ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΝΑΥΤΙΛΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
στην
ΝΑΥΤΙΛΙΑΚΗ ΔΙΟΙΚΗΤΙΚΗ

Cyber threat to ships: How to manage in order to improve safety and security in the maritime sector

Mr Kaligeris Charalampos (MND18017)

Διπλωματική Εργασία

που υποβλήθηκε στο Τμήμα Ναυτιλιακών Σπουδών
του Πανεπιστημίου Πειραιώς ως μέρος των
απαιτήσεων για την απόκτηση του Μεταπτυχιακού
Διπλώματος Ειδίκευσης στην Ναυτιλιακή
Διοικητική

Πειραιάς

Νοέμβριος 2019

Copyright

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

Τα μέλη της Επιτροπής ήταν:

- ΑΓΓΕΛΟΣ ΠΑΝΤΟΥΒΑΚΗΣ (Επιβλέπων)
- ΤΖΑΝΝΑΤΟΣ ΕΡΝΕΣΤΟΣ
-ΑΡΤΙΚΗΣ ΑΛΕΞΑΝΔΡΟΣ

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

Acknowledgments

This thesis was prepared in the context of completing studies in the Postgraduate Program in Maritime Studies at the University of Piraeus.

I would like to express my sincere thanks to my supervising Professor Mr Angelos Pandouvakis for accepting the supervision of this thesis.

Special thanks to my family for supporting me throughout the years of my studies as well as all my friends for support and understanding them.

Περίληψη

Η παγκόσμια κοινωνία αντιμετωπίζει διάφορες τεχνολογικές εξελίξεις που επηρεάζουν κάθε πτυχή της ζωής, όπως η εφεύρεση του Διαδικτύου που μετέτρεψε την πρόσβαση σε πληροφορίες, το παγκόσμιο εμπόριο, την ψυχαγωγία και τις επικοινωνίες σε κάτι εύκολο και εύκολα εφαρμόσιμο από την ασφάλεια του σπιτιού μας.

Από την πλευρά τους, οι εξελίξεις αυτές έχουν προκαλέσει πολλά ζητήματα τόσο στις επιχειρήσεις όσο και στα άτομα και τα οποία αφορούν την ασφάλεια των χρηστών και την ασφάλεια των συναλλαγών τους εν γένει. Ο ναυτιλιακός τομέας είναι μία από τις βιομηχανίες που υποφέρουν πολύ.

Στην παρούσα πτυχιακή θα εξετάσουμε και θα αναλύσουμε τον τρόπο με τον οποίο η τεχνολογία στον κυβερνοχώρο επηρεάζει τον ναυτιλιακό τομέα και τον τρόπο με τον οποίο το επηρεάζει στο σύνολό του. Ταυτόχρονα, θα κάνουμε προτάσεις για μέτρα που μπορούν να ληφθούν για τη βελτίωση της ασφάλειας και της αύξηση της εμπιστοσύνης από την πλευρά των χρηστών.

Λέξεις-κλειδιά: ναυτιλία, πλοία, απειλές, ναυτιλιακή διοίκηση, ασφάλεια και αξιοπιστία, τεχνολογία.

Abstract

The global society faces several technological developments that influence every aspect of the life; the invention of the internet transformed the access to information, the global trade, the entertainment and the communications into something easy and easily implemented from the conform of our home.

On the hand these developments have caused several issues to both companies and individuals concerning the safety and security of their transactions in general; the maritime sector is one of the industries that suffer a lot.

In this thesis we will examine and analyze how cyber technology influences the maritime sector and how it impacts it as a whole; on the same time, we will make suggestions on measures that may be taken to improve the safety and security.

Keywords: maritime, ships, threats, shipping management, safety and security, technology.

Table of contents

Chapter 1
Introduction

In our era of globalization and cyber-space, the word together has a different meaning; the digital technology and the internet have created a world without barriers where communications are easy while millions of other potentials are created. The doors which are currently opened due to technology are countless.

Technology innovations have been adopted and implemented by the countries, companies and individuals into their daily lives; the maritime industry along with its people did that also. The point is that the reliance on that technology has exposed everybody, including the maritime industry to malevolent use.

The technological developments are many and their effect on our lives and in our daily activities is huge. The information and communication areas are the most affected ones due to the power of the internet; regarding the maritime industry, these developments have changed a lot the way that the vessels are navigated or the way they communicate with the port authorities. Currently, a complex computer network covers the whole maritime industry and its activities either on-board or on-shore (Tucci, 2007).

By the term "Internet of Things" (IOT) we refer to *"The inter-connection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data"* (Oxford English Dictionary); that concept has triggered many disputes and conversations regarding the security and safety of the digital inter-connections.

The first Quasi-Internet system was developed in the 1960s by the US Department of Defence; since then the IOT grew rapidly. The digital technology is in general one of the science sectors that advance extremely fast i.e. out TV sets have become thin, flat and large and our cars have sensors around them which detect any object which is around it.

The maritime industry is affected by the huge number of IOT devices; every other business sector is hugely affected too; the problem is that the effects are not only good but they are also bad. The digital communications and the digital computing systems which are used in the maritime industry is not new; the use of the internet is what made the difference and created several new risks and threats.

The naval architectures include software systems in the new-built vessels and use in general the technology in order to improve both their navigation and their overall operation. While the modern vessel interacts daily with other departments of the maritime industries or with port authorities they have essentially become communication hubs, mobile offices, entertainment centres and learning places (Mendes &Guerreiro, 2017).

All the vessels now are equipped with electronic units (ECUs) along with several other in-built items that provide internet access and thus enable them to share digital information with other vessels and with the onshore authorities; the brand new vessels are furthermore equipped with microprocessors that run over one hundred million (1.000.000) patterns of control software (Cavelty 2012).

Currently, all the major companies that manufacture computers create processes that enable the integration of their systems with those of the vessels. This means in practise that the maritime industry is supported by software systems and networks that give a bunch of new opportunities to it while on the same time several challenges have emerged due to these developments such as the fact that the information and data regarding the infrastructure of the maritime industry is exposed to individuals who may be malicious or have an interest in hacking and threating its security. What is important for the maritime industry is to be able to understand where the digital risks may come from, namely to define their sources and in that way to promote the cyber security (Joszczuk & Januszewska, 2013).

Although the term cyber security is broadly used, there is not yet a definition which is able to capture all its levels and its complex dimension. It is for a fact that the context of the concept of the cyber security is sometimes subjective and thus variable; regarding the maritime industry though we may define it as the protection of the electronic systems along with its software and its users and the communication networks from any possible attack or unauthorized access (Tucker 2015).

In this thesis, the contemporary cyber-threats are going to be explored and analysed in general and particularly in the maritime domain. One of the major challenges that the maritime industry faces is how to make the utilization of cyber tools regarding the vessels, the ports and the maritime infrastructure effective and mainly safe and secure.

In the maritime domain, the cyber-security, in general, is absent while there are several vulnerabilities and risks which are not confronted yet; all these vulnerabilities and potential threats and risks will be examined and recommendation will be given regarding their mitigation.

Since technology is not alive the humans are those who manipulate it and thus determine whether it is used for a good cause or not. The development of technology is for sure something that aims to offer to people a better quality of life; that good cause is taken for granted and thus almost everybody either more quickly or with a slower path adopts these developments. It is just like we may view and understand the use of a firearm, meaning it may be used for a good purpose but on the same time it may be used for an evil one the exact same thing happens with the digital technology which designed for a good purpose while people may use it for purposes of ambiguous morality.

1.1. Aim of the thesis

This thesis aims to present an insight into cyber threats and to cyber security solution focusing in the shipping industry. In the dissertation, the key issues of the new era of communication will be presented and the problems that have been created due to the technological developments and the challenges that the contemporary shipping industry faces. Furthermore, the capabilities will be presented that cyber security may offer against the potential cyber-attacks and possible improvements will be discussed.

1.2. Key research objectives

Cyber security is a perspective of the information security risk that focuses on addressing the types of attack that have the potential to cause large-scale harm. Such attacks can have serious consequences for a company or an organization regarding its finances or its reputation; furthermore, the reliability along with the wellbeing and probably the safety of the people and the environment may be also jeopardized.

Cyber- attacks are highly developed and sophisticated in nature i.e. they exploit the potential organizational, technical or physical weaknesses that may exist in a company and essentially take advantage of them.

Since both the private and the public organizations currently, rely on technology which is digital and smart while their systems are almost always inter-connected they have become much more vulnerable than before. Modern organizations must develop cyber security capabilities in order to be able to respond to the new cyber threat while they must know that how their role (critical function, assets, sensitive information) affects their cyber risk exposure, how the cyber security can be incorporated in their strategy, how they must manage the potential cyber risks and mainly how to use the technology without compromising at all cyber security or vice versa.

In this thesis, the importance of cyber security will be underlined while the major changes both social and political that the new computers technology will be also presented. The point of understanding these issues is to find ways to reduce potential cyber-risks through the implementation of cyber security measures.

The primary research objective is to examine how cyber security affects the industries and specifically the maritime industry and whether it is ready or not to confront the potential cyber-risks.

1.3. Methodology

For this thesis qualitative research was used since it matches better to the specific research objectives. The necessary data was collected from a variety of sources and the analysis was based on a review of the gathered academic literature such as books, articles, reports and web pages. The literature review helped me to establish the theoretical foundation of the study while several cases helped me to gain an empirical, I might say, view of the problem.

1.4. Structure of the thesis

The internet has changed radically our lives as individuals but has also changed the way the world of business works; the access to information, to entertainment or the purchase of goods is now implemented from the comfort of our home. Our generation sends and receives messages or buys products with just a click; everything runs fast now and if someone wants to remain within the game he must keep up with that rhythm.

In our thesis we will start with a presentation of our era and how the innovations of technology have affected our lives; the 2nd chapter is a presentation of the existing literature review regarding the cyber-space and the potential risks and threats that exist for both the businesses and the individuals. In the 3rd chapter all the risks, threats and vulnerabilities that exist in general and for the maritime industry, in particular, will be presented and in the 4rth chapter, all the collected data will be thoroughly analysed. The essay ends with the 5th chapter where the conclusions of the analysis are presented and a few improvement recommendations are made.

