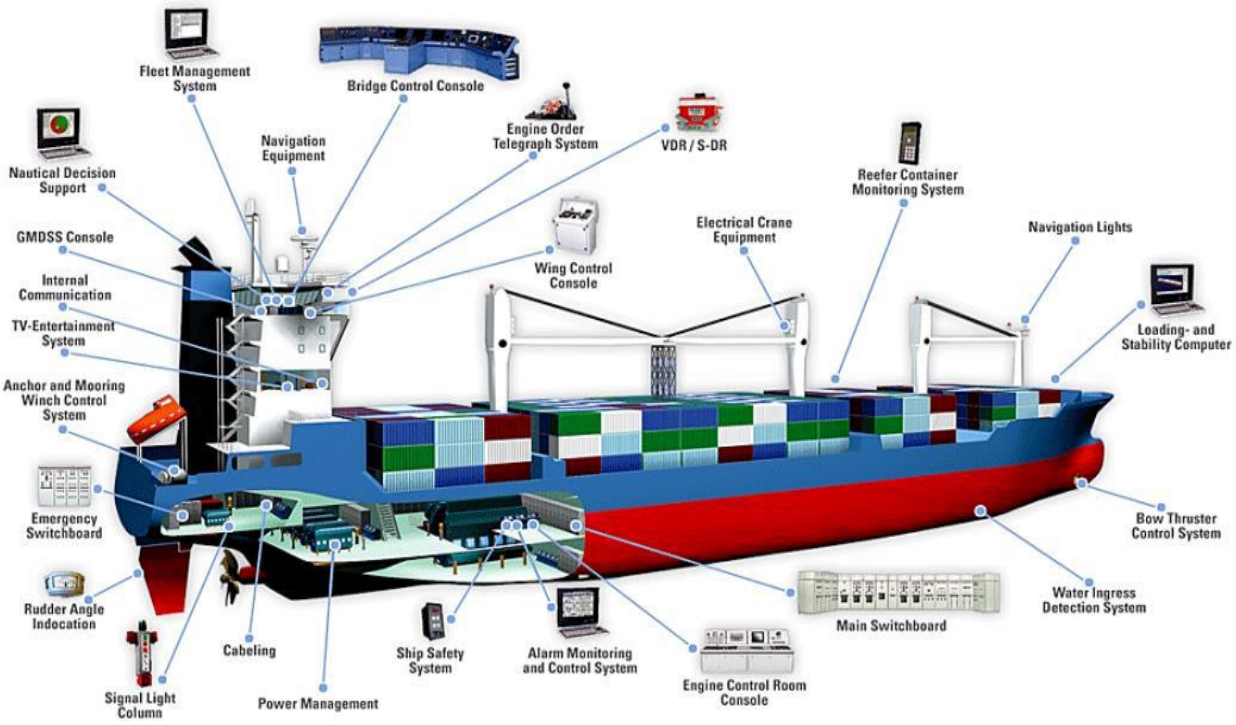

Fig. 2. Electronic System and Equipment onboard Vessels. Source: Deloitte (PowerPoint Presentation)

Gaining access to these systems could allow criminals to disable one or multiple ships transiting strategically important waterways, greatly impacting world trade (BIMCO et al. 2018). Maritime Cyber Threats could be considered that 'are encouraged' also by

- Increasing connectivity of ships
- Ever-greater integration of ICS into onboard networks
- Pre-Internet systems and protocols wrapped in IP
- Widespread use of USB memory devices for data sharing
- Greater use of remote access capability
- Attackers increasing targeting non-conventional IT
- Lack of Leadership in the Maritime Cyber Security Space (NCC Group Approach to Maritime Cyber, https://www.nccgroup.trust › presentations).

Vulnerabilities can result from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyber discipline. In general, where vulnerabilities in

operational and/or information technology are exposed or exploited, either directly (e.g. weak passwords leading to unauthorized access) or indirectly (e.g. the absence of network segregation), there can be implications for security and the confidentiality, integrity and availability of information. Additionally, when operational and/or information technology vulnerabilities are exposed or exploited, there can be implications for safety, particularly where critical systems (e.g. bridge navigation or main propulsion systems) are compromised (MSC-FAL.1/Circ.3 Annex, p. 2).

