Università di Genova

DIPARTIMENTO DI SCIENZE POLITICHE
E INTERNAZIONALI

Corso di Laurea Magistrale in: Security and International Relations

-Cybersecurity and the Protection of Maritime Critical Infrastructures-

-Security Studies-

Relatore

Chiar.mo Prof. Fabrizio Coticchia

Candidata/o

Giulia Grasso

ANNO ACCADEMICO 2023-2024

Abstract

Global communication and interconnections have been forged by the internet, nearly every information is transferred through the cyberspace.

This cyber world is not secure and therefore protection must be enhanced. Cyber security is a fundamental against breaches in the cyberspace. It is today one of the most important aspects of security. It is a field that must be further developed and managed.

Cyber security is not just the protection of critical information, it is the approach that aim at protecting confidentiality, integrity and availability of data and assets used in cyber space[1].

Cyber security is not limited to technology but involved people and business processes. Cyber-attacks can cause metaphysical, physical, and reputational damages. Every enterprise must develop a cyber security plan in order to avoid pitfalls.

In the maritime sector, the problem is amplified. Maritime critical infrastructures are one of the most vulnerable targets of cyber-attacks, not only because they highly rely on technologies and IT/OT systems but also because they are a fundamental part of the supply chain.

According to IMO (International Maritime Organization), maritime cyber security is an emerging issue that requires immediate attention[2].

The rapid developments within the internet and technologies, data availability as well as the speed of processing and transferring data present to shipowners and players in maritime infrastructure are a great possibility for operational

[1] "Towards a More Representative Definition of Cyber Security" D. Schatz, R. Bash Roush, J. Wall in Journal of Digital Forensics, Security and Law, 2017

[2] "*Maritime Cyber Security: A Global Challenge Tackled through Distinct*", (https://www.mdpi.com/2077-1312/9/12/1323).

optimization, cost savings, safety improvements and a more sustainable business. All those developments also bring new threats, they increase the potential cyber vulnerabilities and risks.

It is therefore important to understand what cybersecurity is and how to address it in the context of maritime critical infrastructures. Furthermore, it is fundamental to define a set of measures to protect infrastructures and summarize what are the legislative provisions against cyber-attacks at a national and international level.

This research aims at analysing the problems related to cyber security in the maritime sector. We will firstly have an overview of cybersecurity in broad terms, and then we will focus on the maritime industry. The sector is of substantial importance for the world economy and therefore deserve great attention.

In the third chapter, the attempt of numerous national and international organization in increasing awareness, cooperation and training against cyber breaches is examined.

Steps forward have been made, such as the introduction of the European Directive on security of network and information system (that will be later discuss in section III.I) or the IMO cyber risk management documents (analysed in section III.II).

The final goal of this research study is to raise awareness and to improve our understanding of cybersecurity threat in the field of maritime critical infrastructure.

In the last chapter, we will also investigate the disaster suffered by A.P. Moller Maersk in 2017, when an unprecedented cyber-attack, the “NotPetya” ransomware, shout down the entire company’s activities and services.

Index

I. Introduction

Globalization is the widening and speeding up of world-wide interconnectedness in all aspects of contemporary social life (Held et al. 1999, 5). It strongly affects our lives and the way we perceive the world.

Thanks to globalization, trade and investments increased. We saw great economic growth, productivity improved, and the market took advantages from it.

As shown in figure 1, the world trade volume has grown of 4500% from 1950 to 2022[3].

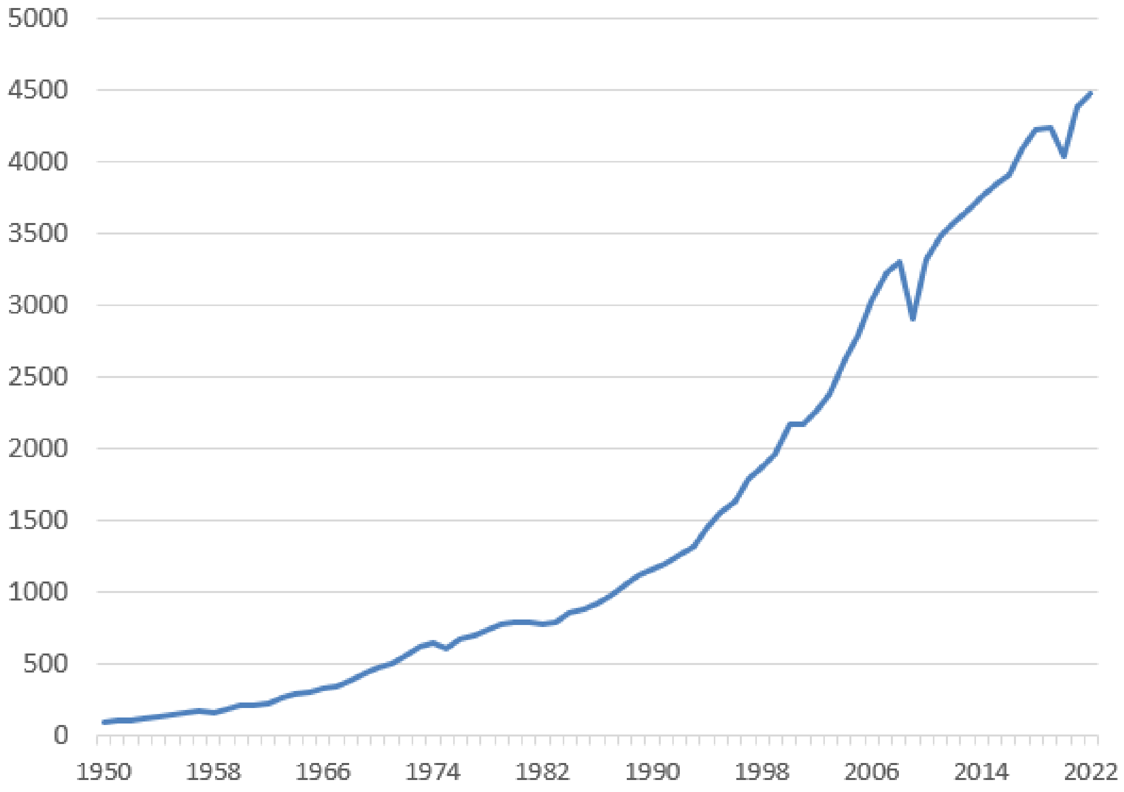


Figure 1 Evolution of world trade from 1950 to 2022, WTO.

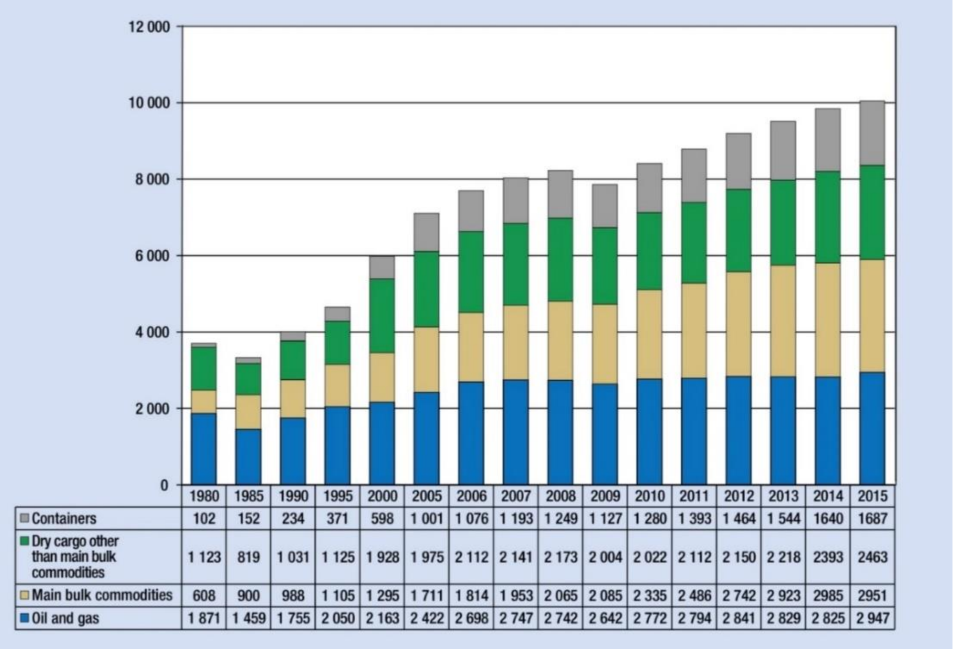
[3] "Evolution of trade under WTO: handy statistics", https://www.wto.org/english/res_e/statis_e/trade_evolution_e/evolution_trade_wto_e.htm

The ratio of world exports and world GDP grew exponentially from the mid-90s and by 1998 it was more than three times what it was forty years earlier[4].

Freight transportation is fundamental for globalization which indeed depends on the trade of raw materials, parts and finished products. The availability of products and their affordability depend much on the capacity to transport them[5].

Maritime transport is the backbone of globalization. As shown in *figure 2* the maritime transportation grew exponentially from 1980, and today around 90% of international trade is transported by sea[6]. Contemporary Global economic trades flows principally through ports.

Ports are the doors for trade, ships are the main vehicle for imports and exports as well as the one of the most used means of transport for people and vectors of the fishing activity. Trade, supply chains and energy rely on the maritime transportation system.



	1980	1985	1990	1995	2000	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
■ Containers	102	152	234	371	598	1 001	1 076	1 193	1 249	1 127	1 280	1 393	1 464	1 544	1640	1687
■ Dry cargo other than main bulk commodities	1 123	819	1 031	1 125	1 928	1 975	2 112	2 141	2 173	2 004	2 022	2 112	2 150	2 218	2393	2463
■ Main bulk commodities	608	900	988	1 105	1 295	1 711	1 814	1 953	2 065	2 085	2 335	2 486	2 742	2 923	2985	2951
■ Oil and gas	1 871	1 459	1 755	2 050	2 163	2 422	2 698	2 747	2 742	2 642	2 772	2 794	2 841	2 829	2 825	2 947

Figure 2 International Seaborne trade (millions of tons loaded) - UNCTAD-

[4] "Globalization and International Trade Policies" R. M. Stern, 2009, World Scientific Publishing CO.
[5] "Transportation and Globalization" J.P. Rodrigue, 2007
[6] "Review of Maritime Transport 2016" UNCTAD, November 2016

Over the past two decades the international maritime trade have increased its dependency on the internet. Maritime transport and related activities are currently conducted by technology-intensive platforms which rely on information systems[7].

The internet emerged rapidly and quickly impacted all aspects of our lives. People can communicate with each other at high speed, and the ease of searchability of information combined with practically unlimited possibilities of exchange, regardless of geographical distances, led to an unprecedented growth in the amount of information available.

Information and Communication Technologies (ICT)'s development is skyrocketing and most of economic, social, commercial, and governmental activities are carried out in the cyberspace. Today, every aspect of our life is carried out on the internet and even Nation State base their activities on the use of complex computer systems and global information networks.

This increasing dependency brought in our world new threats: cyber-threats. The Cybersecurity Act of the EU (Regulation EU 2019/881) defined cyber threat as "any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons".

Their impact is not fully understood, from one side because it is difficult to analyse data and from the other because it is a quite new phenomenon.

However, as cyber threats are spreading and becoming increasingly frequent, cybersecurity turned into one of the serious issues of security.

The International Telecommunication Union, defined Cybersecurity in the Recommendation ITU-T X.1205 as: "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches,

[7] "Global Challenges in Maritime Security", P. Kapalidis, 2020, chapter 8, Springer Editor

actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organizations and user's asset"… "Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment" [8].

As the cybersecurity issue is affecting all aspect of our culture, society, and economies, also the maritime sector that, as we mention before, is increasingly relying on the Internet, must be aware of potential cyber risks.

Ports and maritime operators must enhance their cyber risk assessment. However, empirical analysis shown that there is an alarming lack of knowledge in the field of maritime cybersecurity[9].

Cyber-attacks are dangerous mostly because they are not tangibles therefore it is difficult to initially identify them and when they get to reach the target, they can affect the entire infrastructure, including its fleet, buildings, networks, and offices around the world.

It is fundamental to enact policies and build resilient systems able to resists those attacks. There should be a common methodology for cyber risk assessment but until now, there has not been an efficient effort in this direction. National, and international laws need to be implemented in order to regulate the maritime cyber space.

The reason strategies seem to be ineffective is to be found in the lack of data on cybersecurity incidents, indeed, to avoid reputational and operational consequences, data from affected infrastructures are often kept hidden[10].

[8] "Series X: Data Networks, Open System, Communications and Security – overview of cybersecurity" Recommendation ITU-T X.1205, 18 April 2008

[9] "Global Challenges in Maritime Security", P. Kapalidis, 2020, chapter 8, Springer Editor

[10] "Cyber Risk Management in satellite Systems" C. Kapalidis, C. Maple, M. Bradbury, M. Farrel, M. Fisher, 2019

According to the International Association of Port and Harbors (IAPH), cyber-attacks on ports and harbours have increased by 900% since 2017. The pandemic of Covid-19 increased the scale even more.

ENISA (the European Union Agency for Cybersecurity) tried to introduce a 4-phase approach to cyber risk assessment for ports in its “Cyber risk management for port” report published in December 2020.

The approach is composed as follows[11]:

1. Identification: Identifying cyber-related assets and services. Port operators may enhance their assets and services through the ENISA good practices.
2. Evaluation: evaluating cyber-related assets and risks in order to establish and prioritise security measures. Adapting the guidelines in the context of their risk identification and evaluation methodologies.
3. Adoption: adopting security measures and prioritising those that would be most impactful and practical in each specific context
4. Asset: assessing cybersecurity maturity and priority.

Many international organizations tried to provide guidelines in order to reduce cyber risks, train maritime transportation enterprises, protect the maritime critical infrastructures and finally to enhance awareness.

The European Union, in the last twenty years, adopted many regulatory acts. The first was the EU Directive 2002/21 which created a common plan for information and communication networks among member states. Then we had the Directive 2016/1148, also called NIS (Network and Information Security) which established national competent authority in the field and a national “Computer Security incident response team” to react against cyber-attacks and incidents. This Directive was then abrogated by the Directive

[11] “Cyber Risk Management for Ports – guidelines for cybersecurity in the maritime sector” A. Drougkas, A. Sarri, P. Kyranoudi, December 2020, ENISA

2022/2555 or “NIS-2” which reinforced the first Directive key points and added the will to engage into a strong collaboration between nation States in the field of cybersecurity.

Also, Nation States have enhanced their awareness toward cyber risks, in the Italian case we had various law that reinforced the protection against cyber threats. One of the last interventions was the “Decree-law cybersecurity” that defines cybersecurity as the set of activities needed to protect information networks and systems from cyber threats, in order to ensure confidentiality, integrity and availability for the purpose of national security and national interest in the cyber space[12].

The Decree-law defines the distinct roles attributed to the institutions to safeguard and peruse a national cybersecurity strategy[13].

In the following chapters, we will analyse cybersecurity and its role in the protection of infrastructure with a focal point on maritime critical infrastructures, then we will analyse the role of international institution and national institutions in the protection of those infrastructures and finally we will put theory into practice analysing an empirical case, the case of NotPetya ransomware and A.P. Moller MAERSK of 2017.

[12] Law n. 90, 28 June 2024, “Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici”, GU n.153 del 02-07-2024

[13] “Introduzione al diritto della sicurezza pubblica” P. Vipiana, Giappichelli Editore, 2024

II. Cyber security Strategy

The cyber space is an unmaterialized space through which information are produced, processed, stored, and transferred. It is a system of interconnected networks, processors, and IT infrastructures. This cyber space, also known as the Internet (interconnected networks), has three basic entities: computers, users, and networks.

The cyber space is characterised by pillar features that let it be unique, such as anonymity, low entry prices and asymmetry. The main problem of the cyber space is its lack of transparency: anonymity and uncertainty of geographical application allow anyone to threat cybercrimes, espionage, and cyber terrorism.[14]

To avoid that, we use cybersecurity.

The term Cybersecurity is a rather new term, it was used by IT professionals, lobbyist, and politics to address security concern in the cyber space.[15] The term is used broadly, and its definition is highly variable due to its multidimensionality. Indeed, Cybersecurity is not just an issue in the IT world[16], it involves different domains: Communication security, Operations Security, Information Security, Military Security or even Physical Security[17].

Kemmerer (2003) wrote about “defensive methods used to detect and thwart would-be intruders” (“Defining Cybersecurity, “Literature Review” page 14)

[14] “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments” Yuchong Li, Qinghui Liu in Energy Reports, 2021

[15] “Definition of Cybersecurity – gaps and overlaps in standardisation” C. Brookson, S. Cadzow, R. Eckmaier, J. Eschweiler, B. Gerber, A. Guarino, K. Rannenberg, J. Shamah, S. Gorniak, December 2015, ENISA

[16] A systematic Literature Review on the Cyber Security” Y. Perwej, S. Q. Abbas, J. P. Dixit, N. Akhtar, A. K. Jaiswal, 2021, International Journal of Scientific Research and Management

[17] “Definition of Cybersecurity – gaps and overlaps in standardisation” C. Brookson, S. Cadzow, R. Eckmaier, J. Eschweiler, B. Gerber, A. Guarino, K. Rannenberg, J. Shamah, S. Gorniak, December 2015, ENISA

while Lewis (2006) affirmed that “Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption” (Defining Cybersecurity, “Literature Review” page 14) [18].

The Committee on National Security Systems, the CNSS, expound cybersecurity as the “prevention of damage to, protection of, and restoration of computers, electronic communication systems, electronic communication services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation” [19].

Furthermore, Cybersecurity can be defined as the: “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, organizations and user’s asset (ITU definition, Recommendation ITU-T X.1205)[20].

Even if, there is no unique and uniform definition, we can affirm that an efficient cyber security strategy is characterized by three primary objectives, the “C.I.A. triad” [21] :

- Confidentiality: it refers to the protection of information from unauthorized users and programs. It involves the effort to maintain data secret or private. To maintain confidentiality only people with proper authorization can access data and assets.