Chapter 2
Literature review

The research that has already been conducted regarding the issues of cyber safety and security in general and in the maritime industry, in particular, is rather extensive and it shows that one of its main focus so far is the identification of the various types of attacks that is possible to appear and threaten the security of vessels by i.e. jeopardizing its navigational systems or the security of a port terminal. However, the decisions makers of the maritime industry and the role they have regarding the understanding of the cyber threats was underestimated (Bueger, 2015) and thus left without research.

Through the review of the literature, we will be able to understand in-depth the concept of the cyber-threats and furthermore, we will become able to realize that the need for cyber safety and security is currently more than urgent. As we may easily understand that situation is relatively new, especially for the maritime industry which is not familiarized with the innovations of technology yet; many of the incidents that currently occur are due to ignorance (Tucker 2015, Craigen et al, 2014, Bishop, 2005).

The discussion in the literature regarding cyber security is based in three (3) main elements, namely the information, the people and the technology. Information is related to the data which is used for support by the maritime industry while people are its vital part; technology, on the other hand, has to do with the hardware and software or the platforms that include ports and vessels. Technology is very important for the proper navigation of the vessels and subsequently for the safety of the vessel, the crew and the environment.

Chapter 3
Risks and cyber threats

3.1. Definition and identification of Risks

By the term risk, we refer to a human activity which may lead to several consequences in the future (Aven et al, 2015). These consequences are uncertain and their outcome may be either positive or negative; it is a requirement however that at least one of them will be negative. In order thus, to define an activity as a risk we have to take under consideration the event itself and its possible consequences, the uncertainty of the outcome and the information that we already possess regarding it.

The information always carries uncertainty since it can be easily biased or wrong; thus in every decision, we take a risk of being not 100% sure. When the risk is high the consequences of our decision may not be predicted which affects the quality of its assessment. There are cases that the process of risk assessment contributes more than the actual occurring of the event itself.

The assessment of risk is a very useful tool since it allows the involved in it parties to get acquainted with the potential consequences of their actions. It is essentially a guide for whoever uses it to assess the given information and the available data and predict the potential outcome of the actions; this process makes the awareness regarding the risk stronger and on the same time demonstrates where the possible results will be based on. If someone does not use the risk assessment in the right way he will not understand the risk right and thus he will not predict the conclusion.

As far as the issue of the digital risk, in particular, is concerned it includes threats like the hacking by cyber criminals and the espionage by them; the probability of occurrence of cyber-attack increases more and more every day since the malicious actors become more sophisticated and efficient due to developed tools and methods.

Every company and organization depend on each day more and more to digital tools and systems for its function; this situation makes the company more vulnerable to cyber threats with unknown consequences. In these cases, the risk picture is constantly changing and thus the background knowledge should be regularly updated (Taleb, 2007).

In the world of the digital risks and cyber-attacks the term “black sawn” is used for the description of an extreme event for which we do not know many things and which may have bad consequences for the humans, the environment and of course the company itself (Taleb, 2007). There are three (3) types of “black swans” (Aven et al, 2014, p9):

1. **Unknown-unknowns**, namely events that are completely unknown to the scientific environment.

2. **Unknown-known**, namely events that are not on the list of known events for those who activate in the field of risk analysis but still they are known to others.

3. **Known** but not believed to occur because of low judged probability.

The tolerability limits for each company are different; furthermore, they change from time to time. If the amount of the predicted risk is found within the range that may be accepted, it is then considered to be tolerable; in any other case though the risk must be somehow reduced (Aven et al, 2015). For that purpose, the companies use the ALARM (As Low As Reasonably Practicable) principle under which the selected measure for the reduction will be assessed in comparison with the potential side-effects that may appear and affect the company i.e. the expenses for the measure may be extremely high. Therefore, the measures taken by each company for the reduction of the potential risks are totally different.

3.2. Definition and identification of threats

The cyber risks for each company and each activity are specific; what the companies must do in order to become safer is to understand which one of their operations are more vulnerable to potential cyber incidents and thus take the relevant measures.

A very crucial and thus challenging aspect in cyber security and safety of the shipping industry, in particular, is the fact that due to the fact that the cyber-threats are a rather new problem there is no historic data to be used in order to understand both the threats and their impacts. Regarding the cyber-threats, there is some experience though since other business sectors are also "potential victims" of the cyber-attackers i.e. banks or public authorities. The collected experience is very useful and it helps people to realize that the threat of a cyber-attack is always nearby and it may lead to the loss of assets or money and sometimes even to the loss of human lives. The shipping industry must understand that the danger is rather high and thus take all the required measures in order to mitigate cyber threats (CESG, 2017).

3.2.1. Types of cyber attacks

By the term cyber-threat, we refer to the ability of someone to leverage the contemporary technology of computers and internet in order to exploit its potential victim; in other words, the cyber-threat is a malicious act via which the attacker tries to gain access to a computer network without having the permission to do that. There are several techniques and procedures that may be followed for that to happen i.e. malware is used for the stealing of credit cards and personal data.

The users of technical devices are the most vulnerable parties of the security chain since there is always a security hole in their actions which may not be plugged completely. Furthermore, when an attack derived from inside the overall security is threatened more; the worst-case scenario emerges when the attacker is not aware of the fact that he is an attacker (Walker 2012).

The cyber threats exist since 1975; back at that time Steve Wozniak and Steve Jobs invented the first PC (Personal Computer) which was Apple I. The advent of that invention triggered the advent of hackers, meaning people that manage to access without being authorized the personal information of the users of PCs; the reason for doing that is either profit or just the performance of acts which are mischievous.

The cyber threats may take several forms; their difference has to do with the damage that may accomplish to the network i.e. malware and phishing; the reason that cyber-attacks occur is that the attackers are capable of finding ways to penetrate the network processes (Wert, 2018).

The cyber-attacks are first of all divided into the two (2) following categories (HIS Survey, 2016):

1. Targeted attacks, namely when the ship or the company is the intended target.

2. Untargeted attacks, namely when the ship or the company is potential but not the only "available" victim.

More specifically:

1. Targeted attacks are sophisticated and targeted to a specific company/vessel. Examples of tools which may be used in a potential targeted attack are the following:

A. Brute force is an attack where several passwords may be used while the attacker is trying to guess the right one.

B. Denial of Service is the attack when malware infects a PC which automatically becomes part of a botnet that may be also be infected; these botnets are used for the overwhelming of the server which may be the next target. This action is widely known as DDoS, namely as the Distributed Denial of Service; in order to reduce the risk of a potential DDoS attack the user must disable the services which are not necessary and always update the software and the hardware of the PC while using an effective firewall.

C. Spear phishing is a more developed and thus more dangerous version of the phishing method; the potential attacker here collects all the information he wants regarding his victim by using means of social engineering. The main concept of that method is the sending of a mail that contains a link to a fake and thus malicious website; the difference here is that the victim is called by the attacker with his real name and that the mail contains in general information which is absolutely legitimate. In that way, the whole action does not seem at all to be suspicious.

D. Subverting the supply chain is a company or a vessel is attacked by the use of equipment, software and support services which are being delivered on-board.

Of course there several of other methods which may be used in a targeted cyber-attack such as the impersonation by the hacker of a legitimate employee of a maritime company in order to collect all the information he needs.

For the untargeted attacks on the other side are usually used techniques or tools which provide the opportunity to the attacker to locate its target and mainly to discover all its vulnerabilities; these techniques and tools are often found in the internet. Some major examples of this type of cyber-attacks are the following (Wert, 2018):

1. Social engineering

By the term social engineering we refer to the manipulation of people into providing something i.e. a service or just information that they would not provide under different circumstances i.e. nobody would normally provide his password to a stranger. However, the majority would provide such information only to someone who would seem more trustworthy such a network administrator or a desk employee (Walker, 2015).

When the social engineering is human-based there is always an interactive conversation or some other similar means of communication in order for the necessary information to be gathered; these means require physical access so that the location of the user may be detected and i.e. dumpster diving in order to find a paper that contains passwords or other similar information; furthermore, someone may pretend to be an authorized person such as the tech support employee and convince the victim to give him the right to access the computer.

There is a method which is widely known as reverse social engineering where the attacker manages to be contacted by the victim; in that way trust is gained much easier; a very characteristic example is when the attacker mails a group of people warning them that “tomorrow the network will stop operating for some hours due to technical reasons” and on the same time he provides a contact number for the users to get further information. The next step is to create “a situation” to the computers of those users and wait for them to give him a call in order to solve the problem; the issue is that in order to solve the problem personal details of the users such as their passwords are required (Walker, 2012).

When an attack is computer-based a computer is used (or any other device which has the ability to process data). These devices have pop-up windows which are specially crafted in order to trigger the user to click through a fake site of the web; usually, the attackers use the social media in order to make these websites look more sophisticated and thus believable (Walker, 2012).

2. Phishing

By the term phishing attack, we refer to the creation of an e-mail which seems as being absolutely legitimate but in reality, it contains a link that leads you to a fake website or to the downloading of malicious content. As the sender of this mail appears i.e. a reputable financial institution or a well-known and reliable company. The point is that when the user is convinced to click on the provided in the mail links the attacker immediately gains access to the information that the user will input to the fake website.

These mails are usually designed and presented in a way that even an experienced user may be tricked into believing that it is real; the best solution for that problem is to educate the user more thoroughly in order to make them capable of recognising the phishing emails from the authentic ones. There are some “tips” though for the users to follow in order to be as safe as possible (Walker, 2012):

1. When the sender of the mail is unknown the user must be extremely cautious with its content.

2. When the mail is not addressed specifically to you but goes under a general greeting such as “ideal customer” the user must be extremely cautious.

3. When the mail contains a telephone number the first thing that we have to do is to examine whether it is valid or not.

4. The fake emails usually contain words that have grammar mistakes.

5. A link must be always checked before someone clicks on it; the hovering of the mouse over the link will reveal the actual website that you will be led if you click on it.

Phishing is carried not carried out only by mails but other means such as the links on the Facebook platform or an URL on the Twitter platform; in that way, the attacker is able to collect all the information he needs on order to proceed with the spear-phishing of his victim (Palo Alto Networks, 2016).