2.4 POSSIBLE CONSEQUENCES OF SECURITY THREATS

The magnitude of the consequences of hostile action depends on the nature of the attacks, the complexity of the scenarios and the procedures already established by the industry. The consequences of attacks in terms of safety, environmental and economic impact are:

2.4.1 *SAFETY IMPACTS*

There are many systems, types of equipment and various technologies in the maritime industry and onboard vessels as it described above including bridge, cargo handling, ship control access, propulsion, machinery, communication, and the whole vessel. The International Maritime Organization requires vessels above 500tn, carrying onboard AIS, ECDIS and also having a receiver for a global navigation satellite system (GPS). Any hostile intervention/disruption in those systems, such as jamming (*Jamming* is to deprive navigation of any GPS data by superposing a signal to the received signal), spoofing (*Spoofing* is to trick the GPS with false position/time) etc., could cause severe consequences. As put by David Last, a former president of the United Kingdom's Royal Institute of Navigation, "Jamming just causes the receiver to die, spoofing causes the receiver to lie." (https://www.directionsmag.com)

2.4.2 *ENVIRONMENTAL IMPACTS*

Environmental pollution is an additional potential risk related to security incidents. In the case of security incident by any mean against ships carrying raw materials or oil, the

consequences could be extremely unpredictable. Oil spills on the sea can have severe impacts, including damage to wildlife, habitats, and ecosystems. Also, the equipment on board the vessels that regulate loading, discharge, and emissions, are controlled by electronic systems. If the vessel is under threat (cyber attacked for example), all this equipment is vulnerable and can be used to carry out criminal acts or specific damage, signifying a potential risk to the environment and human health.

2.4.3 *ECONOMIC IMPACTS*

Any damage to vessel, loss of hire or delay, ransom payment, insurance expenses or rerouting as a result of a security incident may cause loss of revenue. Furthermore, particular economic risks involve business interruption, information recovery, equipment repair and system installation costs, representing a great loss for the companies. Such perils are accepted by insurers, but perils related to the consequences of cyber-attacks, confront the unwillingness of insurers to cover them. A very rough idea about the insurance cost of transit in the Gulf of Aden in 2012 was about $30,000; by the end of 2017, when the risk was practically eliminated, the cost was about $1,000 (Pagonis and Pentheroudakis 2019, p. 113).

Furthermore, it has become evident that the company's losses other than the financial ones (e.g. the reputation loss), resulting from an incident of any risk, are particularly hard to estimate and, similarly, the cost of these losses is very difficult to calculate. Consequently, insurers often can take over only the calculable financial loss risk and thereby provide cover only against those cybercrime losses for example, whose financial cost assessment is feasible and thus the corresponding insurance premium rates, as well as the claims, are calculable.

3. METHODOLOGY

The main instrument to record and display the relevant data is to create a list of recent cases with detailed information, through a collection of reports, mainly from maritime electronic journals and articles, showing the specific areas affected and the consequences of the attacks, to demonstrate the importance of the security measures for the maritime industry. Unfortunately, the available data on the cyber-attacks that have appeared during the last years have not been reported, on one hand due to non-existence of relevant international report

center and, on the other, due to the unwillingness of the victims to report cyber-attacks for fear of reputational damage. That makes the effort of this specific task to be considered as "restricted maneuverability", if we may use maritime terminology, in contrast with traditional threats, for which ICC is recognized by IMO as the official report center. Also, the use of the bibliography provides some useful data.

3.1 PIRACY INCIDENTS

Where a risk of attack has been identified, the flag state of the vessel shall advise the ships concerned, of the current security level; of any security measures that should be put in place by the ships concerned to protect themselves from attack; and of the security measures that the coastal State has decided to put in place (http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security). The ICC International Maritime Bureau (IMB) is a specific department of the International Chamber of Commerce (ICC). The International Maritime Organization (IMO) in its resolution A 504 (XII) (5) and (9) adopted on 20 November 1981, has *inter alia*, urged governments, all interests and organization to co-operate and exchange information with each other and the IMB with a view to maintaining and developing a coordinated action in combating maritime fraud" (ICC-IMB 2019, p. 2). Such co-operation has been faithfully implemented and records the data as below.

By the first half of 2019, 78 incidents of piracy and armed robbery against ships were reported to the IMB Piracy Reporting Centre (PRC) – compared with 107 in 2018 and 87 incidents in 2017 for the same period. Vessels were successfully boarded in 78% of reported incidents. The Q2 2019 figures are broken down as 57 vessels boarded, nine vessels fired upon, nine attempted incidents and three hijackings. Globally, 38 crew were taken hostage, 37 kidnapped, four threatened, two injured, one assaulted and one crew reported killed.