[18] “Defining Cybersecurity” D. Craigen, N. Diakun-Thibault, R. Purse, October 2014, Technology Innovation Management Review

[19] “Committee on National Security System (CNSS) Glossary” CNSSI No. 4009, April 2015

[20] “Series X: Data Networks, Open System, Communications and Security – overview of cybersecurity” Recommendation ITU-T X.1205, 18 April 2008

[21] “Confidentiality, Integrity and Availability – CIA in Cyber Security?” Institute of Data, December2023 (https://www.institutedata.com/us/blog/cia-in-cybersecurity)

There are several ways in which confidentiality can be compromised, such as the Man-In-The-Middle attacks where an attacker tries to steal credentials or gain access to obtain information.

- Integrity: it ensures that data are not altered, damaged, or manipulated in a non-authorized way. The integrity is maintained only if the data is authentic and reliable. It is related to data accuracy. Integrity can be compromise intentionally or accidentally.
- Availability: refers to the guarantee that systems, resources, and services are accessible when needed in a continuous and reliable way. Availability can be compromised through unintended disaster, even natural disaster or through deliberate act of sabotage such as the DoS (denial of service attack) which aim to make a computer or a network unavailable to its intended users.

This triad model has tangible implications in the real world, those principles can shape policies and procedures and can guide organizations to protect themselves from cyber threats.

When we speak about cyber threats, we must distinguish between bug and vulnerability.

Both can cause problems but, the bug is a defect, a lack of something due to incomplete information. While the vulnerability is something more, it is a defect that create an undesirable new function in the system. This new function creates weaknesses exploited in improper ways, called a “cyber threat”.

A cyber threat in turn can be used to determine a cyber-attack.

A cyber threat is an event with the potential ability to destroy, sabotage or alter the delivery of a service. The Cybersecurity Act of the EU, at article 8 (Regulation EU 2019/881) defined cyber threat as “any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons".

While a cyber-attack is an unauthorised cyber act aimed at destroying, sabotaging, or altering a cyber-asset causing a damage. [22]

Cyber-attacks are the world's fastest-growing crime[23], and in time they are becoming more sophisticated and difficult to detach and contrast. Moreover, the vague and various nature of cyber-attacks cause the difficulty to create a unique strategy against them.

Cybercrimes started to be deployed decades ago.

The term "hacking" for computer systems first appeared in the sixties[24]. But at that time, it was easier to defend from them because there were less machines and devices and hackers were not as sophisticated as they are now.

The first computer related attacks were seen in the eighties, one of the most famous cases of virus infection of that time was the "ILOVEYOU" virus which in the late nineties infected millions of computers across the world (A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions", chapter 2 "Cyber Security Fundamentals" page 7)[25].

From the 2000s, we have seen an exponential technological development and a consequent growing need of the internet, new devices were introduced in the market, such as smartphones, tablets, personal computers, social media platforms and so forth. And at the same time, hackers developed and

[22] "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments" Yuchong Li, Qinghui Liu, Energy reports, 2021

[23] "A systematic Literature Review on the Cyber Security" Y. Perwej, S. Q. Abbas, J. P. Dixit, N. Akhtar, A. K. Jaiswal, 2021, International Journal of Scientific Research and Management

[24] "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions" Aslam, Serkant Aktug, Ozkan-Okay, Asim Yilmaz, Akin, March 2023

[25] Id: "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions"

launched new types of cyber-attacks, every time more sophisticated and precise.

Today cyber threats represent a real problem and almost everything can be hacked.

The damage caused by cyber-attacks to the economy is expressed in trillions of dollars and the problem is that the trend seems to be growing and to increase gradually.

According to "*Cyber Security Ventures*"[26], cybercrime losses will cost internationally around six trillion dollars per year, which is more profitable that the global trade in major illegal drugs.

Every organisation must enhance its cyber security plan, not only big and powerful enterprises but even smaller ones, because the "it will never happen to me" strategy has proven to be unsuccessful.

Cyber-attacks can involve computer systems of private actors, like enterprises, and this may determine a commercial and reputational damage, such as in the case of MAERSK in 2017 when an unprecedented ransomware paralyzed the company's activities or the case of COSCO shipping in 2018, when the company suffered a cyber breach that affected email and network telephone in Americas' facilities and was obliged to shut down connections with other regions ("A vulnerability centric System of System Analysis on the Maritime Transportation Sector most vulnerable Assets" page 16); Or cyber-attacks can affect computer systems of public and institutional actors that can damage an entire State, such as in the case of the cyber-attack against Estonia in 2007, which involved the website and systems of the Parliament and Ministries or the case of South Korea of April 2016, when 280 ships were forced to return to port due to navigation system problems, the GPS signal

[26] https://cybersecurityventures.com/our-company/

was jammed by hackers. The South Korean authorities blamed North Korea, but this remains unconfirmed ("A vulnerability centric System of System Analysis on the Maritime Transportation Sector most vulnerable Assets" page 14) [27].

Cyber security is an ever-expanding field because every day, new hazards can be found, and hackers can develop new cyber threats and strategies.

Moreover, all the people nowadays are familiar with the internet, even elderly people and illiterate people use smartphones and the information networks; our lives are somehow shaped through the internet which became indispensable; therefore, we need to prevent and protect against cybercrimes.

Cyber security protects networks and computer systems from unauthorized access, attacks, and destruction. It can be defined as a set of strategies and processes for defending computers, networks databases and applications against assaults and illegal accesses. [28]

A good cyber security policy reflects actors' capabilities to protect people, data, and information against internal and external threats.

Cyber security acts as a security barrier.

We can distinguish between diverse types of cyber security depending on their nature[29]:

- Network security: refers to the protection of computer network from hackers. It protects internal networks from intrusion through the

[27] "A Vulnerability centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for port facilities and ships" C. Kapalidis, S. Karamperidis, T. Watson, G. Koligiannis, October 2022, Journal of Marine Science and Engineering
[28] "A Systematic Literature Review on the Cyber Security" Dr. Y. Perwej, Dr. S. Q. Abbas, J. Pratap Dixit, Dr. N. Akhtar, A. K, Jaiswal, International Journal of Scientific Research and Management, 2021
[29] "A systematic Literature Review on the Cyber Security" ..., 2021

restriction of accesses. In other words, it protects the CIA Triad (confidentiality, integrity, and availability).

- Applications security: refers to “the use of hardware and software to protect against external dangers during the development of an application inside the system” (“A Systematic Literature Review on the Cyber Security” 2021, Page 7, chapter 6.4). Application security may include hardware, software and procedures that identify security vulnerabilities. (“What is Application Security? | VMware Glossary”)[30]
- Information security: refers to the control and protection of data from unwanted access or alteration during their exchange from a device to another. Information can be anything, from personal data to biometrics.
- Cloud security: refers to the protection of information in the cloud and try to contrast any possible on-site risk. Cloud-based data storage became a popular choice because of its anonymity but they still need protection through software that monitor activity and notify every unusual fact.
- Data-Loss Prevention: ensures that sensitive or vital data are not sent beyond business network. It prevents data losses and recovery plans in case of cybercrimes.
- User training: refers to individuals. Users are the main threat for cyber security because malware or damages can derive from an erroneous use of systems. Teaching users how to protect from suspicious mails or massages or teach them how to be aware of anonymous USB can prevent majority of cyber threats.
- Critical infrastructure Security: “critical infrastructures are systems that societies rely greatly on, such as: electricity grids, water purification, hospitals, ports,” (“A Systematic Literature Review on the Cyber

[30] “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments” Yuchong Li, Qinghui Liu, Energy reports, 2021

Security" 2021, Page 7, chapter 6.2)[31]. They can be used as a platform for cyber malware from where to infect cyber breach which is somehow connected to the infrastructure. For example, attacking a port to reach an organization that utilizes that port. The security and resilience of this critical infrastructure is vital for our world and society.

The structure of computer systems and communication networks can be an incentive for hackers to perpetrate cyber-attacks. Vulnerabilities in hardware, software and computer networks expose the system to attacks. The problem is exacerbated by the erroneous and unaware use of the digital environment. Hackers exploit those vulnerabilities to attack the system and cause major damages.

Other causes are to be found in the large amount of New Technologies present in the market and therefore on the internet: the higher number of machines the higher number of attacks.

In Addition to that, "virtualization" of life, people spend a considerable high number of hours on the Internet engaging in a variety of activity, ranging from social media environments to politics and education. Also, the virtualization of financial transaction increased, due to the spreading of digital bank account and online transaction. Cyber criminals annually steal millions of dollars due to technical failures and errors during transactions in digital platforms.

Finally, we must mention spatiality, hackers can attack in any moment, and from anywhere in the world, which means that cyber-attacks do not recognise any geographical boundary.

The absence of a common international set of law in the field of cyber security, facilitates cyber criminals to launch attacks. [32]

[31] "A systematic Literature Review on the Cyber Security" ..., 2021

[32] "A comprehensive Review of Cyber Security Vulnerabilities, Attacks, and Solutions" ... 2023

Looking at legislation, according to UNCTAD (UN trade and development agency), the European Union, has the highest level of adoption of cybercrime legislation.

The first European treaty on cybersecurity is the Budapest Convention of 2001.

The Council of Europe's Convention on Cybercrime was the first multilateral binding instrument to regulate cybercrime. ("A World of Difference: The Budapest Convention on Cybercrime and the ...") It is a framework that serves as a "model law" for cybercrime legislation drafting. It is composed by four chapter in which terminology, liability, and sanctions at domestic level, as well as international cooperation are analysed.

"The protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international cooperation" "the present Convention is necessary to deter action directed against the confidentiality, integrity, and availability of computer systems, networks, and computer data as well as the misuse of such systems" … "And to adopt powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and persecution at both the domestic and international levels" (preamble Budapest Convention, 23 November 2001).

The Convention underlines the importance of harmonisation and cooperation among States. "The Parties shall cooperate with each other, …, to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of criminal offence". (Chapter 3, Section 1, Title 1- General principles to international cooperation, Art.23, Budapest Convention).

Due to cybercrime's unique and transnational nature, harmonisation is fundamental, firstly to eliminate or reduce the incidence of "safe heavens", so the possibility for criminals to hide in countries in which their conduct is not criminalised and where they can enjoy impunity, and secondly, it is crucial for effective cooperation between law enforcement agencies[33].

The Budapest treaty aims at improving the means to prevent and suppress computer or computer-related crime by establishing a common minimum standard of relevant offence[34].

Moreover, the Convention adapts traditional procedural measures to new technological environment with the addition of new measures to ensure that traditional measures remain effective in the volatile technological environment.

"Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for the purpose of specific criminal investigations or proceedings" (Chapter 2, Section 2, Title 1 – Common Provisions, Art.14, Budapest Convention).

The Convention speaks about "application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic law" and about a "Urgent mutual assistance, to the widest extent possible".

The Convention deals particularly with infringement of copyrights, computer-related fraud, child pornography and violations of network security.[35]

Although it is a regional treaty, the Budapest Convention is always intended to apply internationally.

[33] "A World of Difference: the Budapest Convention on cybercrime and the challenges of harmonization" J. Clough, Monash University Law Review, 2014

[34] "Explanatory Report – ETS 185- Cybercrime (Convention)" Council of Europe, November 2001

[35] www.coe.int , "Details of Treaty No.185"

II.I Cyber Attacks

The aim of cyber-attacks is to steal, manipulate or destroy data and information systems.

The European Union in the Regulation EU 2019/881[36] defined cyber threat as “any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons”. Due to the large amount of distinct types of cyber-attacks, we need experts to deal with them.

Here, we mention six of the main types of cyber-attacks[37]: Phishing, Malware, Denial of Service, Exploit of Vulnerabilities, Man in the Middle attack, and Social Engineering.

***Phishing* [38]**

One of the most used cyber-attacks techniques is “Phishing”, used in order to steal personal information or data by impersonating a trustworthy entity, such a bank, an institutional entity, tax department or even employers.

Phishing is a type of online fraud that targets consumers by sending an email, message or even through a phone call, pretending to be a known entity or source to steal critical information or make dangerous actions.

There are several types of phishing, the most used is the “*Spear phishing*” due to its effectiveness. Indeed, it targets e specific group or a person: hackers try to get detailed information in order to prepare a personalized attack and enhance the possibility of success.

[36] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881

[37] “A Systematic Literature Review on the Cyber Security” Dr. Y. Perwej, Dr. S. Q. Abbas, J. Pratap Dixit, Dr. N. Akhtar, A. K, Jaiswal, International Journal of Scientific Research and Management, 2021

[38] “A Systematic Literature Review on the Cyber Security” Dr. Y. Perwej, Dr. S. Q. Abbas, J. Pratap Dixit, Dr. N. Akhtar, A. K, Jaiswal, International Journal of Scientific Research and Management, 2021

Then we can distinguish between "*Smishing*" which use text messages containing a link to click on or a phone number to call (a typical smishing attack is the fake bank message advising the user of the compromise of the credit card or the account) or "*Email phishing"*, hackers use mails that informs the users that their account has been hacked and they must respond promptly by clicking on a link.

Malware[39] [40]

Malware or Malicious software is a general term referred to all those cyber-attacks designed to disrupt the normal operation of any device or network. The malware is usually injected into the device through an executable code. Malware are designed to spy and obtain information or simply to cause destruction. There are several types of malwares, some need a host program (like Trojan horses), and some others are independent (like Virus and Worms).

Ransomwares are malware that make essential files, documents, applications, and networks inaccessible to users. They are used to extort money. The attacker makes the computer and data inaccessible to users until they pay a ransom. A possible danger linked to ransomware is the possibility for the attacker to keep copies of data of the user despite the ransom.

Virus is a self-replicating malware that spreads quickly over the hard disk to cause damages. The goal is infection of files to make them unusable.

Viruses change the way a computer works without the user's permission or knowledge. They are not automatic; indeed, they need manual intervention to be activated.

[39] "A comprehensive Review of Cyber Security Vulnerabilities, Attacks, and Solutions" ... 2023
[40] "A Systematic Literature Review on the Cyber Security" Dr. Y. Perwej, Dr. S. Q. Abbas, J. Pratap Dixit, Dr. N. Akhtar, A. K, Jaiswal, International Journal of Scientific Research and Management, 2021

Trojan Horses are in turn, malicious programmes that hide in a useful application and create back doors for attackers to exploit and caused damages. They are presented as useful programs to users that are brought to the decision of download them. They are not easy to detect and show their effect only after the infection. Trojans are malware that allow attackers to obtain access to a user's device and abuse it. They do not self-replicate.

Worms are self-replicant malwares that are designed to propagate from targeted devices to other nodes in the network. They are usually contained in email attachments.

Their potential is amplified by the fact that they can act without the attacker or user's active participation. They can reproduce themselves in large numbers. They are similar to viruses, but they are not user-run programs.

Denial of Service (DoS)

It is a special attack aimed at making a service unusable to users, the attack includes the saturation of the host server with many more requests than it can manage, causing the server to fail. It damages the reputation of an organization by compromising its capacity to respond to users and therefore has a direct influence of customer loyalty.

Exploit of vulnerabilities[41]

Those types of attack exploit bugs of the system or cookies in order to obtain unauthorized access or to cause damages in the system.

The vulnerabilities can be found in web application, software, and operational system, IoT (Internet of Things) devices or third parties' software.

To launch an "exploit of vulnerability" attack, hackers can use other types of attacks: email phishing, Trojan, or Virus.

[41] Francesco Corato, "Gestione operativa dei sistemi e delle reti informatiche", Università Giustino Fortunato, 2024

Man in the Middle (MiTM)

This type of attack occurs when an attacker intercepts communication between two parties with the intent of spying them, stealing personal information or credentials, or altering the dialogue. In short MiTM attacks happen when a hacker is secretly involved in communication between two parties. The hacker can both read and modified the data transmitted by the victim. The purpose of this kind of attack is to obtain personal information such as passwords, bank information, personal data, or secret documents.

Anyway, now, most chat systems use end-to-end encryption (security method that keeps communication and messages secure) which prohibits third parties from acquiring information or spying users' dialogues, therefore, now we have a higher level of protection from MiTM attacks.

Social engineering

Social engineering refers to all those techniques aimed at inducing a target to reveal specific information or do a specific action for illegitimate and unauthorised reasons. It can be seen as a form of trickery that involves the use of ICT technologies. Social engineering can be done through email, phone calls, messages, social medias, or even personal meeting.

This type of technique exploits deception to manipulate individuals and induce them to reveal specific information. It has always existed but with ICT technologies it has significantly evolved.

It usually exploits other forms of attack such as phishing or smashing.

An example could be the well-known false employee of the bank asking for password to solve our unreal card problem.

II.II Protection against Cyber attacks

To protect against cyber-attacks, cyber security technologies must be employed, and great cyber security doctrine must be followed. Many cyber security technologies exist, they can stop unauthorized access, remove risks, or even do privacy audits on all software.

Some of the most useful tools that companies should use to provide the best possible cyber protection are[42]: Firewalls, Antivirus, Public Key Infrastructures Services, Cybersecurity Software Tools, Managed Detection and Response Service, Web vulnerability Scanning Tools, as well as Staff training practices (Chapter 10 – Cyber Security Tools, "A Systematic Literature Review on the Cyber Security).

Firewalls are virtual walls that impede unauthorised users from accessing a network. Firewalls filter any message and information entering and leaving a network, they block those that are suspicious or malicious.

Antiviruses are programmes that prevents, detects, and removes malwares from personal computers, networks, and IT systems[43].

PKI Services, or *Public Key Infrastructures Services,* allow to distribute and identify public encryption keys. In short, they allow to communicate over the internet safely and at the same time to verify the other party's identity. This technology encrypts server communication.

Cyber Security Software Tool, types of software that safeguard sensitive and personal data held by companies or individuals. They check for web application flaws, detect and alert, but also prevent against cyber threats.

Managed Detection and Response Service (MDR), this comprise several types of services that are aimed at help organisations to become more aware of hazards and increase the ability to respond to threats. MDR also use Artificial Intelligence and machine learning.