3. Watering hole

By the term watering hole attack, we refer to the exploitation of security where the attacker targets a specific group of users and infects websites that this group visit. The goal of the attacker is to infect the PCs of the users and thus to access their personal data.

Watering hole attacks focus mainly on websites which are popular and on the same time absolutely legitimate; the attacks are made in order to get access to something else which is the main and final target. The first (1rst) step of the attacker of a watering hole attack is to find out the profiles of his victims; the majority of the victims of such attacks are employees in large companies or governmental offices. Following that step, the attackers try to discover potential vulnerabilities in the websites and inject there i.e. a malicious HTML code that will direct the victim to the site they want and where the malware is situated. When the victim enters that site he will be immediately infected (Tech-Target, 2015).

Watering hole attacks are not very common; due to that, they may not be detected easily. Their target is usually organizations and companies which possess very high-security standards.

4. Malware

By the term malware, we refer to malicious software which is designed to access a PC without the permission of its owner and then damage it. There are several different types of malware such as the Trojans, the viruses and the worms. In order to have an overview of all these types we may divide them into the following groups:

A. Trojans and Rootkits

Trojans and rootkits may be grouped together since both of them are trying to attack a PC. The Trojan horses infect the software of a PC by pretending that they are non-harmful applications; due to that the users download them since they believe that this piece of software is probably something useful to them and not a malware infection.

Rootkits on the other side are something different; under that term, we refer to a malware technique which does not cause an infection of the software though. Rootkits were created so that the anti-virus detection would not detect them and thus they would not be removed. Currently, several anti-virus programs such as the Bull-Guard Internet Security is able to detect and remove them.

B. Viruses and worms

Both viruses and worms are malicious software infection which is designed in order to be spread without the knowledge of the user. The virus infects software which is legitimate in the following way: it gets inside the software and the use by the owner of the PC spreads it all-over. The worms on the other side are spread without any action of the end-user.

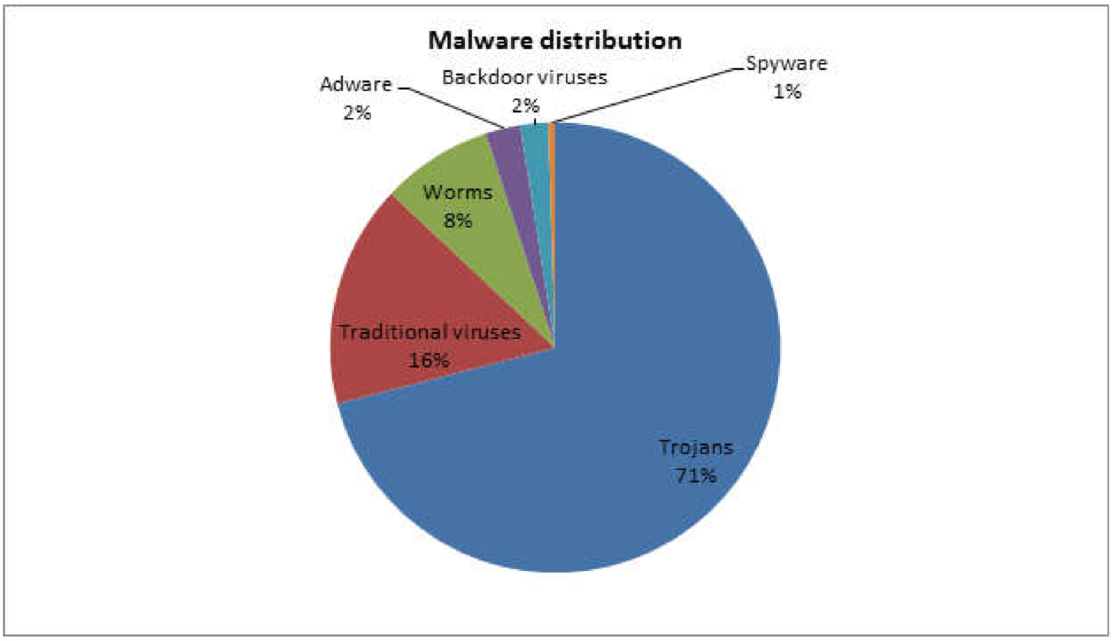
The viruses and the worms may carry a payload, namely a malicious code which is specially designed to cause damage to the PC.

C. Spyware and key-loggers

Both spy-ware and key-loggers are malware infections which are used for cyber-attacks; these threats are designed for i.e. the stealing of money from an unknown computer user or a bank.

Under several conducted security reports the infections caused by Trojan horses are found on the top of the malware list; more specifically more than 70% of the reported attacks on computer systems were caused by Trojan horses, followed by viruses and worms.

The below diagram depicts the distribution of malware attacks all over the world. (Source: Bull Guard Internet Security)



The term malware was initially used for the description of a group of independent agents who were capable of infecting machines and then replicate them; back then their detection was a rather easy task. In our days malware is far more difficult to be detected; according to the Global Security Report it takes up to 188 days from the moment that the pc will be infected since the moment that it can be detected; the reason for that is that the contemporary malware may be easily mutated by the hacker or updated in a form that the existing anti-malware is not yet able to detect (Palo Alto Networks, 2016).

Malware is sometimes designed especially for the hacking and damage of a specific organization or company; furthermore, it is sometimes downloaded through the use of a drive. In this situation the attacker takes advantage of a vulnerable point of the operating system or of the web browser; the user is not able to be aware of what is happening. When the attacker uses the exploitation of software in order to infect the PC essentially an application is being tricked and in that way its code runs. Once the PC is infected the malware is there to make sure that the infection will not be confronted by means such as the disabling of the AV software or the creation of a back-door.

At that point, the malware is absolutely ready to be used by the attacker who wants to gather information or even to take control of the target. Since this communication must remain unrevealed; that may be achieved *"by circulating the traffic, by using port hopping or by encrypting the communication"* (Palo Alto Networks 2016, p.16).

Firewalls are a traditional means of protection from malware attacks; firewalls use protocols and ports in order to identify the filter the traffic in the PC network. The malware has the ability though to hop from port to port; in that case, the firewall is totally ineffective since the malware infection will eventually find an open connection to the network (Walker, 2015).

Currently, a new generation of firewalls is under construction where the classification of the PC traffic will be based beside the ports and the protocols on a process where each application will be analyzed and then it will be decrypted and decoded. In that way the true identity of what circulates in the PC network will eventually be revealed; the pin-pointing and analysis in depth of the PC network's traffic will be the major features of the next generation's firewalls. These features will be absolutely priceless in the fight against malware (Palo Alto Networks, 2016).

5. Network scanning

By the term network scanning, we refer to an identifying procedure of network hosts who are maybe active; the reason for that is either their attack or security assessment of how safe this specific network is.

There are several scanning procedures such as the ping sweeps and the port scans; under these procedures, information is returned regarding the IP address and which of them map to live hosts. The inverse mapping is another method which also returns information on whether an IP address maps or not to live hosts; through that method, a potential attacker becomes able to identify which addresses are viable or which are not.

Scanning is for the attacker one (1) of the three (3) components of intelligence gathering. The first one is known as footprinting phase, where the attacker creates the profile of its target after having gathered all the required for that information i.e. its e-mail server, the range of its IP address and its DNS (Domain Name System). That information is available online.

The second phase, known as scanning, is when the attacker has collected the information regarding the specific IP addresses, their operating systems and the services that run on each PC; in the last phase, known as enumeration, the attacker gathers the information he finally needs such as the user of the network or the names of groups, the routing tables and the SNMP (Simple Network Management Protocol) data.

3.2.2. Stages of a cyber-attack

A cyber-attack is an action that goes through several stages that vary in length and "quality"; the time that each stage will last is determined by factors such as the attacker's incentives and motives and or the toughness of the implemented by the company relevant security controls.

The stages of a cyber-attack are the following (Walker, 2012):

1. Reconnaissance and enumeration

2. Delivery

3. Breach

4. Effect

More specifically:

1. The first objective of the attacker is to find a target; the sources which are public and thus open provide to the potential hacker a lot of information. The gathering of that information before the implementation of his "plans" is known as reconnaissance; rather valuable information for the hacker is the understanding of the credentials of the computer or of the whole network, of the software versions which are being used

and of the settings which are configured properly. The gathering of that information may be complemented sometimes by monitoring and analysing or sniffing the flow of the actual data from the shipping company to the vessel and vice versa.

By the term enumeration we refer to the checking and probably testing of the system's vulnerabilities that the attacker has discovered in the reconnaissance phase; when i.e. not-updated antivirus software is being detected the hacker gets ready for his attack.

2. Once the potential attacker has detected the vulnerability of the targeted system he may find a way to penetrate into the network; his attempt to illegally get an access to the company's or vessel's data may be implemented within the company or the vessel but sometimes through internet from a remote place; for example the attacker may use the online services of the company such as the cargo's tracking system, an e-mail containing malicious elements or containing links to malicious websites, a false website that would lead its user to the disclosure of sensitive personal information.

3. The extent of the potential breach of security and penetration of the attacker into the company's or vessel's data depends on the extent of the detected by him vulnerability. The breach does not always result to changes in the equipment's status and thus it is not noticeable easily. The attacker is able to proceed to changes such as to manipulate the information that is being used for the navigation or to access sensitive data regarding the cargo or to achieve the control of the machinery system of management.

4. The effect of the attacker's action is determined by both his incentives and his objectives i.e. he maybe wants to get access to sensitive commercial data which are highly confidential and manipulate the crew or data regarding the cargo.

It is very important to educate and train the members of the on-board crew of the vessels so that they can be able to know what risks exist and furthermore how to react if something occurs in order to mitigate the upcoming consequences.

3.3. Definition and Identification of vulnerabilities

Each shipping company performs assessments regarding the threats that may face; in that assessment, the threats that derive from potential cyber-attacks to either the company or the vessel itself are also included. These assessments are essentially an examination of how vulnerable the company's systems are.

The checking and then reporting of the systems were implemented by experts, either internal, namely employees of the company and external that have deep knowledge of both the computing systems and the maritime industry. Of course, there are differences between the computing systems of the shore company and of the vessel; IT systems are focused to the usage of data as information while the OT systems are focused on the use of data as part of a monitoring process.