While 43% of the reported 77 incidents took place within the Gulf of Guinea region, 73% of the global kidnappings and 92% of the global hostages are attributed to this region; maintaining it as the highest risk area for seafarers. The number of crew kidnapped in 2019 in the Gulf of Guinea is 27 in 2019, almost unchanged from 25 in the same period in 2018.

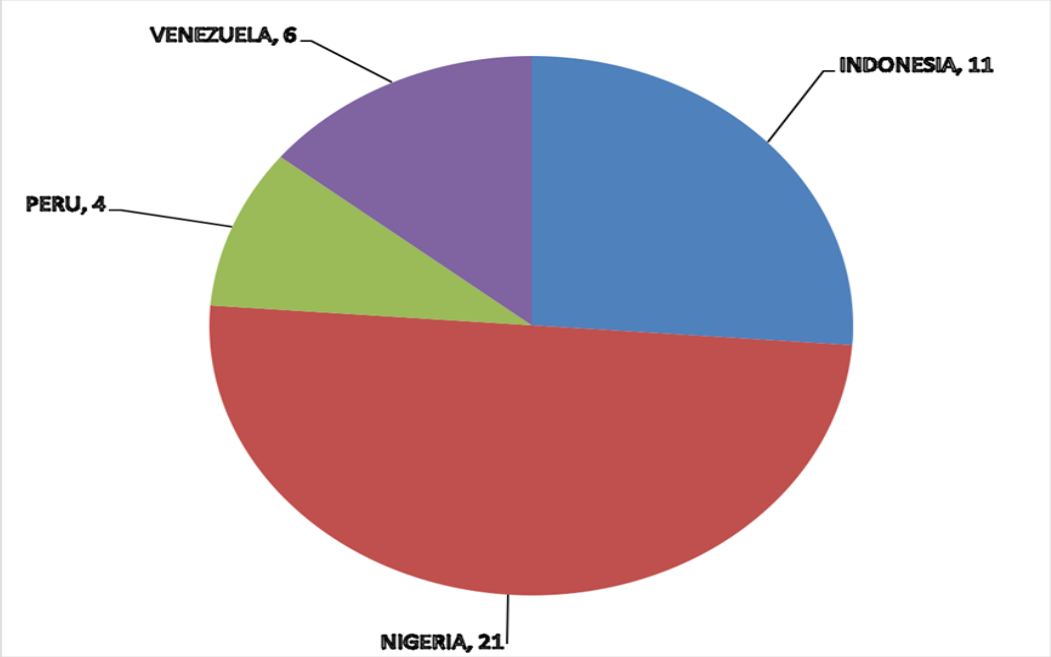

Fig. 2 Locations that contributed to 55% of a total of 77 incidents in the period Jan. – June 2019 (ICC-IMB 2019, p. 6)

Twenty-one incidents were recorded for Nigeria – down from 31 in the same period of 2018. Eight of the nine vessels fired upon worldwide were however in these waters. At the time these incidents occurred, the vessels were at an average distance of 65nm off Brass (south coast of Nigeria) – classifying these as acts of piracy" (ICC- IMB 2019, p. 22)..

TABLE 1: Locations of ACTUAL and ATTEMPTED incidents 2015–19 (January - June) (source: ICC- IMB Piracy and Armed Robbery Against Ships Report)

	Location	2015	2016	2017	2018	2019
SE ASIA	Indonesia	54	24	19	25	11
	Malacca Straits	3				
	Malaysia	11	4	3	2	3
	Philippines	4	3	13	3	3
	Singapore Straits	6		1		
	Thailand	1				
EAST	China		5	1	2	3
ASIA	Vietnam	13	3		2	
INDIAN	Bangladesh	11	2	5	7	
SUB CONT	India	4	13	1	2	2
AMERICAS	Brazil				2	2
	Colombia	2	2	2		3
	Dominican Republic					1
	Ecuador			1	1	2
	Guyana		1	1		
	Haiti	1			3	
	Panama					1
	Peru		4	2	3	4
	Venezuela		2	6	7	6
AFRICA	Angola		1	1		
	Benin				5	1
	Cameroon				2	1
	Democratic Rep. of Congo	1	2		1	1
	Equatorial Guinea					2
	Ghana	2			5	3
	Guinea	3			1	1
	Gulf of Aden*		1	2	1	
	Ivory Coast	1	1	1		1
	Kenya	1	2	1		
	Liberia	1				1
	Morocco					1
	Mozambique	1		1		1
	Nigeria	11	24	13	31	21
	Red Sea*			1		
	Sierra Leone			4		
	Somalia			4	1	
	South Africa		1			
	The Congo	2	1	1		
	Togo		1		1	3
REST	Iran			1		
OF	Oman			1		
WORLD	Papua New Guinea	1				
	Yemen		1	1		
Subtotal for six months		134	**98**	**87**	**107**	**78**
Total at year end		246	**191**	**180**	**201**	

All incidents with * above are attributed to Somali pirates.