[42] "A Systematic Literature Review on the Cyber Security" Dr. Y. Perwej, Dr. S. Q. Abbas, J. Pratap Dixit, Dr. N. Akhtar, A. K, Jaiswal, International Journal of Scientific Research and Management, 2021
[43] "A Systematic Literature Review on the Cyber Security" Dr. Y. Perwej, Dr. S. Q. Abbas, J. Pratap Dixit, Dr. N. Akhtar, A. K, Jaiswal, International Journal of Scientific Research and Management, 2021

Web Vulnerability Scanning Tools are automated programmes that analyse organisations' web applications for security flaws and draw up a list of possible vulnerabilities and recommendations for remediation.

Staff training is not technically an instrument, but it results to be the most effective kind of defence against cyber-attacks. Every company must invest in training of its personnel because cyber thieves are improving their methods and target employers, they take advantage of the power of repetition that individual is accustomed to and will easily enter the organisation systems. All personnel should receive cybersecurity training because "Cybersecurity is everyone's responsibility"[44].

The cost of investing in cybersecurity and training may provide long-term paybacks in terms of security and safety (Chapter 10.9 – Staff Training, "A Systematic Literature Review on the Cyber Security).

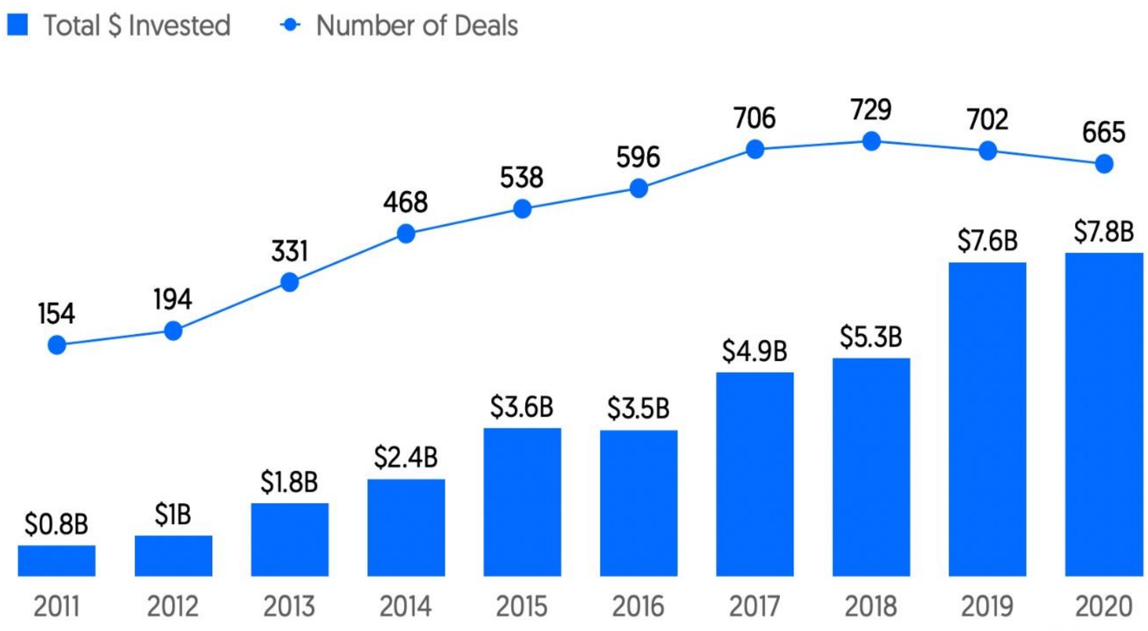


Figure 3 relation between dollar invested and cybersecurity breaches[45]

[44] "Global Challenges in Maritime Security", chapter 8, Kapalidis, 2020 Springer Editor

[45] "Report: The rise of Global Cybersecurity Venture Funding" (https://about.crunchbase.com/cybersecurity-research-report-2021)

As shown in figure 3 the higher you invest, the more the number of cyber incidents decrease.

Data security has become a worldwide priority, a critical part of national and economic security. All organisations need strategic security plans to protect their infrastructures, especially critical infrastructures.

A Security policy should be ensured through distinct phases, starting from planning and risk analysis to a possible incident response. Due to complexity of cyber-attacks, it is not easy to develop an efficient security plan.

For instance, private and public actors shall rely on trusted guidelines and procedures to set their security plans.

Internationally, various cybersecurity entities have produced their cyber security framework to serve as guidance for organisations. Those frameworks can be used to detect, identify respond and recover after a cyber threat.

For example, the framework NIST (National Institute of Standards and Technology) is a set on guidelines and standards aimed at better organisations' cyber security and management of cyber risks to better understand, prioritize, and communicate cybersecurity efforts.

The NIST Cybersecurity Framework (CSF) is composed by three main aspects: Core, Implementation Tiers, and Profile[46].

The most important part is the Core, which is the process of management of cyber security risks, we find the six main functions that the organisation must develop:

- *Govern*: it addresses an understanding of organizational context, establishment of cybersecurity strategy and risk management, roles,

[46] "The NIST Cybersecurity Framework (CSF) 2.0" National Institute of Standards and Technology, 2024

responsibilities, and authorities. In sum, it contains the oversight of the cybersecurity strategy.

- *Identify*: it contains the understand of the context, suppliers and assets which support critical business processes.
- *Protect*: refers to the implementation of measures aimed at protecting business processes and assets.
- *Detect*: refers to the implementation of activities aimed at identifying cyber incidents and timely discovering anomalies or other potentially adverse events.
- *Respond*: it contains the definition and implementation of activities to intervene when a cyber-attack is detected.
- *Recover*: refers to the implementation of activities to manage recovery plans and activities after the cyber incident, to enable timely restoration of normal operations.

The functions shall be addressed concurrently, and all of them are needed and are fundamental for a correct and efficient cybersecurity plan.

We call "Threat Intelligence", the capacity to understand and predict enemies' intentions, reasons and methods used to attack and therefore the ability to contrast them and protect critical assets. This is a proactive approach, in the sense that it acts before the possible attack.

It is a form of prevention, not a response.

A security model is a set of principles, rules and procedures that define how to protect internal systems, networks, and data from cyber-attacks[47].

[47] Fabio Bevilacqua, 2024, "cybersecurity e informatica forense", Università Giustino Fortunato.

The aim of a Security plan is to guarantee a systematic and coherent security approach of information and resources ensuring, meanwhile business continuity and protection of its interests[48].

ENISA (the European Union Agency for Cybersecurity) published a study on "Foresight cybersecurity threats projected for the year 2030" which provides a comprehensive overview of emerging cybersecurity threats with the final aim to improve preparedness of international actors, assess and forecast potential cyber threats.

We can distinguish ten emerging cyber threats[49][50]:

1. *"Supply Chain compromise of software dependencies"*: As the market demands quick product release, integration of components and services is required, but it could lead to unforeseen vulnerabilities, "creating more opportunities for malicious actors to compromise the supply chain from the supplier and costumer side". Through sabotage, theft, malicious code or information leakage, criminals cause disruption, malfunctioning or data losses[51].
2. *Advanced disinformation campaigns:* deepfake technologies can manipulate communities for political and monetary gain. Adversary can train Artificial Intelligence for deepfake attacks. AI can create unreal images, avatars, and speeches to influence the audience, for example during election campaigns.
3. *Rise of digital surveillance authoritarianism and loss of privacy*.
   Location tracking, public cameras, facial recognition are today used

[48] Id: "Fabio Bevilacqua..."
[49] Francesco Corato, 2024, "Gestione operativa dei sistemi e delle reti informatiche", Università Giustino Fortunato.
[50] "Foresight cybersecurity threats for 2030" ENISA, March 2023
[51] "Identifying Emerging Cyber Security Threats and Challenges for 2030" R. Mattioli, A. Malatras, ENISA, March 2023

identified criminals but in the future states actors or even private actors could use them and prejudice individual freedoms and privacy.

4. *Human error and exploited legacy systems within cyber-physical ecosystem*: IoT development, ongoing skill shortage will lead to the lack of knowledge and adequate training which in turn will lead to IT and OT security maintenance issues and allow cyber criminals to launch new form of attacks, intelligent attacks. This can create systematic risks.
5. *Skill shortage*: cybercriminals target organisation with a lack of capacities or competencies. Exploiting these skills' gap they can cause financial outages. "Threat actors will analyse organizational skillsets and deficiencies to gain insight into weaknesses in defence, potential vulnerabilities, and opportunities to exploit their systems and networks" (Chapter 3.8 ENISA, ""Identifying Emerging Cyber Security Threats and Challenges for 2030").
6. *Targeted attacks (e.g. ransomware) enhanced by smart device data:* collection of behavioural data will increase, and a profiling will be ever more accurate. Criminals will try to get access to behavioural data to tailor social engineering attacks. The latter will be a challenge for users as well as law enforcement and governments who will struggle to find new ways to prevent them and improve authentication.
7. *Cross-border ICT service providers as a single point of failure*: ICT sectors that provide services across borders are likely to be targeted and therefore cause outages, damages, unavailable critical infrastructures. The infrastructure sector such as port, airport, but also healthcare and industry are increasingly reliant on ICT services, and they are fundamental for the society, "responsibility for upholding a functioning society was significant back in 2022", "hence they will likely be targeted by governments, terrorists and criminal groups..., exploiting vulnerabilities in their infrastructures, using hybrid attacks".

8. *Rise of advanced hybrid threats*: physical and offline attacks are evolving and becoming combined with cyberattacks. “With a new modus operandi, detection tools need greater correlation capabilities including connecting seemingly unrelated events. They therefore pose a growing challenge for governments, companies, and citizens alike” (Chapter 3.7 “Identifying Emerging Cyber Security Threats and Challenges for 2030” ENISA)
9. *Artificial intelligence abuse*: Artificial Intelligence can be manipulated intentionally. Corrupted training of AI algorithms may cause incorrect actions and decisions. “AI can be used to enhance many nefarious activities such as: creation of disinformation and fake content, bias exploitation, collecting biometrics and other sensitive data, military robots, data poisoning, etc.”
10. *Lack of Analysis and control of space-based infrastructures and objects*: the fast growth of the space sector is an emerging topic for security community. “There is a lack of understanding, analysis and control of space-based infrastructures” (Chapter 3.6 ENISA “Identifying Emerging Cyber Security Threats and Challenges for 2030)

III. Maritime Cyber Security and Critical Infrastructures

The maritime sector is of crucial importance to modern societies, today around 90% of world trade is carried by the international shipping industry; across the globe there are around 50 000 merchant ships, transporting every kind of cargo[52].

Maritime transportation offers numerous advantages such as lower transportation costs, higher transportation capacities, economic efficiency and even less pollution than other transportation method.

Maritime transport plays a key role in the socioeconomic development and welfare of states, ports act as an enabler for economic growth[53].

However, this economy is particularly exposed to danger due to the environment of its operations, its complexity, and its nature of international open transportation network.

Safety is crucial, because accidents in this sector cause major economic losses, fatalities, and even environmental contamination. Risks are numerous and may result from deliberate action or from random ones.

When we think of possible risks related to the maritime sector, we usually focus on foundering of ships, structural failures, or terrorist risks and piracy. Vessels can be vector for, or target of, attacks. Every year cargo, passenger or fishing vessels come under attack by pirates seeking to gain revenue by hijacking and selling cargo and/or ransoming crew[54].

[52] "Safety of Maritime Transport in the Baltic Sea", J. Caban, F. Brumerčik, J. Vrabel, P. Ignaciuk, W. Misztal, A. Marczuk, MATEC Web of Conferences, 2017

[53] "A Vulnerability Centric System of Systems analysis on the Maritime Transportation Sector most valuable Assets: recommendations for Port Facilities and Ships" C. Kapalidis, S. Karamperidis, T. Watson, G. Koligiannis, 2022, Journal of Marine Science and Engineering

[54] "Security in maritime transport: risk factors and economic impact" Maritime Transport Committee, OECD, July 2003

The maritime sector is also of high value for those engaged in unlawful acts like smuggling, narcotics, and human trafficking.

But the “voyage” by sea is just one element in a complex chain, which is composed by a complex web of people, interactions, movements of goods and information.

The maritime industry is constituted by subcomponents: ports, operations, personnel and ships, offshore infrastructures, Operational ad Information Technology Systems, insurance agencies, booking agents, and banking-economic transactions[55].

These subcomponents can be categorised as follow:

- Mobile assets (ship, auxiliary platforms)
- Infrastructures (offshore, onshore, underwater, satellite ones)
- Financial activities

Figure 4 represent this infrastructure and shows how it is articulated.

[55] “Global Challenges in Maritime Security”, chapter 8, Polychronis Kapalidis, Springer Editor 2020

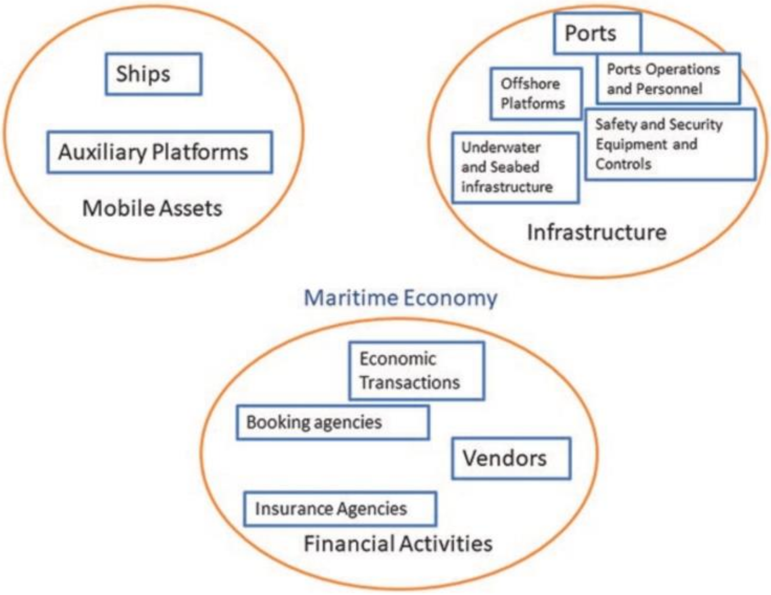


Figure 4 - The components of the Maritime Industry[56]

This complex chain that characterised the Maritime transport sector and all related activities, namely the “Maritime Transport Systems” (MTS) are conducted by technology-intensive platforms which rely on information system. [57]

To be more competitive, comply with standards and optimize operations, the maritime sector is increasingly dependent on the internet[58].

Rapid developments within IT and OT technologies, operational optimisation, costs savings, safety improvements and sustainable business rely largely on connectivity between servers; but great benefits come at great risks, the advantages related to digitalization of the maritime sector are directly

[56] “Global Challenges in Maritime Security”, chapter 8, Polychronis Kapalidis, Springer Editor 2020 page 132
[57] BIMCO, Chamber of Shipping of America, Digital Containership Association, Intercargo, Intermanager, Intertanko, ICS, IUMI, OCIMF, World Shipping Council, 2021
[58] “The guidelines on Cyber security onboard ships” BIMCO, version 4, 2021

correlated to higher risks and indeed, the number of potential vulnerabilities increased proportionally with technological development of maritime sector.

Comparing to the past, maritime cyberattacks have increased exponentially, as we can see form figure 5, from 2009 major attacks occurred, and after the Covid-19 pandemic they skyrocketed. The image take into account only significant cyber incidents, namely attacks which cost over 1.000.000 dollars.

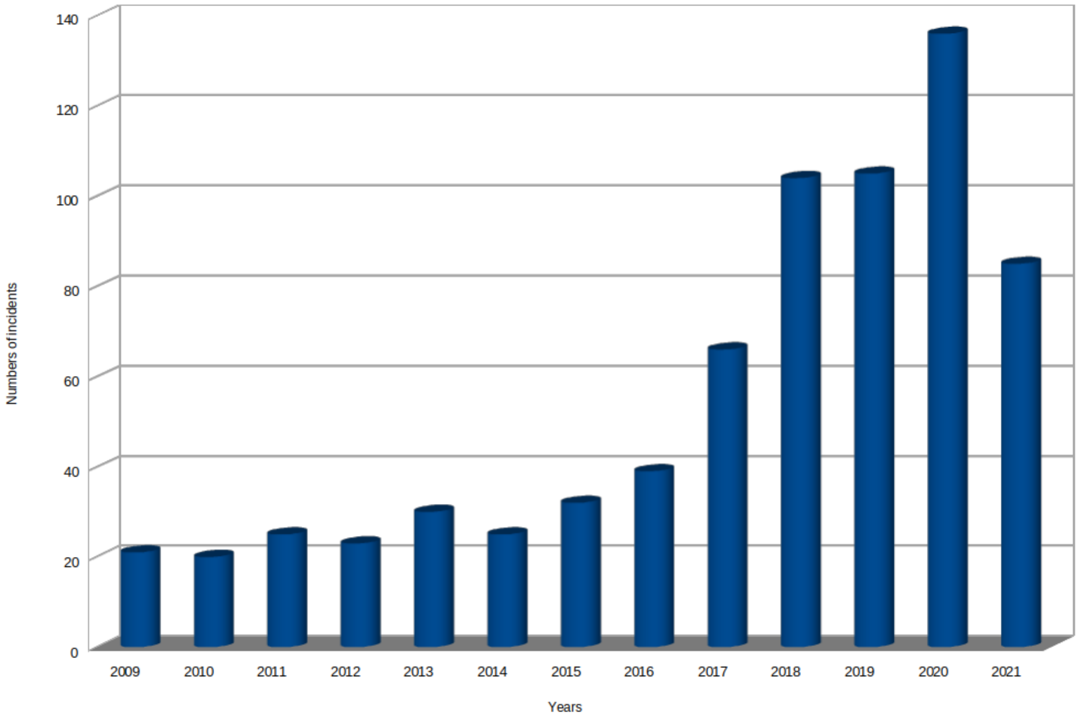


Figure 5 Significant Cyber incidents 2009-2021[59]

Among the most devastating attacks, we recall the 2016 attack against the navigation system of Korean vessels when their GPS signal was jammed by hackers and 280 vessels experienced navigational system issues or the attack suffered by Danish Maritime Authority in 2012 when a virus was introduced by a PDF document infected and then propagated from the Danish Maritime Authority to other institutions[60]. Moreover, the spoofing attack in May

[59] "Maritime Cyber Attacks" M. Bialas, August 2021, Vessel Automation

[60] "Cybersecurity in the maritime industry: a literature review" C. Park, W. Shi, W. Zhang, C. Kontovas, C. Chang, 2019

2017 that caused the collision between a U.S. Navy ship and a South Korean fishing boat[61].