Systems that stand alone are much less vulnerable to cyber-attacks compared to those which are attached to a probably uncontrolled botnet. It is rather important to understand that when a system is connected to a botnet which is not controlled then the human element plays a crucial role and an accident may occur.

3.3.1. Vulnerabilities ashore

In order to understand the vulnerabilities that may exist and may be exploited by a cyber-attacker, it is rather important to consider of all the evolutions that occurred in the maritime industry. First of all, the invention and wide use of the container changed radically the way that the cargoes are being transported; before that the goods were loaded on-board a vessel and then they were unloaded from it as a break bulk cargo; due to that the goods were organized in a loose way, meaning by size or by quantity. The loading was executed either by hand or by cranes; that procedure was very tiring and mainly time-consuming.

A truck driver invented in the '60s the shipping container which caused a revolution in the maritime industry; the loading, unloading, sorting and transportation of the cargoes all around the world changed radically. Due to that development, both the vessels and the port terminals had to be equipped with all the necessary tools in order to implement all the necessary operations efficiently.

Currently, the infrastructure for the loading and discharging of containers consists of cranes and personnel, trains and trucks; some ports also possess items like the Transportation Worker Identification Cards (TWIC), security cameras, unmanned

GPS cranes, and cargo tracking systems. These systems due to their connection with IOT infrastructure they are extremely vulnerable to cyber-attacks.

Here are some related to the maritime industry cases of cyber-attacks (Lelli, 2014):

A. A case of drugs smuggling occurred in the port of Antwerp, Belgium where some individuals tried to access the computer system of the port with a technique of spear-phishing; these individuals were associated with drug cartels. Several workers of the port received e-mails with links that contained malware; if the receiver of the e-mail downloaded that link his pc would be contaminated and the hackers would be enabled to access the computers of the port from the back door. The workers did not click on the link though and the attack was postponed for a while.

The attackers proceeded to other methods such as the breaking into the port offices where the computers were located; these computers were linked to the rest of the network system of the port. The hackers installed on the computers key loggers which were specially designed to allow the control of the whole computing system of the port; in that way, they became capable of gaining access to the system remotely.

In the terminal where equipment for the handling of containers was kept, there were manifest lists of cargo; these lists were changed by the attackers. Furthermore they altered the pick-up date of a shipment full of drugs along with the location of the container in order for it to be in a place where they would be able to bring their own truck into the port area and haul the container with the hidden drugs, namely 1.044 kilograms of cocaine and 1.099 kilograms of heroin.

B. In 2011 another incident occurred which had to do with the infliction by IRISL (Islamic Republic of Iran Shipping Line) which resulted to loss of many crucial files; more specifically due to a cyber-attack all the data regarding the loading, unloading and tracking of containers were erased.

In order for the hackers to do that they gained access to the global movement of goods of this line and they disrupted completely the internal network of communications due to which its cargo operations became unavailable on a global basis. The financial damage of the company was huge.

C. An employee of an oil refinery used a USB device in order to load malware onto the computers of its company. After having completed that criminal activity on a computer he continued on spreading the malware; the result was the infection of the entire network of the company. That type of threat that comes from the inside of companies is rather often in the cyber world and especially in that of the maritime industry.

D. Another incident where an oil ring located off the coasts of Africa occurred; more specifically malicious malware was loaded on computers of the oil ring and they were shut down due to it.

The oil rigs have a complex network which was used by the attackers for its tilt; in other words they try to compromise the stability of the oil ring which is essential for the safety of the people who work there and the surrounding environment since it could result to the loss of human lives and to oil spillages.

3.3.2. Vulnerabilities of the vessel

As far as the cyber-security on-board vessels is concerned we may say that just like the development in ports and infrastructures the vessels also have become more modern in order to follow with the new “era”. The new systems include innovations regarding the i.e. the navigation, the suppression of a potential fire and the data recorders; all these innovative tools use cyber systems in order for their operation to be as effective as possible.

The modern vessels have a wide spectrum of systems and programs that the seafarers use for its proper operation and navigation. The wheelhouse mirrors whatever someone who is not trained may see and understand; a modern wheelhouse is a room full of screens, levers, buttons and switches while the navigators on the bridge are there typically and use several systems, probably redundantly, in order to be sure that the vessel in on track and it moves towards the pre-agreed direction with the proper speed. The navigation systems use programs which are computer-based and furthermore they use GPS data for the display of the location, course and speed accurately and vividly; all these systems make the responsibility for the navigation easier and the navigation itself safer.

The On-board systems may include the following sub-systems:

1. Cargo management systems

2. Bridge systems

3. Propulsion and machinery management and power control systems

4. Access control systems

5. Passenger servicing and management systems

6. Passenger facing public networks

7. Administrative and crew welfare systems

8. Communication systems

More specifically:

1. The Cargo management systems are digital systems which are used for the management and stevedore of the cargo, even the dangerous and hazardous ones; these systems interact with various relevant systems ashore such as the system that tracks via the internet the available tools for the shippers. Due to these interactions with other digital systems the cargo management systems are extremely vulnerable to potential cyber-attacks.

2. Bridge systems are vulnerable to cyber-attacks due to the use of digital navigation systems which interact with the relevant systems ashore for i.e. update; we have to notice here though that even bridge systems which are not connected to other systems may be also vulnerable. A cyber-attack where bridge systems are involved may face i.e. a manipulation or a service denial which will then affect all other systems that have to do with the navigation such as the VDR or the Radar/APRA.

3. The propulsion and machinery management and power control systems become vulnerable due to the use on-board of digital systems for the monitoring and control of

the machinery, the steering and the propulsion; that vulnerability is even more increased when all that equipment is used with other pieces of equipment which are remotely based.

4. The access control systems are digital systems which are used for the safety and security of the vessel and of the cargo on-board; that system includes also the surveillance, the security alarm on-board and the electronic "personnel-on-board" systems.

5. The passenger servicing and management systems are also digital systems which are used for the management of property and the control of access and boarding of passengers; all the contemporary electronic devices that people carry on-board with them such as tablets may also become tools for a cyber-attack since they can be used for the collection of data and the transfer of that data to other systems.

6. Passenger facing public networks means that networks either wireless or fixed which are installed on-board and they are connected to the internet for the passengers to use them are usually uncontrolled and thus they may be used for the collection of confidential data.

7. The administrative and crew welfare systems are networks which are installed on-board for the administration of the vessel along with the entertainment and welfare of the crew; these systems are extremely vulnerable and they could be exploited by a potential cyber hacker for the collection of data. Since these systems are uncontrolled they must not be connected to any other system that has to do with the safety of the vessel. That category also includes the software that the management of the vessel provides to its crew.

8. The communication systems increase the vulnerability and the service provider must implement defence mechanisms in order to secure any possible system and data on-board.

A very interesting case of spoofing was when a team for a US University in Texas took remotely the control of a yacht without changing the members of the crew who were in charge for the navigation; the yacht had a GPS system which was spoofed by a device specially designed for that purpose. That device has the size of a briefcase and it enabled its user to send false signals from the shore so that the navigation is distracted (Zulmat, 2013). That scenario is feasible for every type of vessel with the results to be very serious.

3.3.3. Cyber Propaganda

Another highly concerning issue is that of the sponsors by states of cyber weapons such as in North Korea where an intrusion is alleged to be made into Sony Pictures and digital blueprints of American fighter jets were stolen (Sanger & Perlroth, China's Cyber-Theft Jet Fighter, 2014).

Captain Anillas, head of the operations for the Navy in Peru, gave an insight regarding the ambitions of the government in Peru as far as cyber operations are concerned. He argued that his research was deeply influenced by a decision of the International Court of Justice in Hague concerning a dispute between Chile and Peru:

"Analysing Chile as an objective target, it is a country that shows respect for international law in the international public opinion arena, manifesting it in repeated forums and international appointments. But it has been carrying out an information strategy with the purpose of discrediting Peru. On May 23 of this year the newspaper "El Comercio" testifies to this when reporting that a 209 submarine had been detected in its waters, in an effort to prove that Peru is an aggressor country. It is therefore recommended to pursue the following Information Operations strategy, which covers all possible levels (strategic, operational and tactical), to consolidate the superiority of information: In the areas of intelligence, exaggerate information regarding military equipment, considering all submarines operational, which could generate a dispersion of Chile's forces that are concentrated in the North, to reinforce its ports and bases in other naval zones, for the possibility of an underwater attack on their Internet communications cables or the possibility of using special operators. To create intelligence agents and/or special operators in the bases and centers of command and control, with the purpose that said operators activate with order, computer viruses that affect their computer systems, or alter the information of their databases. We must get the famous Stux-net virus, which as mentioned earlier, affected the Iranian nuclear power plant. Increase the flow of news on the subject in the most popular local media, such as radio and television, reinforcing the idea that we are a country respectful of International Law, unlike Chile, who must be

presented, as a country that seeks permanently to expand and for which it has been prepared militarily in all these years.”.

Chapter 4

Data analysis

4.1. Cyber-security in vessels

Cyber security is a concept which exists for some decades now but for the maritime industry, it is rather new. All the new opportunities, which are created due to the use of software and hardware systems along with the networks of computers, are found both on-board vessels and ashore. In parallel, several issues have emerged regarding the security of data and communication that circulate and are exposed to malicious use.

Since there is no specific definition of cyber security we may say that knowing how vulnerable digital resources are and realizing where the cyber-risks may come from may be used as one. Although the term cyber security is used quite often, its context is very subjective and thus its meaning varies according to the special features of each case (Bay, 2015). As far as the maritime industry is precisely concerned we may say that in the scope of the cyber security we may include the protection of the electronic systems and equipment used either on-board and ashore from potential cyber-attacks along with the protection of the networks used for the communication from malicious actions which may lead to the authorized access to data and information and i.e. their destruction (Bishop, 2005).

The importance of cyber-security has been acknowledged for many years now but as the technology evolves it becomes more and more essential; currently, we must always have in mind that a possible cyber-attack may occur even when a small electronic action is performed. As far as vessels are concerned the security in every level is crucial since it is extremely difficult to be gained while it is the to be obtained while on the same time a lot of money is involved; for these reasons the integrity of the systems is of huge importance.