It is apparent that piracy incidents along the Indian Ocean are under suppression, whilst in other coastal states piracy flourishes.

3.2 CYBER INCIDENTS

Cybercrime's obscure development nowadays has become a digital scourge, taking epidemic dimensions of a digital disease. As a direct result of this, the majority of internet users seem powerless in the face of such a high risk, often becoming dangerously exposed to notorious cyber criminals' intentions and acts.

Unfortunately, the shipping domain is not an exception to this. Based on statistics and other relevant data derived from the Allianz Risk Barometer, cybercrime is amongst the top five risks in this regard. Despite still being a brand-new risk, it ranks third on the list, with company managers consisting more than 31% of the overall participants here.

It is worth noting the incident which came about between the years 2013 and 2015, when significant profile data was "snitched" from more than 86 million Facebook users by Cambridge Analytica, to be utilized in the building of a database, followed by further implications. There are numerous examples of human errors done so far in the shipping domain. Here are the most frequent and notable ones:

- Cellphone plugged to be charged by seaman in ECDIS or other USB port.
- Seaman interfering with M/E Automation and shutting down M/E, after having plugged a computer in network socket.
- Car GPS jammer unintentionally disrupting GPS function for more than 7 hours.
- Unrevealed malware infection, lasting for lots of months.
- Invalid bank account payment (Pagonis and Pentheroudakis 2019, p. 121).

3.2.1 *PUBLISHED/KNOWN INCIDENTS*

This collection of data as primary sources is obtained through an internet search and physical access and concerns the last years.

TABLE 2 (by author): Known/published incidents of cyber-attacks in recent years (2017- 2019)

Date	System	Way of entry	Geographic Area/Name	Consequences	References
22/6/17	Vessel's positioning equipment	Spoofing	Black Sea	Safety issues (25nm false position)	https://www.maritime-executive.com https://safetyatsea.net
7/17	Vessel's positioning equipment	GPS Jamming	Shanghai	Safety issues	https://safety4sea.com https://www.ajot.com
24/7/18	Shipping company's systems	Ransomware attack	Long Beach LA/ Cosco's terminal	1.Company's network broke down 2.Malfuction of company's electronic communications	https://www.portstrategy.com https://www.tradewindsnews.com https://worldmaritimenews.com https://splash247.com
20/9/18	Port's systems	Spam	Port of Barcelona	Malfunction of internal IT systems'	https://safety4sea.com https://www.portstrategy.com https://www.zdnet.com
25/9/18	Port's systems	Ransomware attack	Port of San Diego	Malfunction of internal IT systems'	https://safety4sea.com https://www.zdnet.com
10/18	Shipyard's data management systems	cyber breach	Australian defense shipbuilder Austal	Dispossession of data	https://safety4sea.com https://www.zdnet.com https://www.bairdmaritime.com https://www.abc.net.au
2/19	Vessel's control Systems	Malware	East USA cost	Complete loss of the vessel's control	https://www.ajot.com https://nakedsecurity.sophos.com
7/19	Vessel's positioning equipment	Spoofing	Stena Impero/ Persian Gulf	Malfunction of positioning system/seizure of the vessel	https://www.rivieramm.com

3.2.2 *THE MAERSK LINE CASE*

In June 2017, the container shipping company A.P. Moller - Maersk suffered from a major cyber-attack caused by the NotPetya malware, which also affected many organizations across the world. Consequently, Maersk's operations in transport and logistics were disrupted, leading to unwarranted impact.

The attack reportedly created huge problems to the world's biggest carrier of seaborne freight which transports about 15 per cent of global trade by containers. Maersk's container ships stood still at sea and its 76 port terminals around the world ground to a halt. Even though the recovery was fast, the organization suffered financial losses up to USD300m including loss of revenue, IT restoration costs and extraordinary costs related to operations.