Then, in the same year we had the most devastating attack, the case of Maersk in 2017, when the Ransomware “NotPetya” shut downed the company’s network system and caused a $200-300 million financial lose. We will analyse this issue in the following chapter.

In 2018, the ports of Barcelona, Long Beach and San Diego were attacked.

Seen the increasing number of attacks, maritime cybersecurity is becoming an issue that must be addressed and emphasised. The cyber risks of the maritime industry cannot be underestimating affirmed IMO, the specialized agency of the UN with the authority to regulate maritime affairs, including safety and security.

Indeed, according to IMO (International Maritime Organization) Maritime cyber security is an emerging issue that requires immediate attention. (“In the news - Information Security Forum”)[62].

The maritime transport sector is slow in addressing cyber risks. Compared with other industries, such as military and financing; cybersecurity in the maritime sector is ten to twenty years behind[63]. The existing reliance on digitalization, automation and network-based systems increased the need for cyber risk management.

[61] “Cybersecurity Challenges in the Maritime Sector” F. Akpan, G. Bendiab, S. Shiaeles, S. Karamperidis, M. Michaloliakos, February 2022

[62] https://www.securityforum.org/in-the-news/

[63] “Cybersecurity in the maritime industry: a literature review” C. Park, W. Shi, W. Zhang, C. Kontovas, C. Chang, 2019

Contrary to traditional risk management, addressing cyber risks means facing new challenges for port operators, who often lack internal expertise, structural organisation, and resources to effectively mitigate risks[64].

Cyber risk management should be an inherent part of company's safety and security culture, and it should identify roles and responsibilities of personnel, implement technical and procedural measures to protect against cyber incidents and ensure continuity of operations[65].

Among all types of risks, human error is the most significant risk factor that causes around 80-90% of shipping accidents directly or indirectly[66], that is the reason all ship crew, both senior officers and junior crew members and all ashore staff should receive cybersecurity training because cyber risks have wide-ranging destructive potential.

An effective cyber risk management relies on a clear allocation of responsibilities and tasks.

There are several risk factors that impact maritime cybersecurity[67]:

- *Lack of training and expert for cybersecurity:* Computers can be infected by accidentally opening an e-mail containing a virus and humans can make mistakes intentionally or unintentionally. Awareness is fundamental to mitigate human error (chapter 3.1)
- *Use of the outdated IT system:* the maritime industry is still relying on outdated software such as traditional firewalls and antivirus unable to deal with advanced cyberattacks (chapter 3.2)
- *Risk of being hacker's target:* Hacktivism is the most common threat, in the maritime cybersecurity we can distinguish between targeted and

[64] "Cyber Risk Management for Ports, guidelines for cybersecurity in the maritime sector" ENISA, December 2020

[65] "The guidelines on Cyber security onboard ships" BIMCO, version 4, 2021

[66] Id: "Cybersecurity in the maritime industry: a literature review" C. Park, W. Shi, W. Zhang, C. Kontovas, C. Chang, 2019

[67] Id: "Cybersecurity in the maritime industry..." C. Park, W. Shi, W. Zhang, C. Kontovas, C. Chang, 2019

untargeted attacks, the former refers to company, system or data as intended target, hackers use tools and techniques created specifically for that target. The latter are attacks that use tools and techniques available on the internet and exploit widespread vulnerabilities (chapter 3.3)

- *Fake website and phishing email:* Personnel and crew "using private devices could cause cyber-attacks through accessing or opening fake websites and email and further installing malicious software into vessel system" without knowledge of the victim (chapter 3.4).

Therefore, it is fundamental to train personnel, keep systems updated or even upgrade IT systems, and develop cybersecurity processes.

A port, as a "*complex cyber environment*", can be seen as a set of land and waterside systems, in which the human interventions and participation remain predominant[68].

Increased digitalization expands the landscape for cybercriminals but also possible unintentional human error. IT and OT systems and services offers a wide range of access points from where malware may infiltrate.

"The cyber environment comprises the computers and interconnected networks of both information and operational technology systems that use electronic, computer-based, and wireless systems" (Cybersecurity of Port and Port Systems)[69].

As the UK department of transport define in its "Good Practice Guide", ports typically comprise four main components in which technology plays a fundamental role: buildings, linear infrastructures, plant and machinery, and information and communication systems.

[68] "Cyber Security of Ports and Port Systems" H. Boyes, R. Isbell, A. Luck, 2020, The Institution of Engineering and Technology

[69] Id "Cyber Security of Ports and Port Systems"

The compromise of one of the components has the potential to impact upon the efficiency of the port, the ability of the latter to carry out operations and the health and safety of staff[70].

Plant and machinery used for cargo handling and port management, are the most vulnerable of the four components since they rely on OT (Operational Technology) and Supervisory Control and Data Acquisition systems. The impacts of a cyber-attack on these systems are classified as severe[71]. Other vulnerable components are: Information and Communication Systems and the Vessel Traffic Control Tower (part of the building component).

The ship can also be seen as a cyber environment. It is the sector's most valuable asset and the one operating independently at sea. When at sea, the ship does not rely on internet connectivity to conduct its operation, navigation, and cargo monitoring but several subcomponents, critical to the ship, are digitalised, therefore a holistic risk management approach is needed also for ships[72].

A correct cyber security assessment is needed to identify vulnerabilities in physical structures, personnel protection systems and business processes. It forms the basis for the cyber security plans (CSP) for the port and port facilities[73].

The CSP establishes appropriate security measures to minimise the likelihood of security breaches and their consequences. The plan shall include also suitable mechanism for periodic reviews and should be updated

[70] "Cyber Security of Ports and Port Systems" H. Boyes, R. Isbell, A. Luck, 2020, The Institution of Engineering and Technology

[71] "A Vulnerability Centric System of Systems analysis on the Maritime Transportation Sector most valuable Assets: recommendations for Port Facilities and Ships" C. Kapalidis, S. Karamperidis, T. Watson, G. Koligiannis, 2022, Journal of Marine Science and Engineering

[72] Id: "A Vulnerability Centric System of Systems…" Kapalidis, 2022

[73] "Cyber Security of Ports and Port Systems" H. Boyes, R. Isbell, A. Luck, 2020, The Institution of Engineering and Technology

when necessary to reflect any gaps, organisational changes, or changes of any other nature (political, environmental, technological)[74].

When a CSP is in place, a Cyber Security Officer shall ensure the development and maintenance of the plan, implement, and exercise the plan itself.

The cyber security officer is the person responsible for managing and coordinating the cyber security in the port or port facilities.

As we mentioned, the port environment involves a large variety of technologies, both the port and the ships can be defined cyber environment, and therefore both need a cyber security approach to deal with threat and security breaches.

The cyber security approach is characterized by the C.I.A. triad (Confidentiality, Integrity, and Availability) and safety.

At the international and national level, governments, agencies, local administrations and the shipping and port industries tried to address cybersecurity and create guidelines to contrast cyber breaches and provide the maritime sector with an appropriate framework to build up and developed proper Cyber Security plans.

In the following pages we will analyse different European, International and National documents and guidelines focused on the protection of critical infrastructures and cyber security of maritime sector.

[74] Id: "Cyber Security of Ports and Port Systems"

III.I The European Context

The maritime transport is crucial for the European Union. Within the EU, we can count more than 1200 seaports. Seventy percent of the external borders of the EU are maritime[75].

The EU and its Member States have strategic interests in identifying and addressing security challenges linked to the sea.

III.I.I European Directives

In 2008, the EU adopted the Directive 2008/114/EC on the protection of Critical infrastructures. The directive established an EU process for identification of European critical infrastructures and set out an approach to improve their protection. The document identified critical infrastructures as: "assets or systems essential for the maintenance of vital social functions, health, safety, security and economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions" (Art.2 letter A, directive 2008/114/CE). Ports and sea shipping facilities are included in the list.

The directive 2005/65/CE of the European Parliament and of the Council, on enhancing port security, identified "Port" as "Any specified area of land and water, with boundaries defined by the Member State in which the port is situated, containing works and equipment designed to facilitate commercial maritime transport operations" furthermore, the directive states that Member States shall ensure Port Security plans, which shall be developed, maintained and updated based on specificities of ports and shall identify procedures, measures and actions to be taken to ensure security of ports.

[75] "ENISA Report on Good Practices for Port Cybersecurity" A. Drougkas, ENISA, November 2019

According to ENISA' s good practices of 2019, ports should put in place security measures to protect themselves from cyberattacks, through the definition of a clear governance, involving stakeholders, raising awareness of cybersecurity matters and enhancing training of personnel, enforcing cyber security basis, response capabilities and detection of cyber incidents to react as fast as possible[76].

Ports are central to European interconnection of diverse types of transport. They are also important nodes for passenger transportation and for the European fishing industry.

III.I.II European Maritime Security Strategy

In June 2014, the Council of the European Union published the European Maritime Security Strategy (EUMSS[77]) as a shared and comprehensive tool to identify, prevent and respond to challenges that affect EU in the maritime ecosystem. The strategy was revised several times, last revision was in 2023.

The EUMSS promotes international peace and security, ensure sustainability of the oceans and the protection of biodiversity. ("Maritime security strategy - European Commission - Oceans and fisheries")

"“The Sea is a valuable source of growth and prosperity for the European Union and its citizens." (“The European Union as a Maritime Security Provider – The Naval ...”) The EU depends on open, protected, and secure seas and oceans for economic development, free trade, transport, energy security, tourism, and good status of the maritime environment”. (EUMSS, 11205/14)[78].

The strategy provides the political and strategic framework to enhance cross-sectoral cooperation within, between and across authorities and actors. It fosters solidarity and mutual support in line with existing legislation.

[76] Id: “ENISA Report on Good Practices for Port Cybersecurity” A. Drougkas, ENISA, November 2019

[77] https://ec.europa.eu/commission/presscorner/detail/en

[78] “European Union Maritime Security Strategy”, Council of the European Union, June 2014, 11205/14

The strategy is based on four principles[79]:

- *Cross-sectoral approach*: all partners involved in the maritime domain shall cooperate and respect each other.
- *Functional integrity*: competences of Member States and of the Union remain central, new provisions are built upon existing capabilities and policies in order to avoid creating new structures or legislation or even additional burdens.
- *Respect for rules and principles*: the strategy respect existing "international law, human rights and democracy" … "applicable bilateral treaties and values enshrined therein are the cornerstones of this Strategy and key principles for rules-based good governance at sea" (European Union Maritime Security Strategy, 11205/14, page 5, chapter III, letter c). Moreover, the Strategy recognise the importance of international courts and tribunals in disputes settlements and implementation of the rule of law at sea.
- *Maritime multilateralism*: strategy requires cooperation among international partners and EU, in particular with NATO and the US.

The aims of EUMSS are varied, ranging from the promotion of rules-based governance at sea in waters under sovereignty of Member States, to growth and job potential of the seas. Security is also mentioned among aims, as well as the promotion of the solidarity and the role of the EU as a global actor and security provider at sea and from the sea.

Among a variety of different threats, the strategy identifies cyber-attacks as a potential risk for maritime security. "Maritime security threats are multifaced, pose a potential risk to European citizens and can be detrimental to the EU's and its Member States' strategic interests" among them "Terrorism and other international unlawful acts at sea and in ports against ships, cargo, crew and

[79] Id: "European Union Maritime Security Strategy" … 11205/14

passengers, ports and port facilities and critical maritime and energy infrastructures, including *cyber-attacks*" (EUMSS, page 8, chapter V, letter d).

Recurrent hybrid and cyber-attacks targeting maritime critical infrastructures require the EU to bolster its action and be more effective in their protection[80].

Malicious actors target maritime infrastructures, including undersea cables, pipelines, as well as ports and ships. ("EUR-Lex - 52023JC0008 - EN - EUR-Lex")

III.I.III ENISA Report on Good Practices for Port Cybersecurity

The aforementioned ENISA report on good practices of 2019, underlines that a large amount of data is exchanged between ports and different stakeholders, mandatory declarations, authorisations, operational data, financial data or also documentation on navigation and position. They are all potential target for cyber breaches.

When ports suffer a cyber-attack, they can face numerous challenges, ranging from shutdown of operations which cause port paralysis, sensitive and critical data theft, and even goods stealing. Moreover, we cannot avoid mentioning financial losses and reputational losses due to delays. As the ENISA report showed, there are numerous potential threat attacks (ENISA Report: Port Cybersecurity, page 28, chapter 4, "threat description").

For example, Hackers can intercept communication with the "Man in the Middle" technique and get sensitive data, steal essential information, or even alter the communication between parties. The aim of falsifying information is to disrupt operations or modify them.

Malicious actors can also create a system unavailability, with the Denial of Service, causing significant damages for companies' reliability and therefore the loss of costumers and competitiveness.

[80] "ENISA Report on Good Practices for Port Cybersecurity" A. Drougkas, ENISA, November 2019

Hackers can also spoof geo-localisation signals and change the trajectory of vessel, causing possible delays, sabotage, or theft[81].

Finally, the Report mentions the possibility for hackers to get access to useful systems through phishing: they install components to gain access remotely and bypass network security.

The European Parliament resolution of 17th January 2024, on building a comprehensive European port strategy[82], highlights the importance of critical infrastructures protection at sea for the safety and security of EU waters and operations and emphasises the relevance of cybersecurity and cyber resilience of all actors in European ports to prevent espionage and severe disruption of port systems and operations.

The Resolution, in the “security” section (point.21), “Asks the Commission to do further research and to collect data on the coverage and risks of non-EU companies’ involvement in cyber and data security in critical infrastructures and to support the development of comprehensive contingency plans for ports with technical and operational support from the European Maritime Safety Agency”, furthermore it “considers that the risk of negative spillover effects from a lack of cybersecurity from one port to another is high and therefore high standards should be maintained by all Member States and that the sharing of best practices and experiences is recommended”.

III.I.IV NIS Directives

Considered the importance of cybersecurity for the resilience of critical infrastructures, the directives on Network and Information Security (NIS and NIS 2) were adopted. Directive NIS 2016/1148 was adopted in 2016 for the protection of networks and digital systems.

[81] “ENISA Report on Good Practices for Port Cybersecurity” A. Drougkas, ENISA, November 2019

[82] Resolution of the European Parliament (2023/2059 (INI)) p. 21 - 22

The NIS directive has been the first European legislative measure aiming at increasing the level of security of network and information systems. It contributed to improving cybersecurity capabilities and increasing cooperation between Member States[83].

NIS 2 directive, or Directive 2022/2555 entered into force on 17th of January 2023. The Directive represent a significant enhancement of the exiting legislation, it enforces stricter cybersecurity regulations and aims to enhance the resilience and incident response capabilities of both public and private sectors.

It defines a cyber incident as "any event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the related services offered by, or accessible via, network and information systems"[84].

The directive includes the obligation for Member States to report incidents, in order to create resilience and preparedness against threat and get full pictures of the threat landscape.

Article 20, states that reporting obligation must be extended to encompass "any significant cyber threat that entities identify that could have potentially resulted in a significant incident".

NIS 2 directive recognise ports as infrastructures of high criticality.

The directive requires Member States to comply with a common set of cybersecurity measures: Every States must adopt a national cybersecurity strategy and must designate or establish competent authorities, cyber crisis

[83] "Defining the reporting threshold for a cybersecurity incident under the NIS directive and the NIS 2 Directive" S. Schimtz-Berndt, 2023, Journal of Cybersecurity

[84] NIS2 reporting obligations: Notifications for significant incidents, (https://advisera.com/articles/reporting-obligations-nis2/).

authorities, single points of contact and a computer security incident team (CSIRT)[85].

Each single point of contact shall ensure cross-border cooperation with other State's authorities and with the European Commission and ENISA.

Moreover, the Directive ask each Member State to include in its National Cybersecurity Strategy, objectives and priorities and a governance framework to achieve those objectives. The governance frameworks shall clarify roles and responsibilities of relevant stakeholders at national level.

Finally NIS 2 requires that as part of National Cybersecurity Strategy, Member States shall adopt policies: "addressing cybersecurity in the supply chain for ICT products and services" … "policies related to sustaining the general availability, integrity and confidentiality of the public core of the open internet" … "promoting and developing education and training on cybersecurity, cybersecurity skills, awareness raising and research", and strengthening the cyber resilience, cyber hygiene and cyber protection (Directive NIS 2, chapter II, Article 7)[86].

By October 2024, Member States must adopt all cyber measures included in the Directive.

NIS directives require to conduct risk assessments that "cover all operations including the security, integrity and resilience of network and information systems"[87].

[85] Directive EU 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation 910/2014 and repealing Directive 2016/1148

[86] Directive EU 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation 910/2014 and repealing Directive 2016/1148

[87] Railway cybersecurity - ENISA, (https://www.enisa.europa.eu/publications/railway-cybersecurity-good-practices-in-cyber-risk-management)

However, in the European Union, there is no common methodology among Member States, for port cyber risk assessment.

The closest framework to a common risk assessment methodology is the IMO's International Ship and Port Facility Security (ISPS) Code. This code was implemented in the EU by the Regulation 725/2004, which include the implementation of Port Facility Security Assessments (PFSAs) and Port Facility Security Plans (PFSPs). The ISPS code also defines minimum port facility security assessment elements[88].

IMO code on Ship and Port Facility Security will be analysed afterwards.

III.I.V ENISA Guidelines for Cybersecurity in the Maritime Sector

However, ENISA underlines that across the EU port sector, a fragmented approach in the performance of cyber risk assessment occurs. Additionally, the European Agency argues that port facilities complying with ISPS Code requirements showed gaps in their organisational cyber risk assessments. Key aspects were left un-assessed due to the variability of port resources and perceptions and different stakeholders' degree of engagement. For these reasons, ENISA aimed to provide a set of guidelines for port operators to effectively manage cyber challenges.

The ENISA's "Cyber Risk Management for Port" Report introduced a four-phase approach to cyber risk management in order to provide "actionable guidelines for managing cyber risk that can be mapped to any framework of methodology the port operator is currently using or may wish to use" [89].