Several rules and regulations have been issued regarding the concept of cyber security which was converted due to that in a rather complex notion. The legislation for the protection from cyber-attacks and the achievement of cyber security is huge while all the electronic aids which are used for the navigation such as the GPS, the AIS and the ECDIS have several weaknesses (Tucker, 2015). More specifically:

1. Legislation and guidelines

In 2016 IMO published the Interim Guidelines on Maritime Cyber Risk Management (No 1526, June 2016). According to these provisions, the cyber threats exist for real and thus things must be done for them to be prevented (IMO 2016). There are not any specific suggestions on how to achieve that though; the only thing that these guidelines provide is that the information technology must be distinct from the operational technology system (IMO 2016).

That document has many gaps and furthermore, it has rules which are not mandatory; due to that, the IMO passes the liability to the shipping companies and to the suppliers of the IT systems. Although the computers have been for many years now essential tools onboard vessels IMO has not still managed to provide the appropriate guidelines as far as cyber security is concerned; we must admit here though that the vessels are very different the one from the other and thus it is rather hard to create rules and instructions applicable to all of them.

In order for the cyber security to exist onboard and onshore the shipping companies must follow specific procedures; according to Bridge Procedures Guide (2016, page 59) *"The exchange of electronic data between ships and shore authorities, service providers, charterers and owners/operators have increased significantly over recent years. The use of electronic data exchange, including updates to navigational systems and software, exposes users to the possibility of unauthorized or malicious access. This creates a risk to the safety and security of shipboard systems. To protect commercial interests, as well as to ensure that safety and environmental protection are not compromised, it is important that seafarers comply with Company cyber-security procedures. Company procedures should consider industry guidelines as well as any regulatory requirements addressing cyber-security".*

The above mentioned description of the concept of cyber-security is rather vague and thus ambiguous; no recommendations or guidelines are given to the shipping companies which show that the maritime industry, in general, has not been so far able to adapt to the fact that technology threats exist and measures must be taken for their prevention.

The concept of cyber security is currently mentioned only by few shipping companies in their Safety Management System; that mentions are vague and ambiguous though that do not lead to any specific actions that the shipping companies must take in order to be protected from a potential cyber-attack.

The development of safety and security in the maritime industry depends a lot on the classification societies like Lloyd's Register which issued in 2016 guidelines regarding the cyber-security. That document is rather extensive and it deals with several different areas of ICT (Information and Communication Technology) such as the area of cyber security while on the same time it recognises that all the seafarers must receive the appropriate relevant education (Lloyd's Register, 2016).

Since the vessels do not possess broadband of 50+ Mb (Mega-Bites) but a far slower connection, if a cyber-attack occurs and important files will be possibly damaged or even lost, the time needed for their re-built or re-download will be very long. The majority of vessels do not possess on-board systems discs for their operation or proprietary software and drivers. That slow connectivity is a vulnerability of the system itself and probably they must be designed from the scratch (Lloyd's Register, 2016).

What must be mentioned here is that the main purpose of the ICT systems is help the members of the crew on-board to fulfil their tasks; the guidelines which are issued by the Lloyd's Register provide that kind of help to the seafarers without having the force to be obligatory (Lloyd's Register, 2016).

2. ECDIS

The ECDIS (Electronic Chart Display and Information System) is a navigational tool; more specifically it is a chart system which is used by the vessels that facilitates their navigation since it enables the crew to pinpoint exactly the locations with the use of the GPS (Global Positioning System) and thus to direct the vessel to its destination.

The ECDIS is a very useful tool for the vessel; for that reason, it became from July 2018 mandatory for all vessels to have it on-board and to use it. It is essentially a computer where navigational software is installed; for its utilization, it is connected with other navigational equipment such as RADARs, ARPA, Echo-sounder etc. The information which is contained in other publications such the "Sailing Directions" or "Tide Tables" are also incorporated and displayed by the ECDIS; that information may concern the weather or the ice conditions (Bhattacharjee, 2017).

There are two (2) types of ECDIS charts (Bhattacharjee, 2017):

1. RNC (Raster Chart) is an identical copy of a paper chart that shows in print all the information; that chart may grow smaller or larger when it is zoomed out or zoomed in and when it is rotated everything is also rotated.

2. VNC (Vector Chart) is computer generated; therefore all the included in it information may be turned on or off depending on what the user wants to do. If someone clicks on information more details will appear; furthermore, depths are monitored so that a potential grounding may be avoided.

The ECDIS complies with the Regulation V/19 of IMO and the Regulation V/27 of SOLAS since it displays information from a SENC (System Electronic Navigational Chart). The ECDIS equipment can be used instead of paper charts; in that way, the navigation is easier since the planning of the sea route, its monitoring and the giving of ETA (Estimated Time of Arrival) are given automatically. Additionally, the ECDIS enhances the safety of the vessel by i.e. monitoring continuously all the data regarding the navigation and then by analysing it.

In practice, ECDIS is not been used since the majority of the computer systems run an obsolete software and several issues evolve such as the slow downloading of the new route. Furthermore, they usually run Windows XP that has "zero-day" vulnerability due to the fact that no security updates are received (Rains, 2013). The ECDIS is rarely connected to the internet though and therefore it is difficult to be infected remotely; the cyber- attack may occur when the officer proceeds with the instalment of an update to the system and thus the system becomes vulnerable and may suffer damages or even loss of valuable information.

The computers that use ECDIS are not protected since no antivirus software is installed on them; the main reason for that is that the computers are unable to run both the navigation software and the antivirus software on the same time since they do not so much power. Furthermore, some Antivirus software do not support Windows XP anymore.

Under a survey conducted by the NCC Group regarding the vulnerabilities of the ECDIS several flaws were detected such as the fact that a computer with basic configurations and without an installed firewall was able to browse or download any of the files which were stored in the specific computer and furthermore they were able to upload or delete any file on the ECDIS Windows 7 system (NCC Group, 2014).

3. AIS

The AIS (Automatic Identification System) is a tracking system which is used by the vessels but also by the VTS (Vessel Traffic Services). The information provided by these systems supplements the marine radars which are the basic method for the detection of vessels and thus for the avoidance of potential collisions.

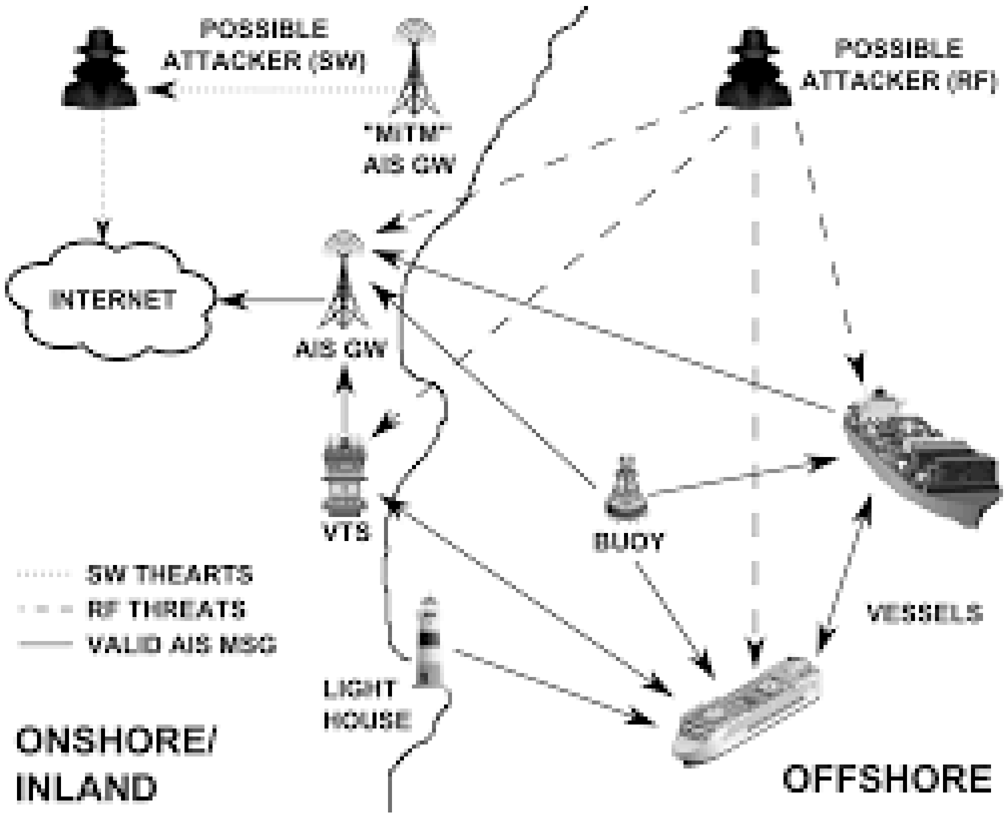
The AIS provides information regarding the position, the speed and the route that a vessel follows; that information is displayed on a screen or on the ECDIS. That system helps the watch-keepers, along with the maritime authorities to monitor all the vessels and their movements; for that purpose, a VHF (Very High Frequency) transceiver is used that has a GPS system along with other electronic navigation sensors. When a vessel possesses VHF it can be tracked by the VHF system which is based on the shore and when it is far away from the coasts by a VHF system installed in a satellite (Balduzzi et al, 2014).

Since 2002 the AIS has become mandatory for all the vessels that sail in international waters of 300 GT or more and for all the passenger vessels also. That system has improved a lot the safety of the navigation especially when the weather conditions are not good i.e. the visibility is low. Furthermore, it is an important aid during the investigation of a marine incident and during a rescue operation; the relevant information is also sent to internet sites such as vesselsfinder.com or marinetraffic.com. AIS is able to send up to 27 types of messages.

AIS remains still though quite vulnerable to external threats since there are no security measures for it yet. First of all, AIS communications do not make any kind of authentication control and they do not employ checks regarding the integrity of the collected information; furthermore, the communication is made over RF and thus it is extremely easy for someone to steal the information and i.e. tamper it.