All began when an employee in Ukraine responded to an email which contained the NotPetya Malware. The virus began its spread on Tuesday, 27th June 2017. The system was affected, and therefore operations practically had to be on hold until the system's restoration. More specifically, the attack resulted in the following:

- Several port terminals run by Automatic Performance Management (APM), including in the US, India, Spain and the Netherlands, were struggling to revert to normal operation after experiencing massive disruptions.
- Dry cargo could not be delivered, and no container would be received. Several IT systems were shut down.
- The costs of operation suspension and cargo damages were extremely high.
- The costs of systems upgrading, and additional protective measures cannot be assessed yet.

Although the incident was serious, the organization responded rapidly, under the supervision of its CEO and top management team. A team of IT experts (including internal and external partners) mobilized to track, identify and remove malware from affected systems in order to put operations back in line, while at the same time media handling was excellent with instant feedback to Maersk's stakeholders about the situation (Pagonis and Pentheroudakis 2019, pp. 121-122).

4. RESULTS

4.1 CURRENT PRACTICE EVALUATION OF ANTI PIRACY EFFORTS

By the end of 2012, IMO had issued 24 MSC circulars and resolutions concerning piracy and armed robbery (https://www.imo.org/Documents/IMO_Piracy_Guidance, see Annex). These suggest possible countermeasures that could be employed by Rescue Co-ordinational Centers (RCC) and security forces, guidance and instructions. The documents contain a set of measures or recommendations, it is imperative for governmental or other agencies concerned to gather accurate statistics on the incidents of piracy and armed robbery against ships, to collate these statistics under both type and area and to assess the nature of the attacks with special emphasis on types of attack, accurate geographical location and modus operandi of the wrongdoers and to disseminate or publish these statistics to all interested parties in a format that is understandable and usable. This documentation is more or less oriented to the Somalia-based piracy, that's why in 9 out of 24 documents the geographic identification is apparent (Somalia, Western Indian Ocean and Gulf of Aden).

Apart from what governments have done, the shipping industry has taken great pains to protect itself. In June 2018, the 5th edition of the piracy-specific Best Management Practice (BMP5) was issued by BIMCO, ICS, IGP&I Clubs, INTERTANKO and OCIMF, compiling a useful and comprehensive guidance which introduces effective measures for the protection of crew, vessels and cargo while transiting, specific, the Red Sea, the Gulf of Aden, the Indian Ocean and the Arabian Sea. BMP have been designed by industry bodies, giving guidelines on how to prepare for and behave during a transit through the High-Risk Area (HRA - the geographic delimitation of the Somali piracy risk area, agreed upon by shipping industry, insurance companies and stakeholder governments) in order to minimize risks. Recommended preparations include the installation of barbed wire and a citadel, recommended behavior e.g. to keep a watch, maintain a long distance from the Somalia coast and sail at higher speeds. The latter two behaviors have contributed much to the cost inflicted

by piracy on the industry (sailing a higher speed is very fuel-inefficient). Moreover, ships have taken to carrying armed guards on board, sometimes military personnel, sometimes civilian/commercial, after flag state and regional governments have adapted regulations to accommodate that. All vessels are advised and encouraged to adhere to the BMP 5 recommendations while transiting these waters. Vessels employing Privately Contracted Armed Security Personnel (PCASP) should be cautious and not mistake fishermen for pirates in some heavy fishing areas. Given that regional instability has introduced other maritime security threats, which include deliberate targeting of ships by extremist groups and collateral damage arising from regional conflict, BMP5 aim to mitigate the risk from piracy and other maritime security threats. Additionally, along with BMP5 publication, a Global Counter Piracy Guidance is a useful tool available for companies, masters and seafarers as well as updated guidelines (version 3) 2018 for operators and masters suggesting effective measures to avoid piracy attacks in the Gulf of Guinea (GoG). This has been developed purely as guidance to be used at the user's own risk to protect seafarers, the ship and cargo and, to facilitate threat and risk assessment and planning for voyages transiting areas where the threat of attack by pirates and armed robbers exists.

Referring to the "off the coast of Somalia" attacks as from 2000 we see a 32-nation naval partnership to undertake protection of merchant ship in high-risk areas (South Red Sea, Somalia, Gulf of Aden, Arabian Gulf), after a Declaration and Authority by the Security Council of The United Nations. Also, many other organizations combined forces, like NATO and individual naval forces for reporting, etc. till end of 2013 when the attacks were reduced to minimum in this area and today do not exist. In 2008, there were 111 attacks which included 42 successful hijackings. From 1 January to 30 June 2019, no incidents were reported to the IMB PRC for Somalia and Gulf of Aden. This is only a fraction of the up to 30,000 merchant vessels which pass through that area. Additionally, a lot of efforts have been made by the UN to stabilize the state of Somalia (Pagonis and Pentheroudakis 2019, p. 113).