[88] "Cyber Risk Management for Ports – guidelines for cybersecurity in the maritime sector" A. Drougkas, A. Sarri, P. Kyranoudi, December 2020, ENISA

[89] "Cyber Risk Management for Ports – guidelines for cybersecurity in the maritime sector" A. Drougkas, A. Sarri, P. Kyranoudi, December 2020, ENISA

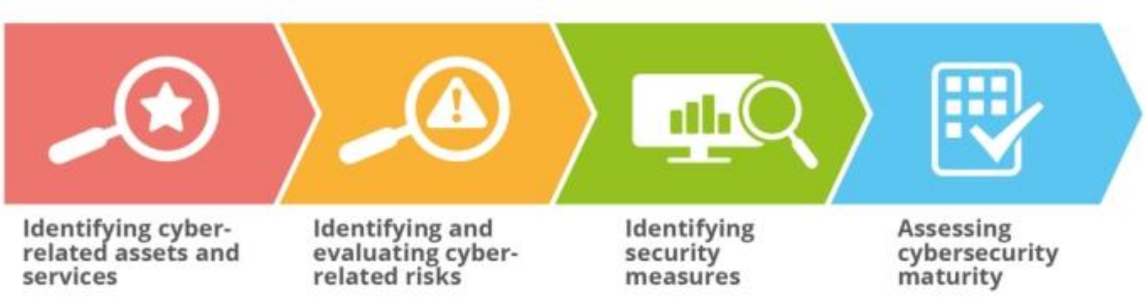

Identifying cyber-related assets and services
Identifying and evaluating cyber-related risks
Identifying security measures
Assessing cybersecurity maturity

Figure 6 - cyber risk management phases[90]

The four phase are divided as follow[91]:

- *Identifying cyber-related assets and services*: this phase focuses on the identification of key IT and OT assets. This phase is not necessarily constrained to the organisation's operational ecosystem, "Ports represents complex ecosystems where assets and systems are increasingly integrated and interconnected, resulting in service-based interdependencies and voluminous data exchanges that occur every day" (ENISA Guidelines, chapter 2.1). Third party interference increase vulnerabilities and the attack surface for potential malicious actors. The port must be able to continue its activities, provide its services, and understand the extent to which rapid re-establishment is possible after a cyber breach.
  Specific actions that can be perform are: identification of cyber-related assets and services, development of indicators to assess cybersecurity incident impact, assessment of the impact on Confidentiality, Integrity, and Availability of cyber-related assets. Finally, identification of internal and external dependencies. Consequently, it is fundamental to define the assessment focus; it can be asset-based or service-based.

[90] "Cyber Risk Management for Ports – guidelines for cybersecurity in the maritime sector" ENISA page 10

[91] "Cyber Risk Management for Ports – guidelines for cybersecurity in the maritime sector" A. Drougkas, A. Sarri, P. Kyranoudi, December 2020, ENISA

Furthermore, assets should be identified and registered in the asset inventory by the Service, System, and Information they support and handle, and dependencies should be identified on the technical interface requirements with third parties, vendors and between IT and OT systems (ENISA Guidelines, chapter 2.3).

- *Identifying and evaluating cyber-related risks*: Regardless the numerous methodologies and frameworks for identification and evaluation, the outcomes of this phase shall include "the identification of all relevant risks, which should be accompanied by an analysis of their likelihood and potential impact expressed in either a quantitative or qualitative way" (ENISA Guidelines, chapter 3.1).

  Port operators shall contextualise the risk identification and evaluation process, identify cyber-related threats, vulnerabilities, and internal/external dependencies, assess the possible likelihood, and impact of cybersecurity incident, and adopt specific methodology and indicators for identifying and evaluating risks. To do so, ENISA propose some related good practices, such as the engagement of representatives from all departments to collect accurate information and solicit cross-functional insights, or the definition of responsibilities for assets and services within each department. The Guidelines also include the definition of a Cyber Threat Intelligence (CTI) and its inclusion in the risk assessment methodology. Cyber vulnerability assessment and penetration tests are also important (chapter 3.3).
- *Identifying security measures*: "security measures should be adopted following a risk-based approach that directs budget, resources and technical capabilities towards the implementation of those security measures that will have the most substantial impact on the organisation's cyber risk posture" (chapter 4.1). Therefore, port operators shall identify security measures to mitigate identified risks and assess their effectiveness and impact, they shall also assess

resources requirements for the implementation of the aforementioned measures and define a process for prioritising them. Some effective good practices are the implementation of security measures based on predefined criteria, test security measures during cyber exercises internally and externally with port stakeholders, the adoption of a “security-by-design” approach in the procurement activities in order to reduce the need for additional allocation of resources during operational cycle of assets and services. Furthermore, the introduction of Key Performance Indicators (KPI) and the incrementation of the levels of staff awareness and training as the first line of defence, response, and recovery (chapter 4.3).

- Assessing cybersecurity maturity: this phase includes the prioritisation of security measures and the development of self-assessment for the determination of current maturity level. “A maturity self-assessment model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline”. To do so, the establishment of an organisation-wide cybersecurity capabilities baseline is required. Port operators must gain situational awareness of their cybersecurity capabilities and potential gaps. It is therefore important to implement technical training programmes to establish minimum cybersecurity awareness across all staff members but also seek advice from external sources (national or international authorities, private companies). Finally, port operators shall develop a cybersecurity programme to identify working group, resource allocations, training, performance objectives, and budgets (chapter 5.3).

  Cybersecurity capability maturity can be assessed through a three maturity levels: basic, intermediate, and optimal.

The ENISA guidelines and good practices represent a practical support for port operators but can be tailored to specific cyber risk management methodologies and context[92]. These good practices can be implemented in alignment with other methodology such as the ISPS code and other international standards.

III.II The International Context

The Protection of Critical Infrastructures is not just a European concern, in recent years, international organisations have shown their interest in cyber security matters and hybrid threats.

IMO, the International Maritime Organization, tried to make the maritime environment as safe and secure as possible through regulation and guidance. The Maritime Safety Committee (MSC) is the authority within IMO that sign and endorse IMO conventions and regulations.

III.II.I SOLAS Convention

The first IMO convention was the International Convention for the Safety of Life at Sea (SOLAS). The first version was adopted in 1914, in response to the Titanic disaster. The present version was adopted in 1974 and entered into force in 1980, however new amendments have been added in the aftermath[93].

“The main objective of SOLAS convention was to specify minimum standards for the construction, equipment, and operation of ships”. (“The SOLAS Convention - DNV.com”) SOLAS convention is divided into fifteen chapter, ranging from “fire protection” (chapter II) to “nuclear ships” (chapter VIII) and “special measures to enhance maritime security” (chapter XI). It does not refer to cyber security specifically.

[92] “Cyber Risk Management for Ports – guidelines for cybersecurity in the maritime sector” A. Drougkas, A. Sarri, P. Kyranoudi, December 2020, ENISA

[93] “SOLAS: the international convention for the Safety of Life at Sea, 1974” IMO, October 1998

It has been amended several times, usually to implement subsidiary regulation and in order to remain a solid milestone for the maritime sector over time[94].

Amendments often followed tragedies, after the 9/11 attack, a new maritime security regulatory regime was adopted into SOLAS, including the International Ship and Port Facility Security (ISPS code). And after the 1987's ferry accident in Belgium, SOLAS was implemented with the International Safety Management (ISM) code. ISM code serves today as the foundation upon which IMO member States have built the 2021 guidelines for cyber risk management[95].

The International Ship and Port Facility Security code (ISPS) is composed by a set of measures to enhance the security of ships and port facilities. ("International Ship and Port Facility Security Code - Wikipedia") It tries to further the intention of SOLAS, to provide a standardized, consistent framework for evaluating risks.

It is divided into two sections, section A concerning mandatory provisions and section B containing recommendatory provisions. Contracting Governments shall set security levels and "provide guidance for protection from security incidents" (ISPS, chapter 4.1)[96].

The aims of ISPS are to establish an "international framework involving co-operation between contracting governments, agencies, local administrations and the shipping and port industries to detect security threats and take preventive measures against security incidents" [97]. The Code allows also to establish roles and responsibilities, ensures early and efficient exchange of

[94] https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx

[95] "The IMO 2021 Cyber Guidelines and the Need to Secure Seaports" C. M. Petta, January 2021, CIMSEC

[96] "International Code for the Security of Ships and of Port Facilities" (ISPS code) Annex to SOLAS 1974, December 2002

[97] "International Ship & Port Facility Security Code and SOLAS Amendments 2002" IMO, 2003 edition.

security-related information, and provides a methodology for security assessment.

The other important document contained in SOLAS is the: “International Safety Management Code” (ISM) aimed at providing an international standard for the safe management and operation of ships. it is based on general principles and objectives. It was amended by IMO by Resolution MSC.104 (73) of December 2000.

The document speaks about “Safety Management Objectives” that should “provide for safe practices in ship operation and a safe working environment, assess all identified risks to ships, personnel and the environment and establish safeguard against” moreover “improve safety management skills of personnel ashore and abroad ships” (ISM code, chapter 1.2).

This general provision can be applied also to potential cyber risks, for this reason the ISM code is consider the predecessor of the 2021 guidelines on Cyber security of the maritime sector.

III.II.II IMO Resolutions

Cyber threats are directly mentioned in MSC-FAL.1-Circ.3 of June 2022. This document contains the guidelines on Maritime Cyber Risk Management by IMO. They provide high-level recommendations on maritime cyber risk management to safeguard shipping from cyberthreats.

According to IMO, cyber risk management is “the process of identifying, analysing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders”[98].

[98] https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

“The purpose of maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyber risks”[99].

The above-mentioned guidelines present five elements that support effective cyber risk management, these elements are also mentioned in NIST framework and will be better analysed in the following pages.

All of them must be employed concurrently and continuously (IMO Guidelines chapter 3.5):

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

the document also underlines the importance of appropriate levels of awareness of cyber risks at all levels of an organization, necessary to gain a sufficient protection against cyber threats.

The aim of the guidelines is to provide stakeholders with the appropriate knowledge and measures to safeguard shipping from current and emerging

[99] “Guidelines on Maritime Cyber Risk Management” IMO, June 2022, MSC-FAL.1/Circ.3/Rev.2

cyber threats and vulnerabilities. The guidelines are designed to foster safety and security management practices in the cyberspace.

However, in the document, it is underlined the fact that, IMO provisions are expressed in broad terms in order to have widespread application, which means that “ships with limited cyber-related systems may find a simple application of these Guidelines to be sufficient” (chapter 2.2.2)[100] but ship with complex cyber systems shall have greater level of care and therefore rely on additional resources from other reputable industries, organisations and Government partners[101].

Bearing in mind MSC-FAL/Circ. 3, another IMO resolution, the MSC.428, deals with Maritime cyber risk management. The document recognizes the “urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping” and recall the ISM code at its provision of “safe practices in ship operation and a safe working environment”. The MSC.428 affirms the increasing relevance of cyber risk management in accordance with ISM code and encourages administrations to properly address cyber risks in their annual verification of the company’s Document of Compliance.

III.II.III BIMCO Guidelines on Cybersecurity Onboard Ships

Other organisations have focused on this emerging issue, BIMCO has published the “Guidelines on Cyber Security Onboard Ships” which are fundamental to assist the development of proper cyber risk management strategy onboard.

[100] https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf

[101] “Guidelines on Maritime Cyber Risk Management” IMO, June 2022, MSC-FAL.1/Circ.3/Rev.2

BIMCO is the world’s largest international shipping association, representing 62% of the world’s tonnage[102]. It involves shipowners, operators, managers, brokers, and agents from all over the globe[103].

As shipping is relying increasingly on digital solutions which are on the one hand, the key for operational optimisation, cost savings, safety improvements and sustainable business, and on the other, as they rely on increased connectivity between servers, the cause of potential cyber vulnerabilities and risks.

BIMCO guidelines specify potential cases in which cyber incidents can arise, for example an unintended system failure occurring during software maintenance, or the manipulation of external sensor data, critical for the operation of a ship, infected USB or even crew interaction with phishing attempts (chapter 1.1)[104].

Cyber risk management approach is fundamental for a company’s safety and security culture, and it should be able to identify threats and vulnerabilities, assess risks exposure, develop protection and detection measures, establish response plans, and respond to and recover from cyber security incidents.

The document frequently recalls the ISPS and ISM codes, as they represent the milestone for security of the maritime sector.

The guidelines suggest that an “Effective cyber risk management relies on a clear allocation of responsibilities and tasks within the company” (chapter 1.3). the whole company shall be involved in the cyber risk management planning, usually following the normal chain of command; for example, Cyber

[102] *Press - BIMCO*, (https://www.bimco.org/about-us-and-our-members).

[103] https://www.bimco.org/

[104] “The Guidelines on Cyber Security Onboard Ships”, version 4, BIMCO, Chamber of Shipping of America, Digital Containership Association, Intercargo, Intermanager, Intertanko, ICS, IUMI, OCIMF, World Shipping Council, 2021

input to safety, which is the most critical tasks shall be appointed to the Managing director.

Organisations and individuals can constitute an intentional or even unintentional threat to the safety and security of the maritime sector.

The BIMCO guidelines set out two categories of cyber threats that may affect companies and ships: untargeted attacks, where company or ship's systems may be potential targets, and targeted attacks, where a company or a ship's system are the intended target.

The former use tools and techniques available on the internet to exploit vulnerabilities, such as virus, worms, and ransomware, while the latter are more sophisticated and use tools and techniques designed to specifically target a certain company or ship, such as social engineering, denial of service or phishing (chapter 2.2).

"The likelihood of a cyber security event happening is the product of threat and vulnerability" which means that if either of these factors is closer to non-existent, so will the likelihood (chapter 4.1). Risk assessment is carried out system by system and every connection is a potential vulnerability.

A company's Safety Management System (SMS) normally contain a risk assessment matrix where impact and likelihood of a given event are measured. The impact assessment should be carried out for every system and infrastructures in the maritime sector[105].

Detection is a central part of risk management. Scanning software, which can automatically detect and address the presence of malware, should be installed and managed. "Computers on board should be protected to the same level as office computers ashore, Anti-virus and Anti-malware software

[105] "The Guidelines on Cyber Security Onboard Ships", version 4, BIMCO, Chamber of Shipping of America, Digital Containership Association, Intercargo, Intermanager, Intertanko, ICS, IUMI, OCIMF, World Shipping Council, 2021

should be installed, maintained and updated" this would reduce potential cyber-attacks (chapter 8.1, 8.2).

Finally, the guidelines underline the importance of an effective response. Cyber incidents require active responses to return to normal operation, and sometimes this may go beyond the company's competencies, therefore external assistance shall be considered[106].

III.II.IV NIST Framework

NIST, the National Institute of Standards and Technology, part of the U.S. Department of Commerce. established a five key phases to incident response[107]:

- *Preparation*: critical components and their location must be determined and regular back up of all relevant data must be done. Moreover, an incident response plan must be created and rehearsed regularly, including roles and responsibilities, guidance on clear communication, and critical network and data recovery processes.
- *Detection*: the response team must be able to find out how the incident occurred, which IT and OT systems were affected, the extent of the damage and to what extent any threat to the systems remains.
- *Containment and Eradication and Recovery*: this is fundamental to contain the outbreak of an incident, where it is possible, it is mandatory to isolate the device from the network, checks firewalls and potential back doors, ensure updated anti-virus and anti-malware, and take a full disk image of any impacted systems.

[106] Id: "The Guidelines on Cyber Security Onboard Ships", version 4, BIMCO

[107] "Computer Security Incident Handling Guide", revision 2, NIST, P. Cichonski, T. Millar, T. Grance, Scarfone, August 2012

- *Post-incident activity*: this final phase is composed by the recovery of systems, the investigation of the causes of the incident and the attempt to prevent a re-occurrence of the event.

Then NIST published a "Cybersecurity Framework" to understand, manage and reduce cybersecurity risk and protect networks and data[108].

The first NIST framework was published in 2014 but then it was amended and implemented in the version "Framework for Improving Critical Infrastructure Cybersecurity" of 2018.

The aim is to "identify a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks" [109]. NIST framework want to enable organizations to apply the principles and best practices for risk management to improve security and resilience. It is a tool for aligning policy, business, and technological approaches. ("Cybersecurity and Infrastructure Security Agency | U.S ... - CISA")

It is composed by three main parts: the Framework Core, the Implementation Tiers, and the Framework Profiles.

The former provides a set of activities to achieve "specific cybersecurity outcomes"[110]. It comprises four elements:

- *Functions*: Identify, Protect, Detect, Respond and Recover. They are helpful for organizations to organize their management of cybersecurity risk by organizing information, enabling risk

[108] "The NIST Cybersecurity Framework" Federal Trade Commission, NIST, SBA, Homeland Security, (www.ftc.gov)

[109] "Framework for Improving Critical Infrastructure Cybersecurity", NIST, April 2018, version 1.1.

[110] *Tailoring the NIST Cybersecurity Framework for a Precise Fit* (https://www.tenable.com/blog/tailoring-the-nist-cybersecurity)

management decisions, addressing threats, and improving by learning from previous activities” (NIST framework, chapter 2.1)

- *Categories*: they are subdivisions of the Functions, such as the “Asset Management” or the “Detection Processes”.
- *Subcategories*: further division of the Categories into specific outcomes, such as “External Information systems” or “Data-at-rest is protected”.
- *Informative References*: they are specific sections of standards, guidelines, and practices common among critical infrastructure sector that illustrate method to achieve the outcomes. (“The NIST Cybersecurity Framework (CSF) 2.0 Functions, Profiles ...”)

The Functions are the fundamental part of the core, from which all other elements derived. They should be performed concurrently and continuously to efficiently address cybersecurity risks.

“Identify” is the development of an organizational understanding to manage cybersecurity risk. It comprises the understanding of the business context, resources available, and related cybersecurity risks. This enables an organization to focus and prioritize its efforts towards an efficient cyber risk management and business needs.

The “protect” phase enshrines the development and implementation of appropriate safeguards to ensure delivery of critical services. This phase allows to limit or contain the impact of a potential cybersecurity event, for example through the outcome category “Awareness and Training” or “Data Security”.