"IMO and more specifically the Maritime Safety Committee agreed during a session (the 79th) that was held in 2004 that "in relation to the issue of freely available automatic information system (AIS)-generated ship data on the world-wide-web, the publication on the world-wide-web or elsewhere of AIS data transmitted by ships could be detrimental to the safety and security of ships and port facilities and was undermining the efforts of the Organization and its Member States to enhance the safety of navigation and security in the international maritime transport sector. The Committee condemned the regrettable publication on the world-wide-web, or elsewhere, of AIS data transmitted by ships and urged Member Governments, subject to the provisions of their national laws, to discourage those who make available AIS data to others for publication on the world-wide-web, or elsewhere from doing so. In addition, the Committee condemned those who irresponsibly publish AIS data transmitted by ships on the world-wide-web, or elsewhere, particularly if they offer services to the shipping and port industries" (IMO, AIS transponders, Maritime Security).

The following picture presents how a cyber-attack of an AIS system may occur (Balduzzi et al, 2014).



There are three (3) categories of identified threats which are related to the AIS, meaning Spoofing (sending of false information), hijacking and availability disruption; however, it is possible to avoid all the threats if the AIS data is compared to other sources (Balduzzi et al, 2014).

4. GPS

By the term GPS (Global Positioning System) we refer to a device which is used for the determination of the position of a ship in the open sea; that device collects information which is then being used by several navigational systems. In other words it helps the mariners to navigate, to measure the speed of the vessel and to determine exactly where the vessel is located.

GPS has essentially changed the way that the maritime industry operates both in normal conditions or when a search and rescue operation is conducted. While the conditions are normal the GPS helps allocate the vessel in the open sea but also in harbours or waterways that are congested. It is very important to know the exact position of a vessel when it enters a port or when it leaves from a port since a potential traffic jam or a sudden change of the weather conditions may lead to an incident.

Both mariners and scientists like the oceanographers use the GPS very much since it helps them in i.e. navigation under difficult conditions such as a hazardous location or for a survey which is conducted underwater. The fishing fleets also use the GPS a lot for their activities since it enables them to find the best fishing spots while on the same time it helps them to be sure that they comply with the relevant rules and regulations.

Currently, an enhanced GPS signal is being used which is known as DGPS (Differential Global Positioning System); that signal provides more accurate information regarding the position of the vessel and thus increases the level of safety. That signal is often used for activities such as the positioning of buoys, dredging or sweeping; furthermore, the navigation inside a harbour becomes much better and effective.

GPS is very important not only for the vessels but also for the management of the maritime port authorities; when the GPS is combined with the GIS (Geographic Information System) both the operation and the management of the port facilities such as the cranes for the loading and discharging of containers becomes much more efficient.

As already stated above, the GPS is included in the AIS which is approved by the IMO for the tracking and control of the traffic of the vessels especially in waterways that are very busy. That system is used for the navigation but also for the security of the ports and the waterways since it provides to the people in charge all the necessary information regarding the vessels and the cargo on-board it (Hi-Marine, 2016).

In 2013 a group of students from the University of Texas along with their professor, Todd Humphreys, decided to make a test in order to prove that the GPS is spoofy; what they did was to replace a genuine GPS signal with a fake one that was showing that the vessel was out of its original route (Psiaki & Humphreys 2016). A GPS device is not capable of identifying whether a signal is real or not; the same people that sent the spoofy signal worked on the counter-measures for it. When GPS signals are genuine they come from different directions and from various satellites; on the contrary, the fake signals will come only from one source. That fact may be used in their defensive device which is able to understand within six (6) seconds whether a signal is fake or not (Psiaki & Humphreys, 2016).

5. Integrated Bridge

By the term integrated bridge system, we refer to *"A series of interconnected and closely grouped screens and modules allowing centralised access to navigational, propulsion, control and monitoring information. The aim of IBS is to increase safe and efficient ship management by qualified personnel."* (Wartsila Encyclopaedia, 2017, p.82). In other words, the integrated bridge is a combination of systems which are connected in order to allow central monitoring of all the available tools which are used for the navigation. A lot of information regarding the operation is acquired through that system such as information on the execution of a passage or information concerning the safety and security of the vessel.

The IBS is a management system of the navigation which essentially links the other systems in order to provide all the details that concern the navigation of the vessel; what is remarkable is that all types of vessels have the same IBS.

Every IBS must be able to support at least two (2) of the following perspectives:

1. Execution of passage
2. Communications
3. Machinery control
4. Cargo operations
5. Safety and security

IBS is not mandatory; the criteria for the installation and design are drafted by the classification societies such as DNC; factors that determine the layout include the design of the bridge, the type of the fitted equipment or the place where they are located on the bridge. There are four (4) major parts in each IBS:

1. Technical System
2. Human Operator
3. MMI (Man Machine Interface)
4. Operational Guidelines

According to the Regulation 19, paragraph 6 of Chapter V of SOLAS *"Integrated bridge systems shall be so arranged that failure of one sub-system is brought to the immediate attention of the officer in charge of the navigational watch by audible and visual alarms, and does not cause failure to any other sub-system. In case of failure in one part of an integrated navigational system, it shall be possible to operate each other individual item of equipment or part of the system separately."*

The bridge integration is from late 1960; back then the computers were not advanced and analogue connections (transmitters, receivers, pulses and analogue DC voltage) were used for the interfacing of the various devices. Currently, due to the development of technology serial cables are used for the various connections of the navigational equipment in accordance with the Marine Industry Standard Serial Data Communication; in that way, all the devices become compatible the one with the other. Analogue information is still used however for some devices i.e. the rudder angle indicators or the propellers (Hi-Marine 2016).

What happened up until recently what that the navigational devices were bought separately the one from the other; this means in practise that it was very possible that the devices would not be compatible the one with the other. Currently, the bridges are always integrated since all its parts come from the same manufacturer; in that way, the shipping company is positive that the parts of the equipment will be compatible between them (Hi-Marine, 2016).

Devices such the ECDIS or the RADAR receive information from various input sources; that data is transmitted through serial cables and in our days with Ethernet cables. In the future the devices for the navigation will be all connected by a single network in order for the procedure of cabling to become easier; there are still some issues regarding the security though i.e. if an ECDIS is connected to the internet the whole system of the vessel will be also connected to the internet; in that way the navigational network will be exposed to several cyber risks and thus measures must be taken in order for cyber security to be provided and potential unauthorized access to be prevented.

6. On-board computers

On-board a vessel there are several computers which are used for various tasks; some of the most crucial function which are implemented by a computer is the calculation of the stability of the vessel and the exchange of data and information with the offices of the company on-shore and with the competent authorities. The majority of the on-board computers are connected with the internet all the time and thus they exposed to several cyber risks; the computers which are used for the control of the main engines or other machinery on-board or those that monitor sensor data are not connected continuously to the internet though. The use of ICT increases their efficiency when the computers have the proper design while on the same time they become safer since the monitoring is improved and the communication and awareness on the bridge or in any other operational area become better (Lloyd's Register 2016).

A major vulnerability for the onboard computers is the e-mail addresses of the members of the crew which are almost always formed in a specific way, namely as "jobtitle.shipname@shippingcompany.com". If a potential cyber-attacker wants to guess the e-mail addresses of the members of the crew his task is rather easy since in almost all cases they will the above described form.

In 2015 a study was conducted by the Panda Security under the name "Oil Tanker, the Phantom Menace" where it was proved that it is very easy to infect a PC since all it takes is just the opening of a PDF file which then opens to several other files which collect information for the future attacker (Panda Security, 2015). The malware uses tools which are absolutely legitimate and in that way the antivirus protection is not able to detect them.

Apart from the computers which are used for several tasks on-board such as the navigation, there are also many computers which are used by the members of the crew for their personal entertainment; these computers are available to everybody and as you may easily understand the perfect tool for a potential cyber-attacker. Special attention should be also taken by anyone who uses a USB device since it is rather possible to infect i.e. a computer.

Regarding these issues the regulations which were drafted by the IMO were almost completely incapable to offer essential protection; to be clearer there not any regulations that may offer protection to the on-board computers since the only reference that IMO has done regarding that matter is the “MSC/Circ. 891 Guidelines for the On-board Use and Application of Computers from 1998”. Back at that time, the computers were very few and even fewer were found on-board vessels; this means in practice that a regulation which is drafted back then may not for sure all the matters that exist today. However, that regulation is still in force; even SOLAS 2014 refers to it. Although the onboard computer systems should be protected against all the potential cyber-attacks there are no means to achieve that yet.

4.1.1. Education of the professionals

When someone wants to become a professional seafarer he must be educated and trained; the STCW code which is issued by IMO dictates exactly what the seafarer must learn in order for him to become capable to work on-board a vessel. In 2012 the STCW was amended; however, there is no mention of the word “cyber” anywhere in that text. Someone who wants to become an electro-technical officer must be able to understand the following issues: “main features of data processing, construction and use of computer networks on ships, bridge-based, engine-room based and commercial computer use” (STCW 2011, 172). We have to mention here that even today the majority of vessels do not possess an electro-technical officer but they have an electrician or in the worst scenario no one who may understand the network of the vessel.

The officers of the deck are obliged to learn how a computer works and to be able to use the radio equipment which is based on a computer; furthermore, they must know how to fix a potential software problem (STCW 2011, 320). Even though the fact that the computers are a rather important part of the shipping industry for many years now, the SCTW Code does not mention them at all. Things are starting to become better though i.e. in several shipping universities courses related to IT education started to be part of the program.

4.1.2. Insurances

A rather interesting point regarding cyber security is to investigate whether a cyber-attack would be covered by an insurance policy. Currently, the insurance contracts include clauses that exclude cyber-attacks from the risks that may be covered and thus the liability is removed from the insurance companies; such clauses may have the following structure:

"1.1 Subject only to Clause 1.2 below, in no case shall this insurance cover loss damage liability or expense directly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software program, malicious code, computer virus or process or any electronic system.

1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1. Shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system computer software program, or any electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile" (Hellenic Shipping News 2016).

4.1.3. Automation

Things change very quickly i.e. the sending of the consumption of fuel by internet to the offices of the shipping company is already a fact; furthermore, the access of the automation system of the vessel may be implemented remotely i.e. a vessel which is equipped with Wartsila's Integrated Automation System, the Wartsila's service personnel is able to connect to the vessel via a VPV connection and have the same view that has the engineer who is found on-board. Wartsila says that *"even though it is possible to make corrections remotely, they will then guide the crew to make those corrections instead of making the changes themselves remotely"* (Wartsila, 2016).