Obviously, the efforts that have been made by all actors to address that natural and tangible threat have proved effective for the specific area of the Indian Ocean. On the other hand, the reaction concerning the rest geographical areas of maritime interest to the international community looks like numb and not effective yet.

4.2 CURRENT PRACTICE EVALUATION OF ANTI CYBER EFFORTS

As we move towards 2021, the level of cyber awareness among the maritime community is increasing rapidly. There has been a marked change in attitude over the last few years, particularly since the well-publicized Maersk cyber-attack as it was presented above, which shook all the shipping industry, which often thought cyber was a problem that might disappear. Contrary to the aforementioned worries and concerns, the use of the term **"cyberworthiness"** still seems to be quite limited, remaining on the sidelines, but is expected to become more and more widespread going forward, considering that the term has made its first appearance recently.

Only in 2017, IMO along with other organizations issued guidelines and recommendations for protecting the Maritime infrastructure from cyber threats (MSC-FAL.1/Circ.3, 5 July 2017), recognizing (a) the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping industry, which is operationally resilient to cyber risks, (b) also that administrations, classification societies, ship-owners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities.

The Guidelines on Cyber Security Onboard Ships version 3 issued in 2018 by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI are aligned with the IMO guidelines and provide practical recommendations on maritime cyber risk management covering cyber aspects.

In 2017, the International Maritime Organization (IMO) adopted its Maritime Cyber Risk Management in Safety Management Systems resolution, which requires ship owners and managers to incorporate Cyber risk management into ship safety by 2021 (Resolution MSC.428(98), adopted on 16 June 2017).

Cybersecurity is an aspect that has lately come to the attention of the international community and the shipping community in particular. Cyber threats may seem intangible and

elusive, but are real and call for sound preventive measures, without which any economic activity, not least shipping activity, could be dramatically impaired.

Maersk's incident has been a clear confirmation. The attack successfully occurred regardless of the measures that Maersk had in place for such events. In its Annual Report 2016, the organization had clearly stated the following: "A.P. Moller - Maersk is exposed to cyber security threats that could materially affect operation and the financial condition. Cyber-attacks targeting systems or production facilities could result in severe business disruptions and significant losses, as A.P. Moller - Maersk is involved in complex and wide-ranging global services and engaged in increased digitization of its businesses, making it highly dependent on well-functioning IT systems. The risk is managed through close monitoring and enhancements of cyber resilience and focus on business continuity management in the event that IT systems, despite their efforts, are affected" (A.P. Moller - Maersk Annual Report 2016, p. 30).

Of course, security training has to be updated in response to these new risks. As Captain Andrew Kinsey puts it, "New technology and the Internet of Things have introduced many new exposures and threats, in many ways current security training reflects the same goals and objectives we had when steaming in piracy waters in the 1980's; present a hard target and have a plan that can survive a punch in the mouth" (https://www.maritimeprofessional.com/news/cyber-hack-fortifying-maritime-port).

5. CONCLUSIONS/DISCUSSION OF FINDINGS

Maritime shipping today is exposed to various threats, both physical and intangible. The former are more easily understood and potentially addressed, as they typically affect a given geographical location. The latter are less obvious and more difficult to avert, as they are not restricted by geographical borders or any other physical barriers. These are called cyber threats and have led to the emergence of cyber security as a brand new field in the maritime security domain. Indeed, the new technologically advanced systems that are present in the modern shipping industry facilitate efficient operation, but at the same time represent specific vulnerabilities for the different systems, which can result in catastrophic scenarios. The increasing interdependency of cyber risks, coupled with the fragility and vulnerability

of a company's systems due to their constant interaction, obviously renders the security of these systems highly exposed if not compromised.

Cyber-attack incidents and/or other sorts of cyber-security violations may have a wide and diverse range of business implications. The great difficulty in accurately assessing the risk occurrence possibility and in identifying and quantifying the impact and overall effects on the business perplexes the cybercrime risk measurement and prediction process.

The bigger and more multinational (in nature) a company is, the more vulnerable to cyber-attacks and other similar incidents its computer systems' software and infrastructure can get. The evident lack of legal standards and law-abiding definitions, capable of determining clearly and precisely cyber liability in global dimensions and effects, hinders cyber risks to grow fairly insurable. Moreover, the limited competence (due to inevitable geographical restrictions) of country legislation has proved not enough to cover the global needs and demands of the internet.