“Detect” refers to the development and implementation of appropriate activities to identify the occurrence of a cybersecurity event. It enables timely discovery, for example through “Detection processes” category.

Finally, we have “Respond” referred to the implementation of appropriate activities to detect and contain the impact of a potential cybersecurity incident, and “Recover” which comprises the development of activities to maintain plans for resilience and to restore capabilities or services impaired due to cybersecurity incidents.

Then, the NIST Framework present the “Implementation Tiers”, which aid to determine the extent to which cybersecurity risk management is developed and integrated into an organization’s risk management practices. Tiers rang from partial to adaptive, however they do not represent maturity levels, they are meant to support organizational decision making about the management of cybersecurity risk. Progression in the Tiers level is suggested when cost-effective and feasible reduction of cyber risks is expected (Chapter 2.2).

The Framework “Profile” is the alignment of the Core with the business requirements, risk tolerance and resources of the organization. It can be used to describe the current state of the organization or the desired target state of specific cybersecurity activities. (“Examples of Framework Profiles | NIST”) A profile enables the organization to establish a work schedule to reduce cybersecurity risk, aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices (chapter 2.3).

The NIST framework provides a means of “expressing cybersecurity requirements to business partners and customers and can help identify gaps in an organization’s cybersecurity practices. It also provides a general set of considerations and processes for considering privacy and civil liberties implications in the context of a cybersecurity program” (chapter 3.0) [111].

The framework provides a “common language” to communicate requirements among stakeholders responsible for the delivery of essential critical

[111] “Framework for Improving Critical Infrastructure Cybersecurity”, NIST, April 2018, version 1.1.

infrastructure services (chapter 3.3). Communication among stakeholders if crucial due to the complexity and interconnectedness of supply chains.

Supply Chain Risk Management (SCRM) is a critical organizational function and comprises a set of activities necessary to manage cybersecurity risk associated with external parties. SCRM shall include cybersecurity requirements for suppliers, formal contracts and agreements, and the verification that all those requirements are respected.

III.II.V IACS Recommendations on Cyber Resilience

To give a complete overview of the international cybersecurity landscape, another document deserves to be analysed: IACS "recommendation on Cyber Resilience". This document is particularly important because it gives reference guidelines, standards, goals and definitions for design and implementation and for verification testing.

Robert Ashdown, IACS Secretary General affirmed that "*The network design forms the basis for a reliable and robust network. Issues such as compatibility of various devices, communication between devices, communication from various systems and sub systems, need due consideration during design phase. This Recommendation is a crucial step in addressing cyber resilience from the earliest stages of a vessel's life*"[112].

IACS is the International Association of Classification Societies, it is a non-governmental association with the purpose of providing classification, statutory certification, and services; it also assists the maritime industry and regulatory bodies to safeguard maritime safety and pollution prevention[113].

[112] https://iacs.org.uk/news/iacs-launches-single-standalone-recommendation-on-cyber-resilience/

[113] https://iacs.org.uk/

IACS recommendations on Cyber Resilience aim at providing technical requirements to stakeholders to protect and provide ships with cybersecurity resilience which should be maintained throughout their service life[114].

Resilience is defined as "the characteristic that provides crew and ships the capabilities to effectively cope with cyber incidents occurring on computer-based systems onboard which contribute to operate and maintain the ship in a safe condition" (chapter 1.1.2).

The recommendation applies to onboard OT systems and to equipment that may have an impact on human or vessel safety. ("No. Recommendation on Cyber Resilience 166")

The Recommendation sets out functional requirements (chapter 6), in line with the five elements of risk management (Identify, Protect, Detect, Respond and Recover) and technical requirements (chapter 7) such as the inventory of computer-based systems, which must be done before vessel's delivery and must be updated during the life of the ship, modification should be tracked. Then we have System documentation which must be developed during design phase and include Network Communication Document (network technologies and cables, external connections, data flows) and risk assessment.

Finally, the document, in chapter 8 deals with "Testing". Verification and testing should be carried out at different stages, after construction of new vessels and during ship life, in order to ensure the functionality and efficiency of ship cyber risk management and resilience.

Despite all these regulations and guidelines, the maritime sector is slow in addressing cyber risks, maybe because their consequences are not palpable

[114] "Recommendation on Cyber Resilience" IACS, No. 166, April 2020

or because senior maritime stakeholders struggle to understand the changing risk environment[115].

The maritime sector is a multinational environment, and even if today the cyber risk management is a requirement of IMO, and therefore it would be expected that all maritime transport stakeholders should take similar actions, different postures and approaches are adopted, depending on individual level of understanding of specific topic. It seems that the perception of cyber security change according to diverse cultures. In an interesting study, made by Karamperidis, Watson and Kapalidis, this issue is taken into account.

They affirm that east Asian perceive cyber security as part of the overall aggregated risks affecting maritime transport operations, while western stakeholders perceive cyber security as a standalone risk element. Both eastern and western managers consider cyber security to be especially important, but approaches are quite different.

According to Europeans the maritime sector is prepared to address cyber risks while Asians believe the opposite.

Finally, Asians understand cyber security challenges better than Europeans and consequently incorporate them in the aggregated business risk management, they think “holistically”. In turn, western maritime stakeholders perceive cyber security as an “impartial risk factor to be dealt in isolation”. Differentiation can be assimilated to the level of maturity regarding cyber security, namely western maritime transport stakeholders seem to be less mature than east Asians[116].

[115] “Maritime Cyber Security: A global challenge tackled through distinct regional approaches” S. Karamperidis, C. Kapalidis, T. Watson, in Journal of Marine science and Engineering, November 2023

[116] “Maritime Cyber Security: A global challenge tackled through distinct regional approaches” S. Karamperidis, C. Kapalidis, T. Watson, in Journal of Marine science and Engineering, November 2023

Speaking about western maritime sector, it is now mandatory to look at the specific case of Italy. In the following section we will analyse Italian legislation and documentation regarding cyber security.

III.III The Italian Context

Maritime critical infrastructures are vital for Italian economy and stability; the "Italian boot" is surrounded by sea, and it is characterized by a long coastline and a maritime tradition.

Italian harbours play a logistic role as international interchange centres, thanks to their position within commercial routes with Europe, North Africa, and Asia. Italy has the third-largest intake traffic in the EU with five of the top forty ranking ports for tons and freights loaded, namely Trieste, Genova, Livorno, Gioia Tauro and Venezia[117].

Italy is the worldwide leader for short sea shipping (SSS), in terms of gross tonnage and passenger cargo, as reported by SRM (Research group for Intesa Sanpaolo), with Trieste and Genova in the EU top ten of commercial ports[118]. As these infrastructures become more reliant on digital technologies, they are increasingly vulnerable to cyberattacks.

In the last decade, Italy implemented a robust legal framework to address the cybersecurity of critical infrastructures, aligned with the European directives and guidelines, as well as with international standards.

Firstly, in 2012 with the decree n.21/2012 on energy, transport and communication, that from one side, specifies criterion to identify systems, networks, goods and relations of strategic relevance for national interest in the aforementioned sectors, and from the other, the possibility for the

[117] "Shipping and Air Quality in Italian Port Cities: State-of-the-art Analysis of Available results of estimated impacts" Merico, Cesari, Gregoris, Gambaro, Cordella, Contini, 2021, Atmosphere
[118] "Italian Maritime Economy" SRM, January 2023

President of ministries to veto over acts adopted by companies operating in energy, transport and communication if they may represent a threat for national interests and national security[119].

Then, decree n. 65/2018 that gives effect to NIS directive 2016/1148. This decree establishes a framework for the security of network and information systems in essential services, including maritime transport; it includes the identification of NIS competent authorities (ministries of economic development, infrastructures, transport, economy and finances, health and environment), and establishes the Italian CSIRT (Computer Security Incident Team), responsible for monitoring, managing and responding to cybersecurity incidents affecting critical infrastructures[120]. The decree also establishes obligations for operators of essential services, who must implement security measures, proportional to the risks they may encounter, and report incidents that significantly impact the continuity of their services (chapter 1, decree 65/2018)[121].

III.III.I Cybersecurity Decree

After the entry into force of NIS directive of 2016, Italian government revised the “DPCM Monti” of 24 January 2013 on the protection of cyber space and ICT security, with “DPCM Gentiloni” of 2017 also known as Cybersecurity Decree[122].

The latter aimed at optimising the management of cyber crisis and try to centralize responsibilities. The decree reflects the Italian response to increasing cybersecurity threats and the need to protect critical infrastructures. In the text critical infrastructures that require enhanced protection are identified, and they include sectors like: energy, transport,

[119] “Introduzione al diritto della sicurezza pubblica” Giappichelli Editore, Vipiana, 2024

[120] Id: “Introduzione al diritto della sicurezza pubblica”

[121] https://www.gazzettaufficiale.it/atto/stampa/serie_generale/originario

[122] DPCM Gentiloni, “Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali”. (17A02655) (GU Serie Generale n.87 del 13-04-2017) 17 February 2017

finance, healthcare, and telecommunications (article 1). It also reinforces the role of the department of information and security (DIS – Dipartimento di Informazione e Sicurezza) which incorporates the “National Cybersecurity Cell” (NSC – Nucleo di Sicurezza Cibernetica). NSC is an intergovernmental body for cybersecurity[123].

NSC is a permanent body that support the President of the Council of Ministries in the field of cybersecurity (Article 8); it is responsible for aspects related to prevention, preparation for possible cyber crisis and for the activation of warning procedures[124].

Finally, the Cybersecurity decree encourage private companies, especially those managing critical infrastructures, to collaborate with government agencies to enhance cybersecurity resilience and it suggests educational initiatives to improve skills and awareness (article 11).

III.III.II National Cybersecurity Perimeter

Then, law n.133/2019, established the PSNC (Perimetro di Sicurezza Nazionale Cibernetica), the National Cybersecurity Perimeter, which is a regulatory framework designed to protect critical infrastructures[125]. Indeed, it mandates stringent cybersecurity requirements for providers of essential services and public administrations that manage critical infrastructures. It was established to “ensure a high level of security of networks, information systems and computer services of the public administrations, public and private entities and operators” … “on which depends the exercise of an essential function of the State” … and “from its malfunctioning, interruption, even partial, or improper use of which could derive a prejudice to national security” (Art.1, law 133/2019).

[123] “Il futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici” R. Baldoni, R. De Nicola, P. Prinetto, Cybersecurity National Lab, gennaio 2018

[124] https://www.acn.gov.it/portale/en/coordinamento-interministeriale

[125] “Introduzione al diritto della sicurezza pubblica” Giappichelli Editore, Vipiana, 2024

The framework requires to report incidents promptly, to comply with regular security audits and to create a National Cybersecurity Agency for the coordination of cybersecurity responses in different sectors.

III.III.III National Cybersecurity Agency

In 2021, the National Cybersecurity Agency was established (ACN – Agenzia per la Cybersicurezza Nazionale) with the decree 82/2021[126], it is responsible for coordinating Italy's cybersecurity efforts, including the protection of critical infrastructures.

It is also responsible for preventing and mitigating as many cyber-attacks as possible and promoting the achievement of technological autonomy.

The key objectives of ACN are[127]:

- Prevention and mitigation: the agency support public and private entities in the prevention and mitigation of incidents and on the restoration of system.
- Strategic autonomy: ACN pursues national and European autonomy in the field of cybersecurity.
- Certification and supervision: the cybersecurity agency also evaluates IT products and services and conducts inspections to verify compliance with standards and regulations.
- Cyber Culture: the agency encourages training and awareness for the development of a cyber culture of the workforce in order to achieve national cyber readiness.

The ACN is also a point of contact between public actors, the production system, universities, and the world of research. The final aim is to raise

[126] https://www.normattiva.it/esporta/attoCompleto?atto.dataPubblicazioneGazzetta=2021-06-14&atto.codiceRedazionale=21G00098
[127] https://www.acn.gov.it/portale/en/chi-siamo

national cyber resilience and to this end, it also develops collaborations at the international level[128].

Law n.15/2024 gives effect to NIS 2 directive and impose the European stricter requirements[129], among them: establishment of policies and procedure, proper training and awareness, assessment of risks, report of significant incident within 24 hours and less significant incidents within 72 hours. NIS 2 directive requires States to adopt a national strategy for cybersecurity.

III.III.IV National Strategy for Cybersecurity 2022-2026

Italy positively responded to this request, implementing the National Strategy for Cybersecurity 2022-2026. It is a strategic document coordinated by ACN, to bolster national cybersecurity posture over a five-year period.

It emphasizes the importance of collaboration between public and private sectors, the development of cybersecurity capabilities and the constant monitoring of threats[130].

The Strategy has the aim of measuring progresses in the implementation of required measures, strengthen cyber resilience, and improve cyber crisis management[131].

In the text 82 measures are presented and analysed, among them: the reinforcement of national technological scrutiny that support security of the supply chain (measure #1, chapter 2.1.1), support of cyber development in accordance with cybersecurity certification for the evolution of the entrepreneurial system to achieve competitiveness in the market (measure #5, chapter 2.1.2), or the improvement of national defence, and resilience of

[128] https://www.acn.gov.it/portale/en/chi-siamo

[129] "legge 21 febbraio 2024 n.15" Gazzetta Ufficiale, Delega al governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea.

[130] "Manuale Operativo Implementazione Misure #82: piano di implementazione strategia nazionale di cybersicurezza 2022- 2026" ACN

[131] "Manuale Operativo Implementazione Misure #82 …" ACN

national critical infrastructures against cyber threats, counter-crime and cyber intelligence by further strengthening situational awareness through monitoring and analysis of threats, vulnerabilities and attacks (measure #12, chapter 2.1.3). Moreover, chapter 2.1.5 is dedicated to the protection of national infrastructures, and it contains measures to promote the development and implementation of procedures for monitoring and control of vulnerabilities and systems of public administration and private infrastructures against possible attacks.

The National Strategy for Cybersecurity also promotes International Cooperation (measure #43, chapter 2.2.5 and chapter 2.4.3), from the one hand, it recognizes the global nature of cyber threats, and from the other, it underlines the importance of partnerships to share best practices and coordinate responses to transnational breaches[132].

III.III.V Association of experts in Critical Infrastructures

Finally, it is interesting to mention the Italian Association of experts in Critical Infrastructure (AIIC), an association that promotes and favours research, training, analysis, awareness in the field of critical infrastructures, it also promotes their protection and cyber resilience[133]. The AIIC is composed by specialists, academicians, scholars, and experts in the field of critical infrastructures.

The Association collaborate with authorities, institutions, and public and private actors to better apply and understand current legislation. The primary focus is on services and critical infrastructures essential for safety, economic stability, and national security (energy grids, transportation networks, water supplies and communication systems).

[132] "Manuale Operativo Implementazione Misure #82: piano di implementazione strategia nazionale di cybersicurezza 2022- 2026" ACN

[133] https://infrastrutturecritiche.it/associazione-italiana-esperti-in-infrastrutture-critiche/

AIIC also pursue and promote the implementation of regulations and best practices concerning critical infrastructures[134]. It facilitates exchange of knowledge between experts and AIIC is also committed to the ongoing education and training of professionals working in the sectors.

The Association created a working group, the "Cyber Security Framework for Supply Chain" as part of its broader mission to protect and enhance the resilience of critical infrastructures, with the aim of determine strategies and framework necessary to spread the culture of cyber security of critical infrastructures and developed examples, best practices and guidelines for providers of essential services. The Framework is based on the National Cybersecurity Strategy[135].

This framework will help personnel of private and public organisation to detect, respond and recover after a cyber breach. Indeed, it emphasizes the importance of a comprehensive risk assessment to identify cyber threats within the supply chain, and critical points of failure. It also outlines the minimum cybersecurity standards necessary to protect critical infrastructures, such as: encryption, access controls, and incident response protocols.

In the end, the Cyber Security Framework for Supply Chain would play an essential role in enhancing the resilience of supply chains, and in the management of cybersecurity risks to safeguard a pivotal sector for national economy, welfare, and security, such as the one of Critical Infrastructures[136].

Italian maritime infrastructures are modernizing and growing, and their influence in the global trade is impactful, Italian ports moved half a billion of tons of goods, and sixty millions of passengers in 2022[137], in this developing context, it is fundamental to take into account the role played by cybersecurity.

[134] "Statuto Associazione AIIC" AIIC, 2021

[135] "Sensibilizzazione e Formazione in materia di Cyber Security" AIIC, June 2016, I. Corradini, R. D'Alessandro.

[136] Id: "Sensibilizzazione e Formazione in materia di Cyber Security" ...

[137] "Italian Maritime Economy" SRM, January 2023

Even if the country’s legal framework provides strong basis, ongoing efforts are needed to address emerging threats and ensure security and safety of Italian maritime activities.

IV. Case Study: Ransomwares and the "NotPetya" Attack suffered by A.P. Moller Maersk

IV.I Ransomwares

Between 2010 and 2020, ransomware attacks became increasingly common, they have evolved into one of the biggest cyber security threats[138].

Figure 7 shows how the incidence of ransomware attacks grew over the year and skyrocketed in 2021 after the Covid-19 pandemic that has witnessed a huge surge in the rate of ransomware attacks[139]. In 2023 international organizations detected 317.59 million of ransomware attempts[140].