As we stated above the modern vessels possess integrated bridges and thus the navigation is absolutely automatic i.e. when a route is planed the autopilot will drive the vessel to its destination automatically or when a vessel is equipped with a dynamic position system the propulsion system is controlled by a computer that implements the orders of the competent officer. This system relies heavily on accurate GPS data to keep the vessel in place, making if rather vulnerable to spoofing.

4.1.4. Autonomous vessels

Rolls-Royce is currently studying a project of replacing the conventional vessels with automatic ones; that project, known as AAWA (Advanced Autonomous Waterborne Applications Initiative) is funded *"by Tekes and they have co-operation with several Finnish universities. They are now studying technological, safety, legal and economic aspects of autonomous shipping. They claim to have a proof of concept by the end of 2017 and to have a remote-controlled vessel in commercial use by the end of 2020. In their vision, they will have an ocean-going autonomous vessel in 2035" (*Rolls-Royce, 2016).

During the Autonomous Ship Technology Symposium 2016 that took place in Amsterdam in 2016, Rolls Royce presented the Advanced Autonomous Waterborne Applications Initiative regarding the transformation of the shipping industry and the entering into the digitization era and gave the following time-table (Autonomous Ship Technology Symposium, Amsterdam, 2016):

2020 → the crew will be reduced due to the remote support and operation of certain functions of the vessels.

2025 →The coastal vessels will be remotely controlled and thus they will be unmanned.

2030 → The ocean-going vessels will be remotely controlled.

2035 → The ocean-going vessels will be autonomous and unmanned.

When a vessel is completely autonomous many sensors inputs are needed; these sensors would be processed by a computer system which is able to operate according to the rules of the sea; in other words a computer is needed which must be capable of making all the decisions regarding the sailing of the vessel while a remote operator will oversee it. Although that project seems extremely interesting several problems would emerge; Antti Aijala listed a few of these problems in his bachelor's thesis under the title *"The Risks of Operating an Autonomous Vessel"*; the first one is the transmission of data since there no means yet for doing that quickly and effectively from a distance (Aijala, 2015). Furthermore, the communications should be extremely accurate, scalable and supported by several systems which would eliminate the potential risks and on the same time would create redundancy (Rolls-Royce 2016). Finally, even if a vessel is autonomous an internet connection will always be needed and the cyber security would be again threatened.

Since Rolls-Royce acknowledges all the potential cyber risks it argues that the taking of control of a vessel from a distance, if something goes wrong, would be always possible; furthermore they stated that in order to minimize or even eliminate the potential cyber-threats for the computer systems of the vessel measures should be taken for their detection and thus their destruction. Of course, an update of the systems is required while encryption and verification of the data are also mandatory (Rolls-Royce 2016). All in all, the same things that should be taken into account on conventional vessels. Even the human factor remains as the remote operator still has access to the vessel's systems.

4.1.5. Cyber security management

As we already stated above the environment of the maritime industry has changed a lot during the last years due to the technological developments that the world has experienced in general such as the use of internet; the point is that the maritime industry is a rather complex business sector which became due to all these mobile devices that allow the crew and the ashore stuff to access all kind of data and information within a minute even more vulnerable to several risks such as potential cyber-attacks.

The complexity of the maritime industry is not only the fact that numerous elements interact within a digital "space" of the maritime world but also the fact that these interactions are not linear (Egan et al., 2016); due to that complexity the cyber security of the maritime industry is a concept very important which must be treated with diligence.

The problem of cyber security especially for the maritime industry is very serious since the cyber-space offers to the potential cyber-attacker several opportunities to reach his target and be successful. The dynamics of the cyber security in the maritime field have the following three (3) dimensions (Egan et al, 2016):

1. Scale, meaning that the potential cyber-attackers can use the web for their communication or training while at the same time they use it for the scaling of their attacking units.

2. Space is the domain where the criminals may operate; as far as the maritime industry is concerned that space is essentially an infrastructure that supports all the operations.

3. Time is running very fast in the maritime industry and the changes are constant; this means in practice that the potential cyber-security risks keep on augmenting and it is rather difficult for the people in charge to keep up with them. Furthermore, a cyber-attack may place over time and that makes the identification and seizing of the attacker extremely hard.

From all the above-analysed features it is easily understandable that the maritime industry must become capable of finding the way to address the dynamics of the cyber security; the industry must urgently adapt to the nature of the cyber-risks which are constantly changing if it wants to be protected. All the sectors of the maritime industry must improve their strength and their ability to confront a potential cyber incident while on the same time they must find ways to reduce the existing cyber-threats (Rich and Buchanan, 2015). It is rather hard though to achieve these goals; in order, for the maritime industry, to try to be successful, it must first of all, understand that the cyber security strategy which must be followed must be based on assumptions since the cyber risks have a huge variability and may sometimes be unpredictable. For that reason, knowledge regarding cyber security must be constantly updated.

4.2. Cyber safety

The cyber safety is very important since they may affect the safety of the crew on-board along with the safety of the vessel itself and he loaded cargo. Cyber safety has to do with the risks from the potential loss of integrity or the availability of the data that have to do with the safety while the cyber security has to with the protection of the IT and the data from the access of someone who does not have the right to do that or from a possible disruption.

An incident of cyber safety may arise as a result of i.e. an incident of cyber security that may affect the integrity or availability of the operational technology such as the corruption of charts that holds the ECDIS (Electronic Chart Display and Information System) or a failure that may occur during the maintenance of the software.

The causes of a cyber-safety incident may be the same but they may also be different from those a cyber-security one; the measures are taken for both though are based upon the awareness and understanding of the appropriate policies and procedures and the training of the employees.

4.2.1. Procedures

Each company follows several plans and procedures regarding the management of the cyber risk; these procedures should be complementary to the security planning and measures that already exist and mainly to the requirements of the safety risk management which are provided by the ISM (International Management Code for the Safe Operation of Ships and for Pollution Prevention) Code and the ISPS Code (International Ship and Port Facility Security Code).

Cyber security must cover all the levels of a company, meaning from the senior management to even the seafarers since it is part of the inherent culture regarding the safety and security of both the company and the vessels.

Under the chapter 8 of the ISPS Code, each vessel must conduct an assessment regarding the security; this assessment includes all the mandatory operations for its protection i.e. the communications systems, the computer systems and the networks (Paragraph 8.3, Part B, ISPS Code). According to the requirements which are set by the ISPS Code, the vessel must be controlled by being monitored from the shore via an internet connection.

The SMS (Safety Management System) aims to the provision of an environment which is safe and secure; that goal is gained by the establishment of safe practises which are appropriate along with procedures which are based on a report regarding the risks that a vessel may meet that concern the crew, the environment and the vessel itself.

When a vessel faces a cyber-threat that means that something may happen regarding its safety or security; physical effects may happen too. In these cases, the shipping company must assess the potential risks that may arise from the use of OT and IT on-board the ship and take measures in order to confront a potential cyber-incident.

The SMS includes procedures and instructions that ensure the safe operation of the vessels and furthermore they provide measures for the protection of the environment; these measures must comply though with the relevant regulations both international and national, namely that of the vessel's flag state.

These procedures and instructions take under consideration all the guidelines, international standards and of course international codes regarding the potential cyber-risks. When the risk management and the SMS Code is incorporated into a company I must be taken under consideration that each vessel is a totally different situation with different needs; therefore the designed risk assessment and the proposed risk management are each time specifically provided.

The cyber risk management in order to be effective and thus successful should:

- Identify the position of each user and then clarify their responsibilities individually.
- Identify the assets of the company, the existing systems and their capabilities and then predict what each risk may cause if it occurs o them.
- Implement measures which will prevent a potential cyber-incident and thus ensure that the safe and secure operation of the vessel will continue without any disruption. To succeed a configuration of the networks must be included along with their control. Furthermore, the communication and the software must be protected.

- Implement plans and procedures which will provide the required resilience for the protection of a potential cyber-incident; these plans usually include training and education of the involved parties along with the constant update and maintenance of the software.
- Implement procedures which will prepare the parties for a potential cyber-incident; in that way, they will know how to react and thus to confront it effectively.

We have to notice here that several risk management systems include information which is commercially or personally sensitive and confidential; this information must be protected by the companies and must be used only when it is necessary to do that.

4.2.2. Defence

For the defence against potential cyber threats measures of procedural or technical protection are recommended; in that way, the most crucial systems of the vessel are protected while the role of the crew on-board is very important into detecting possible cyber incidents or attacks.

The defence in depth is the approach under which there is a combination of physical security of the vessel according to its SSP (Safe Security Plan) and network protection where segmentation is included along with whitelisting of the software and procedures regarding the use of the media. Finally, the crew must be aware of the risks that exist and furthermore must be familiar with the means of confronting them.

The policies that each company follows must be able to ensure that cyber security is considered to be a major part of the overall safety and security of the company and the vessel. Because the cyber threats may be extremely persistent and complex a defence in depth is needed. In general, when data and equipment are protected in layers they are more resilient to a potential cyber-attack; on-board a vessel though the cyber systems are highly integrated and thus the in-depth defence works only when the protection measures are applied in multiple layers. That defence is characterized as “in breadth” and is used for the coverage of any possible vulnerability of the system.

These two (2) types of defence, namely the defence in-depth and the defence in breadth are complementary the one to the other; when they are implemented together they provide a holistic coverage and protection of the systems against potential cyber threats.

4.2.3. IMO

In June 2017 the MSC (Maritime Safety Committee) of IMO adopted the Resolution MSC.428 (98) on *Maritime Cyber Risk Management in Safety Management Systems*. This Resolution provides that a management system in order to be approved should take into account cyber risk management according to the requirements and objectives of the ISM Code.

The above Resolution was based on the Guidelines on Maritime Cyber Risk Management (MSC-FAL1/Circ.3), namely on recommendations concerning existing risk management practices; what the Resolution did what to confirm that these practises should be used for the address of operational risks that arise from the dependence on systems which are cyber-enabled which is constantly augmenting.