In the preceding chapters, we looked at incidents of piracy and armed robbery against ships that occurred in the past few years, as well as cyber incidents. We also searched the available literature and official reports for evidence. The investigation showed that piracy and armed robbery incidents have declined in number and frequency, especially in the Indian Gulf. This can be attributed to the concerted effort and willingness of the international community, targeting the specific region as a High Risk Area (HRA). A similar improvement has not been achieved yet in the Gulf of Guinea, but it is probably a matter of time before it is achieved there as well.

The effectiveness of the ISPS Code, as it currently stands and with its updates but also with the willingness of the international community, is held to be satisfactory. With time, as the Code's requirements are increasingly better understood and internalized by the parties involved, its effectiveness is expected to substantially improve. The inclusion of specific guidance in the SMS aimed to address the threats proves how useful the ISPS Code can be. The success in confronting piracy in the Indian Ocean is a good case in point, showing that when circumstances are mature and the international community joins forces, effective action can be taken. In other areas of less significance, it seems that the effort to curb piracy is still

at a too early stage, as illustrated by the limited number of issued guidance documents as well as by the growing number of incidents.

Unlike piracy or other tangible/physical threats, cyber-threats have no borders, as there is no precisely identified High Risk Area (HRA), nor is there any standard frequency. As far as these threats are concerned, IMO has delayed in taking specific action. The pending entry into effect of the cyberworthiness accreditation by the competent authorities by the year 2021 confirms this belated response.

In this regard, the ISPS Code, and not only, still seems to be in a premature (experimental) stage, with no solid and tangible results yet.

On the other hand, it is obvious that awareness of the involved personnel is absolutely necessary, in order to mitigate the consequences of such threats.

It is necessary to understand that the risks that the maritime industry is facing in terms of cyber security are real, and it is necessary to develop a training strategy on cyber security awareness for employees. Shipping companies, governments, port facilities, ship-owners and operators should build culture to cover the gap of risk awareness, across cyber and traditional threats, even if this would require additional paperwork, extra man-hours, more administration work and operational costs. This is the great challenge. Cyberworthiness should not be considered any more as an extreme term, but should be as frequent and equally taken into account as seaworthiness.

REFERENCES

A.P. Moller - Maersk (2017). *Annual Report 2016*.

Bichou, K. (2015). "The ISPS Code and the Cost of Port Compliance: An Initial Logistics and Supply Chain Framework for Port Security Assessment and Management", in Haralambides (ed.), *Port Management*. Palgrave Macmillan, London.

BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and World Shipping Council (2018). *The Guidelines on Cyber Security Onboard Ships Version 3*.

Bueger, C. (2014). "What is maritime security?", *Marine Policy*, 53, March.

Germond, B. (2015), "The geopolitical dimension of maritime security**"**, *Marine Policy*, Volume 54, April**,** 137-142.

ICC - IMB (2019). *Piracy and Armed Robbery Against Ships Report – Second Quarter 2019*.

IMO (2017), MSC-FAL.1/Circ.3, 5 July.

Kessler, G.C., J.P. Craiger and J. C. Haass (2018). "A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System", *The International Journal on Marine Navigation and Safety of Sea Transportation,* 12 (3).

Kusi, B. (2015). "Port Security - Threats and Vulnerabilities", Thesis, Laurea University of Leppävaara, October.

Mazaheri, A. and D. Ekwall (2009). "Impacts of the ISPS code on port activities: a case study on Swedish ports", *World Review of Intermodal Transportation Research*, Vol. 2, No. 4.

Møller, B. (2009). *Piracy, Maritime Terrorism and Naval Strategy*, Danish Institute for International Studies, DIIS Report 2009:02.

Pagonis, Th. and N. Pentheroudakis (2019). Chartering Manual by Practitioners, London: Practitioners' Book Avenue LLP.

Silgado, D.M. (2018). "Cyber-attacks: a digital threat reality affecting the maritime industry", World Maritime University Dissertations.

Stopford, M. (2009). *Maritime Economics*, 3rd edition, Routledge.

Suppiah, R. (2009). "International Ship and Port Facility Security (ISPS) Code and Crew Welfare". *Maritime Affairs: Journal of the National Maritime Foundation of India*, June.

HM Government (2014). *UK National Strategy for Maritime Security*, May.