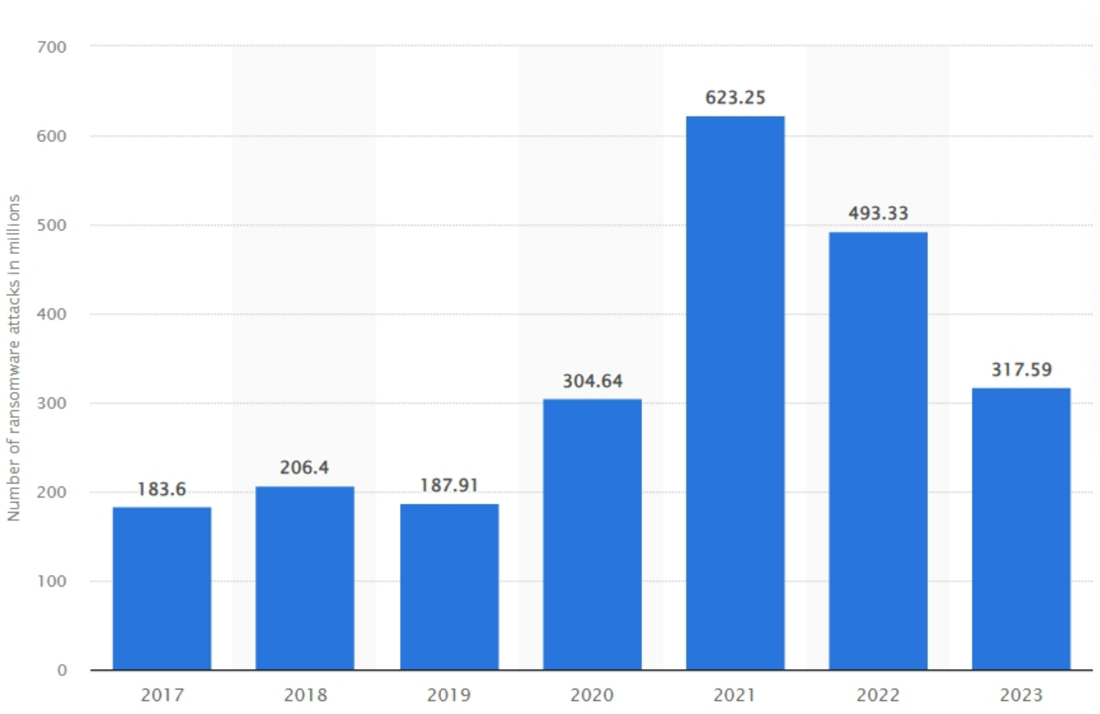


Figure 7 Annual number of ransomwares attempt worldwide from 2017 to 2023[141]

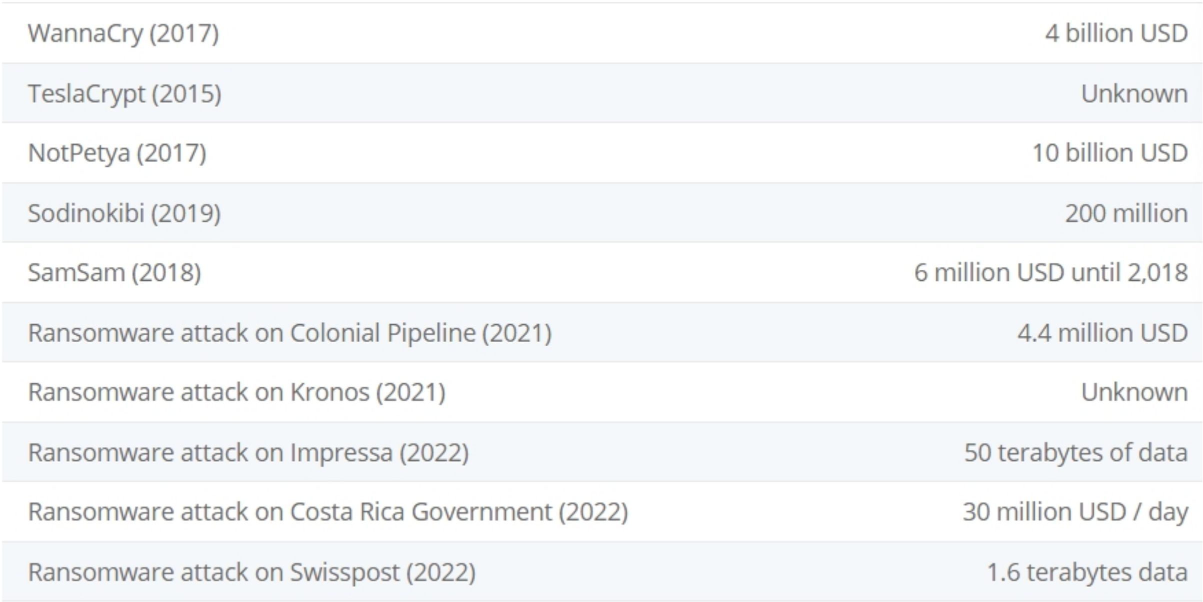
[138] ""Evolution of a ransomware" P. O'Kane, S. Sezer, D. Carlin, May 2018, The Institution of Engineering and Technology

[139] "Ransomware: recent advances, analysis, challenges and future research directions" C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, M. K. Khan, December 2021

[140] "Number of ransomwares attempts per year 2017-2023" A. Petrosyan, April 2024, Statistica

[141] https://www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide/

Among the most significant and devastating attacks, we recall the “WannaCry” ransomware that caused damages all over the globe encrypting computer systems through a Windows vulnerability with an estimate total damage of 4 billion US dollars, as shown in figure 7 or the TeslaCrypt famous for infecting gaming files such as user profiles, recorded replays or even the CovidLock ransomware that in 2020, during the pandemic, encrypted data on Android devices and denied access to data[142]. One of the most devastating ransomwares, however, was the NotPetya ransomware, that in 2017 cause major damages for several organisations and Ukrainian entities; we will better analyse this case in the hereafter.



WannaCry (2017)	4 billion USD
TeslaCrypt (2015)	Unknown
NotPetya (2017)	10 billion USD
Sodinokibi (2019)	200 million
SamSam (2018)	6 million USD until 2,018
Ransomware attack on Colonial Pipeline (2021)	4.4 million USD
Ransomware attack on Kronos (2021)	Unknown
Ransomware attack on Impressa (2022)	50 terabytes of data
Ransomware attack on Costa Rica Government (2022)	30 million USD / day
Ransomware attack on Swisspost (2022)	1.6 terabytes data

Figure 8 Most significant ransomware attacks worldwide by impact[143]

[142] “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions” O. Aslan, S.S. Aktug, M. Ozkan-okay, A.A. Yilmaz, E. Akin, March 2023, Electronics
[143] https://www.statista.com/statistics/1410605/largest-ransomware-attacks-worldwide/

The extortion of digital data and files have existed since the eighties and remains a global threat at peak level still today[144], the first sample of ransomware was the Cyborg Trojan in 1989[145]. During the nineties and early 2000s a curious characteristic was that ransomwares were mostly carried out by hobbyist hackers who wanted to gain notoriety over cyber pranks. Only after 2005 we had the appearance of modern ransomware attacks; they quickly became a financial business for hackers. Targets shifted from individuals to organisations in order to fetch larger ransoms[146].

As we already mentioned in chapter II, ransomwares are malwares, that encrypt files, documents, data, and applications in a computer and make them unavailable. After the ransomware infects the computer, victims are asked to pay a ransom in cryptocurrency and in return, their data are promised[147].

However, often criminals keep copies of the data to use them in future fraud or phishing attempts or even they never reestablish the original status of the encrypted files.

Hundreds of millions of dollars are stolen as a ransom by hackers every year[148].

A complex infrastructure has grown to support Ransomware attacks, as shown in *figure 9.*

O'Kane, Sezer and Carlin analysed this particular infrastructure, showing that it includes social engineering tactics to tailor phishing emails and engage with

[144] "The 2023 Global Ransomware Report" Fortinet (https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2023-ransomware-global-research.pdf)

[145] "A comprehensive survey: ransomware attacks prevention, monitoring and damage control" J. Tailor, A. Patel, 2017, International Journal of Research and Scientific Innovation.

[146] "Ransomware: Recent advances, analysis, challenges and future research directions" C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, M. K. Khan, December 2021, Science Direct

[147] Id: "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions"

[148] "Ransomware Detection using Random Forest technique" B. M. Khammas, November 2020, Science Direct

the victim, then it includes a “booby-trap”, the “Landing page” that tries to scan a victim’s computer looking for vulnerabilities and trying to install the ransomware in the victim’s computer.

After the infection, the ransomware proceeds with the data encryption and finally, only after this phase, the victim become aware of the encryption through a pop-up demanding a ransom to regain access to data[149].

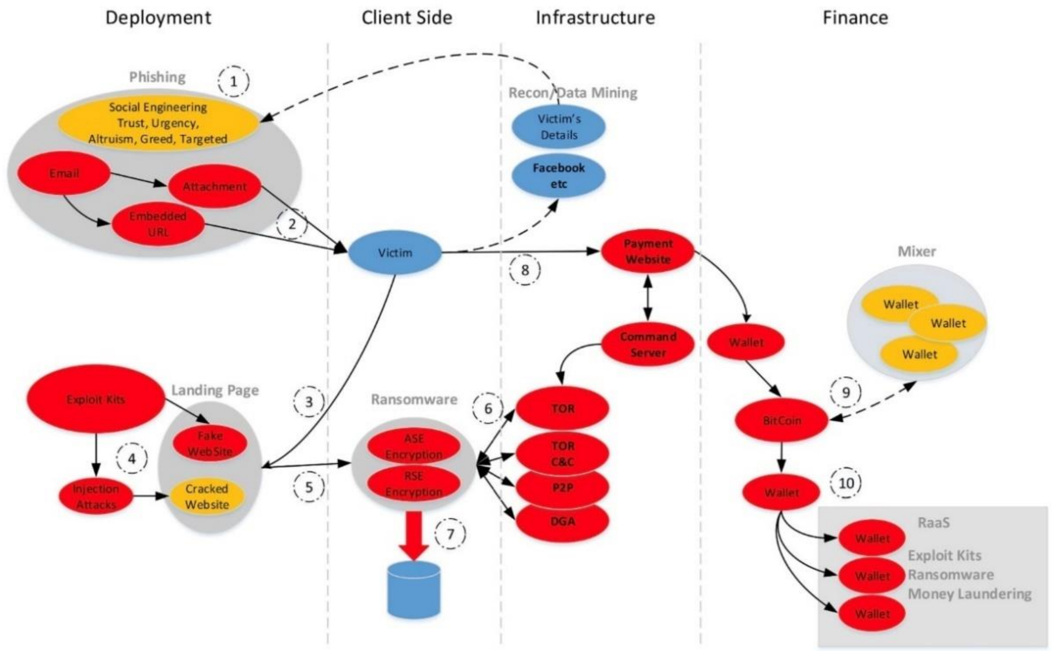


Figure 9 - Attack Landscape[150]

The Ransomware is a profit-driven business, a form of extortion that rewards online criminal activities. Over the years the payment techniques have evolved and today short message service to premium rate numbers (chapter 5, The Evolution of ransomware) or Payment services such as website similar

[149] “Evolution of a ransomware” P. O’Kane, S. Sezer, D. Carlin, May 2018, The Institution of Engineering and Technology

[150] “Evolution of a ransomware” P. O’Kane, S. Sezer, D. Carlin, May 2018, The Institution of Engineering and Technology

to PayPal, where the victim deposits the payment specified in the ransom note, are the most used methods[151].

Ransoms are typically demanded in Bitcoin, which makes it difficult to track the recipient of the transaction and moreover, it allows hackers to evade law enforcement agencies[152].

The General advice that experts suggest is not to pay the ransom, when dealing with criminals, the victim has no guarantee of recovering data. Paying the ransom does not guarantee the release of locked systems or files.

Ransomware can be categorized into three forms, as shown in figure 10.

A locker ransomware impedes the access to the computer or device and then prompts the user to pay a ransom to restore functionalities. This type of ransomware leaves intact the systems and files, experts can use tools and techniques to access the computer infected and restore its default status. The impact of the attack is therefore limited or at least less dangerous than the other types[153].

A crypto ransomware blocks the access to specific files or data. This type of ransomware encrypts important data stored in the infected computer and makes them inaccessible then it demands a ransom to obtain the decryption key. Even if Crypto ransomware does not interfere with basic computer functions its effects are irreversible and devastating[154].

Finally, Scareware ransomwares are different from the two mentioned above, indeed they do not cause any harm to the victim's computer, but they use pop-up ads to manipulate users. They claim to have detected a virus on a

[151] Id: Evolution of a ransomware"

[152] "Ransomware: Recent advances, analysis, challenges and future research directions" C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, M. K. Khan, December 2021, Science Direct

[153] "A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat: Proceedings of ICDMAI 2018" A. Tandon, A. Nayyar, chapter in Advances in intelligent Systems and Computing, January 2019

[154] Id: "A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat..."

device and ask users to download or buy a fictitious antivirus that hides the malicious software. Hackers exploit the victim's fear[155].

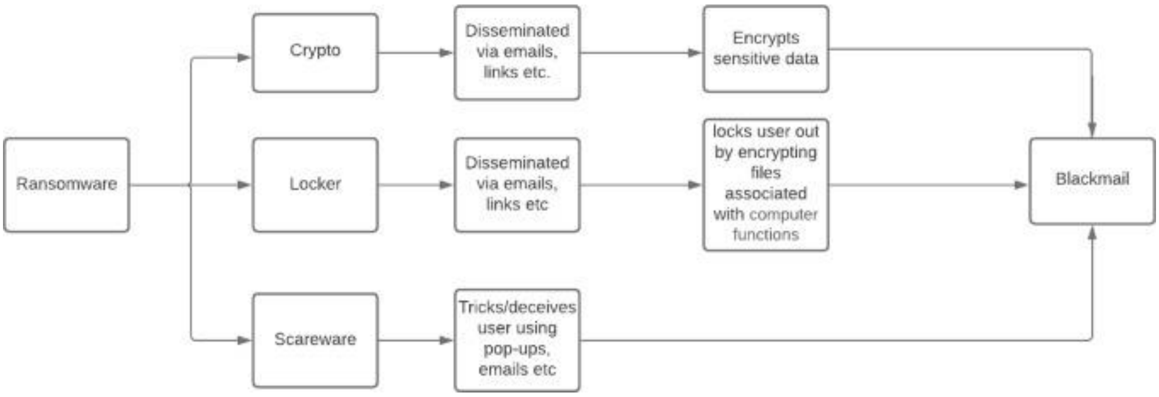

Ransomware
Crypto
Locker
Scareware
Disseminated via emails, links etc.
Disseminated via emails, links etc
Tricks/deceives user using pop-ups, emails etc
Encrypts sensitive data
locks user out by encrypting files associated with computer functions
Blackmail

Figure 10 Categories of Ransomware[156]

IV.II The Case of NotPetya ransomware

Ransomwares usually target organizations that collect numerous data especially critical data[157], indeed those malwares are dangerous for individual users, but they are much more dangerous for organisations that after the infection cannot conduct their day-to-day operations[158].

This is the case of A.P. Moller Maersk, the Danish maritime company that suffered one of the most high-profile and disastrous maritime cybersecurity incidents to date[159].

Still today numerous studies are conducted to analyse NotPetya attack and its consequences. Indeed, NotPetya campaign represents a turning point that explains from one side the relevance of international law and cyberwarfare

[155] "Ransomware: Recent advances, analysis, challenges and future research directions" C. Beaman, A. Barkworth, T. D. Akande, S. Hakak, M. K. Khan, December 2021, Science Direct
[156] Id: "Ransomware: Recent advances, analysis, challenges and future research directions" t
[157] "Number of ransomwares attempts per year 2017-2023" A. Petrosyan, April 2024, Statistica
[158] "A Systematic Literature Review on the Cyber Security" Dr. Yusuf Perwej, S. Qamar Abbas, J. Pratap Dixit, N. Akthar, A. Kumar Jaiswal, 2021, International Journal of Scientific Research and Management
[159] "Maritime Cyber Attacks" M. Bialas, August 2021, Vessel Automation

and from the other, the disastrous effects that cyber breaches can cause to organisations whether public or private ones[160]. Before analysing the Maersk's crisis and collateral damages, we will contextualise NotPetya and its origin.

IV.II.I NotPetya Backstory and the International Response

NotPetya campaign started on the 27th of June 2017 in Ukraine. The 27th of June is an important date for Ukrainian because it is the day of the celebration of their Constitution.

This date was food for thoughts, some argue that it was a clear signal of the intention of attacking the nation during such an important holiday, others argue that the date was chosen because the majority of IT operators would be on leave and therefore defence would work with less promptness and resources[161].

Even if the malware hit other countries, most machines infected were Ukrainian, therefore it is suspected that the target was Ukraine as a state and not some companies, such as Maersk or Merck, which were however massively affected[162].

The Malicious code had the characteristic of a ransomware, but the email address provided to send the ransom was fake and therefore there was no chance of recovering the lost data. "If the attack was financially motivated, the attacker would have remained available and would have secured the return of the data in exchange for a ransom" affirmed Csaba Krasznay (page 485 -technical perspective-)[163].

[160] "Cyber-attack impact estimation for a port" Konig, Rass, Schauer, 2019, Hamburg International Conference of Logistics

[161] "Case Study: The NotPetya Campaign" C. Krasznay, January 2020, ResearchGate

[162] Id: "Case Study: The NotPeya Campaign"

[163] Id: "Case Study: The NotPeya Campaign"

The code of NotPetya showed similarities with the "Petya" ransomware, a strain of ransomware appeared in 2016 that encrypted files on computers; but it was soon discovered that this was an intentional camouflage. The name NotPetya comes from this resemblance[164].

"The reason NotPetya was so different, and even scary, is that it seems that a lot of what happened during the attack was automated, intended to deceive and distracts its victims, and thereby disrupt the response" affirmed Oleh Derevianko, the head of Kiev-based cybersecurity firm Information Systems Security Partners (ISSP) a week after the attack during an interview[165]. Ukraine was devastated by NotPetya, an estimated 10% of all Ukrainian computers were destroyed[166].

On the 2nd of July 2017, the BBC News reported a statement by Ukrainian intelligence, who claimed to find proof that Russia was behind it. However, Moscow denied any involvement and declared any possible proof "unfounded"[167]. International actors started questioning whether this was a form of warfare and whether international law shall be applied.

NATO Cooperative Cyber Defence Centre of Excellence experts stated that "the ransomware was probably launched by a state actor or a non-state actor with support of approval from a state"[168].

Michael Schmitt and Jeffrey Biller tried to illustrate the complexity of applying international law to ambiguous cyber scenarios like this one in their article "The NotPetya Cyber Operation as a Case Study of International Law".