Under the above-mentioned guidelines the following actions should be done for the support towards the cyber risk management to be effective (Gard, 2018):

- Identification and definition of the responsibilities regarding cyber risk management.
- Identification of the assets, the data, the capabilities and the systems of the vessel; if any of them stops operating correctly the vessel will be found in risk.
- Implementation of processes regarding risk control.
- Implementation of measures to prevent a potential cyber-incident and to ensure that the vessel will continue to operate.
- Creation and implementation of the required processes to detect a potential cyber-attack and thus prevent it from occurring.
- Creation and implementation of actions to protect the cyber systems but furthermore to be able to restore them if an attack has occurred.
- Identification of how to protect and restore the necessary for the operation of the vessel's cyber systems that have been hacked by a cyber-attacker.

The Resolution MSC 428 (98) of IMO encourages all the states which are currently members of the Organization to find ways to be protected from potential cyber-attacks; more specifically it urges them to ensure that the cyber risks are addressed in systems of safety management up until the 1rst annual verification of the company's Document of Compliance will take place but surely not later than January 2012.

4.3. Cyber-attacks on vessels

Currently, around 50.000 vessels sail in the seas; the experts of cyber-security argue that it is more than easy for someone to break into the navigational equipment of a ship and hack it. According to the statistics, 17.000.000 attacks occur every week; FDI argued that *"the maritime industry appears still to be ill-equipped to deal with such future challenges as the cyber-security of fully autonomous vessels"* (Grey, 2018). There is a wide range of threats i.e. in the case of Maersk the attackers asked for ransom while in other cases the security is breached and even the people on-board, either they are members of the crew or passengers may be found at danger.

Some major cyber-attacks in the maritime industry that were reported are the following:

1. The Phantom Menace was a cyber-campaign which targeted the sector of oil tankers; the attacks could not be detected by the majority of the existing defence tools. When the investigations were completed it was found that the criminals had stolen data and the "hacks had the hallmarks of a targeted attack" (Stevenson, 2015). The Panda Security that had uncovered the attackers stated that more than 80.000 text files were found stored on a server; these files contained credentials that were stolen from ten (10) companies.

2. The hijacking of Enrico Ievoli, namely of an Italian tanker, off the coasts of Oman in 2011. This chemical tanker was carrying 15.000 tons of caustic soda from Fujairah, UAE towards the Mediterranean Sea and it was captured by pirates off the coasts of Oman.

3. Drug smugglers hacked the cargo tracking system of the port of Antwerp; the attackers managed to have access to the data regarding the location and security

details for the containers and thus they were able to send them to the drivers of the tracks and steal the cargo. That crime lasted for almost two (2) years.

Chapter 5
Conclusions

A major feature of the maritime industry is the fact that it reacts and sets up new rules and regulations only when something tragic and catastrophic happens; a very characteristic example is the accident of the "unsinkable" vessel Titanic in 1912. This incident occurred on 15th April 1912 while the vessel was sailing from the port of Southampton in the UK towards New York City, USA; during that voyage, it hit an iceberg and it sank in the middle of the Atlantic Ocean (History, "This Day in History: April 15").

Titanic left the UK on its maiden voyage with lifeboats and lifejackets only for the members of the crew and some passengers; that lack of safety equipment resulted to the death of more than 1.500 lives. The immediate response to that accident from the global maritime community was the issuing of SOLAS (Safety Of Life At Sea) which set several international regulations and rules regarding the safety (Bender, 2010); more specifically several requirements regarding the safety on-board became mandatory such as the loading procedures, the maximum capacity and the durability. Furthermore, under SOLAS each passenger must have access to a lifejacket.

Currently, the maritime community has the crucial issue of cyber threats to resolve; the cyber-attacks have started to happen rather often and even more frequently than it is officially known since many of the attacks are not reported and some others maybe even not detected (Cyber-keel, 2015).

Although as we have already analysed the maritime industry is rather vulnerable to cyber-attacks still very few are done for their prevention and thus the protection of the industry. The maritime cyber-security and safety are thus very crucial issues that the global maritime industry must urgently face. Since technology and cyber computing systems keel on developing the problem will become more and serious and complex.

All the “parts” that constitute the maritime industry, namely the vessels, the ports, the companies and the related to them infrastructure are sometimes unaware of the protocols and programs which are necessary for the processes, the assets and the people to be protected.

To ensure the security and safety of the maritime industry a combination of initiatives from the state along with international initiatives are necessary; one of the first things that should be done is to train the people who are involved in the maritime industry. In that way, the cyber world will be clearer while the functions of the maritime process will not be influenced.

The shipping must be safe and secure to be efficient and thus to provide its services all over the world; currently, the cyber-security and safety are the most challenging issues that the maritime world is called to face.

The digital infrastructure is prevalent in the maritime industry while at the same time it constantly develops and becomes more refined. The benefits that the maritime industry has due to the innovations are many and very important; the practises which are being followed in work, in the management and the controls are being implemented by all the involved in the parties, either ashore or on-board. These systems though and their innovative practises, require controls and measures for the cyber security to be effectively maintained and thus for them to remain safe.

In our analysis, we referred to several examples of vulnerabilities and potential threats which make clear that the maritime world faces great risks and the need for effective measures to be taken is more than urgent. Cyber security management must be followed; the development and implementation of such a strategy though are rather difficult since there are many obstacles. The need for changes and the objective to achieve a model that could comply with all the parties within the maritime industry which is extremely diverse leads to the introduction of several variables. Coupled with the dynamics of cyber security highlights the need for an effective industry-wide cyber security management strategy.

Thus a strategy regarding the cyber security must be introduced; the management of that strategy could provide the industry with the right way towards a deep understanding of the industry as a whole and its dynamics; that understanding, in turn, would facilitate the protection and put it on a better level. A model should probably be developed that would outline the principles of a cyber-security knowledge management strategy for the maritime industry. The developed model will assist the industry in understanding the requirements for the future.

References

- *Äijälä A, 2015, Riskit miehittämättömän aluksen operoinnissa*
- *Aven, T., Renn, O., and Rosa E., 2015, "On the ontological status of the concept of risk" in Safety Science 49*
- *Balduzzi M., Wilhoit K. & Pasta A, 2014, A Security Evaluation of AIS*
- *Bender D, 2010, "How the Sinking of the Titanic Changed the World," Coast Guard Compass, Official Blog of the U.S. Coast Guard, available at http://coastguard.DoDlive.mil/2010/04/how-the-sinking-of-the-titanic changed-the-world/*
- *Bhattacharjee S, 2017, AIS, Integrating and Identifying Marine Communication Channels, Marine Insights, 2017*
- *Bishop M, Goldman E, 2003, The strategy and tactics of information warfare, Contemp Security Policy 24*
- *Bueger, C., 2015. What is maritime security?, Marine Policy, 53*
- *CESG, Common Cyber Attacks: Reducing the Impact*
- *Grey E., 2018, The state of affairs: is shipping still unprepared for cyber-attacks?, 24/9/2018, available at www.shiptechnology.com/features/*shipping
- *Cyber-keel, 2015, Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas, available at http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf*
- *Egan D., Drumhiller, N., Rose, A. and Tambe, M., 2016, Maritime Cyber Security University Research: Phase 1 (No. CG-D-07-16). US Coast Guard New, London United States*
- *Hellenic Shipping News, 2016, Cyber Risks and Insurance in the Marine Industry, available at http://www.hellenicshippingnews.com/cyber-risks-andinsurance-in-the-marine-industry*
- *Hi-Marine, 2016, Introduction to Operation and Maintenance of Bridge Navigation Equipment*
- *HIS/BIMCO Survey, 2016*

- *History, "This Day in History: April 15," available at http://www.history.com/this-day-in-history/titanic-sinks*
- *IMO, AIS, http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx*
- *IMO, 2016, MSC.1/Circ.1526: Interim Guidelines on Maritime Cyber Risk Management*
- *Joszczuk Januszewska, J., 2013, Importance of Cloud-Based Maritime Fleet Management Software, In International Conference on Transport Systems Telematics, Springer Berlin Heidelberg*
- *Lelli A, 2014, Sophisticated Viknok Malware Proves That Click-fraud Is Still a*
- *Moneymaker for Scammers. Symantec Official Blog, available at Retrieved https://www.symantec.com/connect/blogs/sophisticated-viknok-malware-proves-click fraud-still-moneymaker-scammers*
- *Lloyd's Register, 2016, Cyber enabled ships*
- *Mendes J. and Guerreiro, M, 2017, Conceptualizing the cruise ship tourist experience, Cruise Ship Tourism: 205.*
- *NCC Group 2014, Preparing for Cyber Battleships – Electronic Chart Display and Information System Security*
- *Palo Alto Networks, 2016, Cybersecurity for dummies, 2nd edition, Hoboken: John Wiley & Sons, Inc.*
- *Panda Security, 2015, Operation "Oil Tanker" The Phantom Menace*
- *Psiaki M. & Humphreys T, 2016, Protecting GPS From Spoofers Is Critical to the Future of Navigation, Available at http://www.spectrum.ieee.org/telecom/security/protecting-gps-from-spoofersis-critical-to-the-future-of-navigation*
- *Rich and Buchanan, 2015*
- *Rolls-Royce 2016, Autonomous Ships the Next Steps*
- *Sanger, D.E., Perlroth, N., 2014, December 17, U.S. Said to Find North Korea Ordered Cyber-attack on Sony, The New York Times, Retrieved from https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony hacking.html?*

- *Stevenson A., 2015, Phantom Menace hackers targeting oil sector with malware-free cyber-attacks, available at https://www.v3.co.uk/v3-uk/news/2409148/phantom-menace-hackers-targeting-oil-sector-with-malware-free-cyber-attacks*
- *SOLAS, Regulation 19*
- *STCW Code, 2011, London: International Maritime Organization*
- *Tucci, A.E., 2017. Cyber Risks in the Marine Transportation System. In*
- *Cyber- Physical Security, Springer International Publishing*
- *Tech-Target, 2015*
- *Walker M, 2012, Certified Ethical Hacker, Exam Guide. Columbus, McGraw Hill Osborne*
- *Wärtsila, 2016, Remote Monitoring and Assistance System (RMS), available at http://www.wartsila.com/products/marine-oil-gas/electricalautomation/automation/remote-monitoring-and-assistance-system-rms*
- *Wert M, 2018, Cyber Threats: Definition & Types, available at https://study.com/academy/lesson/cyber-threats-definition-types.html*
- *What is cyber threat, October 2016, available at www.threatconnect.com/category/featured-article*