INTERNET SOURCES

http://www.imo.org/Documents/IMO_Piracy_Guidance.

http://www.imo.org/en/ourwork/security/guide_to_maritime_security/pages/solas

http://www.imo.org/Documents/IMO_Piracy_Guidance

https://www.directionsmag.com

https://www.maritime-executive.com

https://www.maritimeprofessional.com/news/cyber-hack-fortifying-maritime-port

https://nakedsecurity.sophos.com

https://www.abc.net.au

https://www.ajot.com

https://www.bairdmaritime.com

https://nakedsecurity.sophos.com

https://www.nccgroup.trust › presentations

https://www.portstrategy.com

https://www.rivieramm.com

https://www.safetyatsea.net

https://www.splash247.com

https://www.tradewindsnews.com

https://www.worldmaritimenews.com

https://www.zdnet.com

ANNEX

IMO PIRACY GUIDANCE

Privately Contracted Armed Security Personnel (PCASP)

MSC.1/Circ.1405/Rev.2 Revised interim guidance to shipowners, ship operators and shipmasters on the use of privately contracted armed security personnel on board ships in the High-Risk Area 25 May 2012

MSC.1Circ./1406-Rev-2 Revised Interim Recommendations for Flag States regarding the use of Privately Contracted Armed Security Personnel on board ships in the High Risk Area 25 May 2012

MSC.1Circ./1408-Rev-1 Revised Interim Recommendations for Flag States regarding the use of Privately Contracted Armed Security Personnel on board ships in the High Risk Area 25 May 2012

MSC.1/Circ.1443 Interim guidance to private maritime security companies providing privately contracted armed security personnel on board ships in the High Risk Area (25 May 2012)

MSC.1/Circ.1444 Interim guidance for flag States on measures to prevent and mitigate Somalia-based piracy (25 May 2012)

MSC-FAL.1/Circ.2 Questionnaire on information on port and coastal State requirements related to Privately Contracted Armed Security on board ships 22 September 2011

Piracy and armed robbery

Resolution A.545(13) Measures to prevent acts of piracy and armed robbery against ships 29 February 1984

Resolution A.683(17) Prevention and suppression of acts of piracy and armed robbery against ships 21 November 1991

Resolution A.738(18) Measures to prevent and suppress acts of piracy and armed robbery against ships 17 November 1993

Resolution A.923(22) Measures to prevent the registration of "Phantom" ships 22 January 2002

MSC.1/Circ.1233 Piracy and armed robbery against ships in waters off the coast of Somalia 15 June 2007

Circular letter No.2933 Request for information on national legislation on piracy 23 December 2008

MSC.1/Circ.1302 Piracy and armed robbery against ships in waters off the coast of Somalia 16 April 2009

MSC.1/Circ.1332 Piracy and armed robbery against ships in waters off the coast of Somalia 16 June 2009

MSC.1/Circ.1334 Guidance to shipowners and ship operators, shipmasters and crews on preventing and suppressing acts of piracy and armed robbery against ships 23 June 2009 (revokes MSC/Circ.623/Rev.3)

MSC.1/Circ.1333 Recommendations to Governments for preventing and suppressing piracy and armed robbery against ships 26 June 2009 (revokes MSC/Circ.622/Rev.1)

SN.1/Circ.281 Piracy and Armed Robbery against Ships in Waters Off the Coast of Somalia – Information on Internationally Recommended Transit Corridor (IRTC) for Ships transiting the Gulf of Aden 3 August 2009

Resolution A.1025(26) Code of practice for the investigation of crimes of

Piracy and armed robbery against ships (revokes resolution A.922(22)) 18 January 2010

MSC.1/Circ.1390 Guidance for company security officers (CSOs) – Preparation of a Company and crew for the contingency of hijack by pirates in the Western Indian Ocean and Gulf of Aden 09 December 2010

Circular Letter 3164 Responding to the scourge of piracy 14 February 2011

Resolution MSC.324(89) Implementation of Best Management Practice Guidance

20 May 2011

MSC.1/Circ.1404 Guidelines to assist in the Investigation of the Crimes of Piracy and Armed Robbery against ships 23 May 2011

MSC.1/Circ.1339 Best Management Practices for Protection against Somalia Based Piracy (BMP 4) (revokes MSC.1/Circ.1337) 14 September 2011

Resolution A.1044(26) Piracy and Armed robbery against ships in waters off the coast of Somalia (revokes resolution A.1026(26)) 20 December 2011