The two researchers affirm that sovereignty was violated during NotPetya attack[169], indeed the unavailability of a cyber infrastructure for a prolonged

[164] "Case Study: The NotPetya Campaign" C. Krasznay, January 2020, ResearchGate

[165] "The day a mysterious cyber-attack crippled Ukraine" C. Borys, July 2017, BBC

[166] "The Economics of Cybersecurity and Cyberwarfare: A Case Study" L. Carrazana, December 2018

[167] Id: "The day a mysterious cyber-attack crippled Ukraine"

[168] https://cyberlaw.ccdcoe.org/wiki/NotPetya_(2017)

[169]"The NotPetya Cyber Operation as a Case Study of International Law" M. Schmitt, J. Biller, July 2017

period of time can be seen as a damage to national physical facilities and therefore a violation of territorial integrity. They also state that “If a State launched NotPetya, Russia is the most likely suspect”[170].

If Russia was involved and NotPetya was used as a cyberweapon, we may be entering a new territory in geopolitics. NotPetya is the first cyber incident that appears to be targeted to a sovereign State during peacetime. The purpose of this ransomware was destruction not extortion[171]. The tactics of NotPetya were new and highly sophisticated, clearly planned.

The two researchers try to understand if the operation constituted “hostilities”, and they affirm that “cyber operations that result in physical damage, injury, or death obviously constitute an attack”[172]. The NotPetya ransomware was directed to national critical infrastructures and caused great damages such as delays, interruption of critical services and of communication and loss of critical data.

Then, Schmitt and Biller underline the fact that, according to the Geneva Convention of 1949 on International Armed Conflict, it is prohibited to conduct (cyber) attacks in an indiscriminate manner, NotPetya had widespread effects on civilian infrastructures, including Kiev Airport, the Chernobyl power plant and even the Ukrainian healthcare system.

Schmitt and Biller conclude their study affirming that “NotPetya malware appeared to cross the line of cyberwarfare, as evidenced by its effects on infrastructures”[173].

[170] Id: “The NotPetya Cyber Operation as a Case Study…”

[171] “Case Study: The NotPetya Campaign” C. Krasznay, January 2020, ResearchGate

[172] “The NotPetya Cyber Operation as a Case Study of International Law” M. Schmitt, J. Biller, July 2017 Blog of the European Journal of International Law

[173] Id: “The NotPetya Cyber Operation as a Case Study of International Law”

Cyberwarfare works in shadow and rather than revolutionary break can cause strategic instability in rivals' actions[174].

Cyberwarfare may be a new domain of warfare. Indeed, even if cyberattack may not cause physical violence, they may be used as part of a broader conventional war to cause destruction[175]. At a tactical level, rather than soldiers on the field, cyberattack can be launched by a single person form anywhere on Earth causing destructive effects, moreover it has the unique capability of targeting military forces, as well as economic capacity of a nation[176].

The U.S. Government attributed the ransomware attack to Russia affirming that: "In June 2017, the Russian military launched the most destructive and costly cyber-attack in history. The attack quickly spread worldwide, causing billions of dollars in damage. It was part of the Kremlin's ongoing effort to destabilize Ukraine" (The Press Secretary of the White House)[177].

Also, other countries, close U.S. allies, attributed the attack to Russia; for example, the U.K. Foreign and Commonwealth Office that affirmed that "the UK Government judges that the Russian military was responsible for the destructive NotPetya cyber-attack. The attack showed a continued disregard for Ukrainian sovereignty"[178], or the Australian Government in official documents that declared "We condemn Russia's behaviour, which posed grave risks to the global economy, to government operations and services, to business activity and the safety and welfare of individuals" (Minister for law Enforcement and Cyber Security A. Taylor)[179].

[174] "Fancy Bears and sigital trolls: Cyber Strategy with Russian twist" B. Jensen, B. Valeriano, R. Maness, January 2019, Journal of Strategic Studies

[175] Id: "Fancy Bears and sigital trolls: Cyber Strategy with Russian twist"

[176] "The Economics of Cybersecurity and Cyberwarfare: A Case Study" L. Carrazana, December 2018

[177] "Case Study: The NotPetya Campaign" C. Krasznay, January 2020, ResearchGate

[178] Id: "Case Study: The NotPetya Campaign"

[179] "Australian Government attribution of the 'NotPetya' cyber incident to Russia" 16 February 2018 (https://www.dfat.gov.au)

In February 2018 the United States, The United Kingdom, Denmark, Lithuania, Estonia, Canada, and Australia jointly condemned Russia for the NotPetya attack, with the support of Norway, New Zeeland, Latvia, Sweden, and Finland[180].

"What we are doing is maturing this approach in order that the consequences will be felt further in the future. So, another part of deterrence is signalling to another country, to provide clear, consistent, and credible messaging to adversaries that there will be repercussions for their behaviour" (Tobias Feakin, Australia's Ambassador for Cyber Affairs)[181].

In other cases, such as in the Stuxnet case, Russia was accused of using cyber operations to cause discomfort and destruction. Cyber disruptions are "low-cost, low-payoff form of cyber strategy"[182].

Cyber destructions are designed to sabotage the enemy's networks and operations[183]. Russia's cyber operations threaten stability targeting critical systems and infrastructures, such as the Chernobyl nuclear plant that was partially blocked by NotPetya.

IV.II.II Methodology of Attack

In terms of actions, NotPetya infected the computer's master boot record, the hard disk responsible for loading the operating system. NotPetya combined two powerful hacking tools: EternalBlue and Mimikatz. The former was a penetration tool stolen from the U.S. National Security Agency able to find a vulnerability in Windows operating systems and execute arbitrary code on Windows devices and the latter was created by the French researcher

[180] "Blaming Russia for NotPetya was coordinated diplomatic action" Stilgherrian, April 2018
[181] "Blaming Russia for NotPetya was coordinated diplomatic action" Stilgherrian, April 2018
[182] "Fancy Bears and sigital trolls: Cyber Strategy with Russian twist" B. Jensen, B. Valeriano, R. Maness, January 2019, Journal of Strategic Studies
[183]Id: "Fancy Bears and sigital trolls: Cyber Strategy with Russian twists

Benjamin Delpy in 2011 with the aim of demonstrating that Windows passwords could be retrieved from system memory and allow attackers to access compromised devices[184].

When the National Security Agency was hacked and EternalBlue stolen, Windows released promptly a patch, but it was compatible just with newer Windows systems, the older operating systems received the patch too late or never received it[185].

Before NotPetya, another malware, the WannaCry ransomware, exploited EternalBlue, so the potential harm of this tool had already been demonstrated before NotPetya, the problem was that millions of operating systems continued to lack proper updates in the aftermath of WannaCry.

Mimikatz was able to store users' encrypted passwords but also their decryption keys. This allowed Mimikatz to pivot to all machines on the same network. When it was stolen and used in NotPetya attack, it allowed hackers to move easily onto all computers within the same network.

NotPetya combined those two tools and on the one hand was able to infect machines and encrypt data easily and repeatedly (EternalBlue) and on the other hand, before making the machine unusable it tried to spread in the computer network with an effective tactic: firstly, it collected the administrator password and credentials and then it used them to access other machines (Mimikatz)[186].

The same Mimikatz inventor, Benjamin Delpy declared the NotPetya ransomware was a "virulent combination" of the two tools and that the Windows patch was not enough to save a device because "you can infect

[184] "NotPetya: A Columbia University Case Study" School of International and Public Affairs, January 2022

[185] Id: "NotPetya: A Columbia University Case Study" 2

[186] "Case Study: The NotPetya Campaign" C. Krasznay, January 2020, ResearchGate

computers that aren't patched, and then you can grab the passwords from those computers to infect other computers that are patched"[187].

The first infection was made through a software update of the MEDoc application, a Ukrainian tax return programme. This is the reason it could hit so many infrastructures and companies, they all relied on MEDoc for tax accountability, the application was used by about one million businesses operating in Ukraine[188].

According to the cybersecurity company Talos, on the 24th of April an update of Medoc containing a backdoor was released. This backdoor was the element that allowed the attack to be carried out[189].

The victims include Ukrainian critical infrastructures such as 22 Ukrainian Bank, Kyiv Borispol Airport, ATM and card payment systems, Ukrainian energy companies among which the Chernobyl nuclear plant, hospitals and the national postal service. "It was a massive bombing of all our systems" declared Volodymir Omelyan, the Ukrainian minister of Infrastructures[190].

While NotPetya was aimed at Ukraine, it went beyond Ukrainian borders and caused tangible effects, approximately $10 billion of damages worldwide[191]; indeed, also several States (as shown in figure 11) and foreign companies were infected, for example the American medical company Merck, the Hungarian OTP bank, FedEx, and the Danish maritime company A.P. Moller Maersk[192] who suffered the most devastating effects of NotPetya.

[187] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History" M. Mcquade, August 2018, Wired

[188] "NotPetya: A Columbia University Case Study" School of International and Public Affairs, January 2022

[189] "Case Study: The NotPetya Campaign" C. Krasznay, January 2020, ResearchGate

[190] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History" M. Mcquade, August 2018, Wired

[191] Id: "The Untold Story of NotPetya, the Most Devastating Cyberattack in History"

[192] "Case Study: The NotPetya Campaign" C. Krasznay, January 2020, ResearchGate

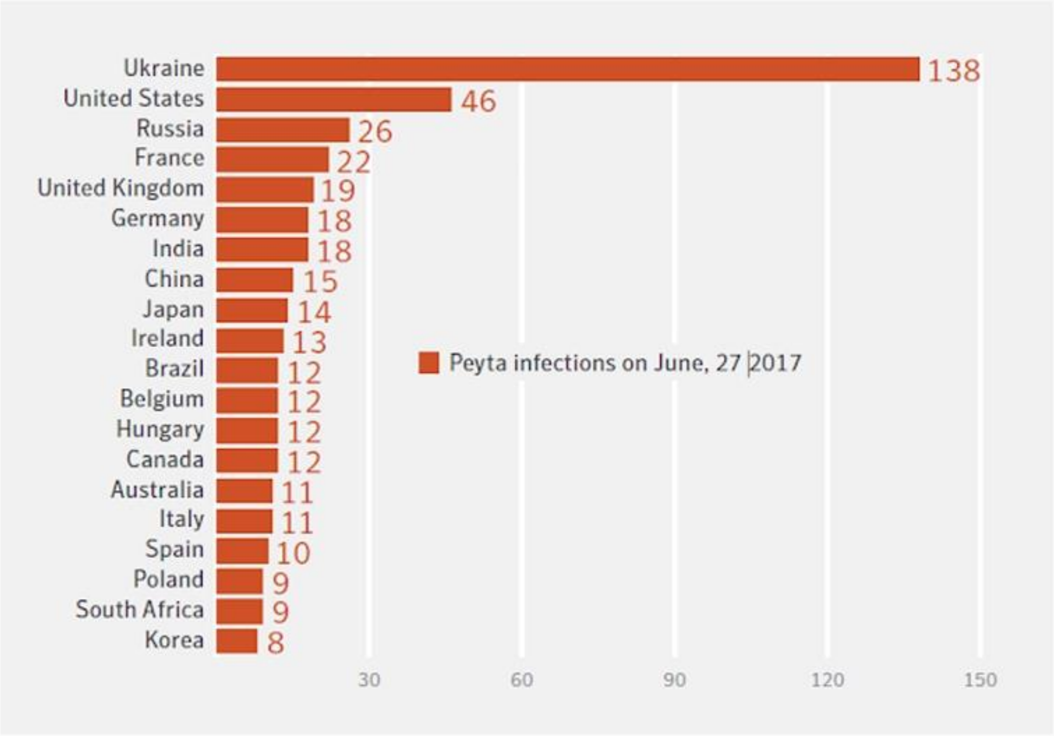


Figure 11 NotPetya attacks by country[193]

IV.II.III A.P. Moller Maersk disastrous incident

Back in 2017 A.P. Moller Maersk was the largest maritime shipping company, with offices across 130 countries and over 75.000 employees around the world[194].

At that time, like many other companies, Maersk did not see itself as a potential target for cyberattacks and the negligence in develop a proper cyber security response and risk assessment cost the company over 49.000 PCs and 4.000 servers for an estimated value of over $300 million (According to the company's esteem) [195].

[193] "NotPetya: A Columbia University Case Study" School of International and Public Affairs, January 2022

[194] Id: "NotPetya: A Columbia University Case Study"

[195] "Maritime Cyber Attacks" M. Bialas, August 2021, Vessel Automation

When the malware hit Maersk, it propagated in around 7 minutes through the network. Computer screens faded to black showing a message demanding payment in exchange for decryption keys, the account from which the ransom was sent was later discover being fictitious and data could never be retrieved[196].

NotPetya entered Maersk system through MEDoc application in a computer in Odessa, Ukraine. The lack of proper segmentation in the network systems allowed the malware to spread beyond Maersk Ukraine computers and run throughout the company's global operations[197].

The IT staff tried to coordinate a defence but there was no time, and all computers shut down in near simultaneity. IT staff needed to disconnect the entire Maersk global network, which means that every employee had been ordered to turn off their devices. Maersk's network was completely destroyed and in that situation IT staffers were helpless[198].

Seventeen of the seventy-six Maersk international ports were paralyzed, loading and unloading of containers was not possible, truckers did not know what to do with goods and also the shipment booking tools were disabled so the core source of revenue of Maersk was cut off[199]. Terminal operators could not know what was to be unloaded from container ships and which container were to be loaded onto which ships or where to be sent from the port terminal[200].

Computers on the company's ships were not infected but as the terminals' software were destroyed, Electronic Data Interchange from those ships was completely wiped away[201].

[196] Id: "Maritime Cyber Attacks"

[197] "NotPetya: A Columbia University Case Study" School of International and Public Affairs, January 2022

[198] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History" M. Mcquade, August 2018, Wired

[199] "NotPetya: A Columbia University Case Study" School of International and Public Affairs, January 2022

[200] "The Economics of Cybersecurity and Cyberwarfare: A Case Study" L. Carrazana, December 2018

[201] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History" M. Mcquade, August 2018, Wired

From Los Angeles to Mumbai, Maersk's terminals and offices were paralyzed.

The Danish company hired the consulting firm Deloitte (based in London) to manage the recovery. IT staffers tried to rebuild Maersk's network, but they sooner discover that no backup prior to NotPetya contained a crucial layer: the company's domain controller[202].

Maersk owned approximately 150 domain controllers responsible for mapping the network and determining the division of responsibilities of users. The company programmed them in a way that any could function as a backup for all the others. But the decentralized backup strategy did not take into account the scenario in which all domain controllers were wiped away simultaneously[203].

The glimmer of hope arrived after a desperate search from a remote office in Ghana. Before NotPetya attack, the Ghanaian office suffered a power outage, and all machine remained offline. Therefore, the Ghanaian computers remained disconnected from the network[204].

However, the remote office had low bandwidth, and the domain controller was so sizable, we speak about hundreds of gigabytes that would have taken days to be transmitted.

Therefore, it was decided that a Ghanaian employee would have flown to the UK and transport physically the server. However no Ghanaian employee had the British visa, so a new plan was then approved: a Ghanaian employee had to fly to Nigeria to meet another Maersk employee and transmit the hard drive containing the precious domain controller. The Nigerian employees has then to fly to London where Maersk and Deloitte staffer were trying to fix the problem[205].

With this operation completed, Maersk could start the backup of core services. The priority was the restore of port operations, but sooner also booking services came back. After more than a week also the Maersk's global terminals were back to normal[206].

[202] Id: "The Untold Story of NotPetya, the Most Devastating Cyberattack in History"

[203] "NotPetya: A Columbia University Case Study" School of International and Public Affairs, January 2022

[204] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History" M. Mcquade, August 2018, Wired

[205] Id: "The Untold Story of NotPetya, the Most Devastating Cyberattack in History"

[206] "NotPetya: A Columbia University Case Study" School of International and Public Affairs, January 2022

The full recovery took approximately two months. A key part of Maersk's response was transparency, internally with employees and externally with other firms[207]. Since then, with the aim of reducing the likelihood of future attacks, Maersk had worked to improve its cybersecurity and to make it a "competitive advantage"[208].

Multifactor authentication, upgrades and training are today milestone of the company's cybersecurity Risk Assessment. Maersk set out a cybersecurity culture based on the concept that "security is everyone's responsibility" and therefore from that moment on, the company invest much on training and technical support[209].

However, the lesson learnt demonstrated that firms when implementing their cybersecurity, must take into account three substantial costs of cyberattacks: firstly, they must assess the cost of being offline which means that firms must consider the fact that due to a cyberattack, they may be unable to use the network. Being offline has an associated cost that firms must consider[210].

Secondly, they must have regard to the costs of paying specialists to repair the damages, in the case of NotPetya, Maersk had to pay millions of dollars to replace the destroyed hardware[211].

And thirdly, firms must consider the cost of losing reputational respect among consumers[212]. After the NotPetya attack Maersk suffered a reputational damage that took long to be healed, but today the company consider Cyber Security as a top-line growth capability, able to create trust in costumers and to increase business revenue.[213]

The Maersk's experience with NotPetya also emphasizes the importance of two cybersecurity practices[214]: Network segmentation in order to avoid the

[207] "Rebuilding after NotPetya: How Maersk moved forward" D. Swinhoe, October 2019, CSO

[208] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History" M. Mcquade, August 2018, Wired

[209] "The 2017 MAERSK Cyber Incident: learning from and applying the lesson of a major cyber incident" Maersk, October 2020

[210] "The Economics of Cybersecurity and Cyberwarfare: A Case Study" L. Carrazana, December 2018

[211] Id: "The Economics of Cybersecurity and Cyberwarfare: A Case Study" L. Carrazana, December 2018

[212]"Cybersecurity and Cyberwar: What Everyone Needs to Know", P. W. Singer, 2014, Oxford University Press.

[213] "The 2017 MAERSK Cyber Incident: learning from and applying the lesson of a major cyber incident" Maersk, October 2020

[214] "NotPetya: A Columbia University Case Study" School of International and Public Affairs, January 2022

problem of simultaneous destruction and proper Recovery plans for when the attack occurs.

Considered all this above, the fact that cyber threats and risks are expected to remain, and the central role played by ports and ships in the supply chain, the importance of cyber-security in the maritime sector shall never be underestimated and maritime stakeholder must invest on it, no system can be 100% secure and no maritime stakeholder can consider itself safe.

Big or small, public, or private, national, or international companies are at danger, as we saw in the case of NotPetya attack and its disastrous effects on A.P. Moller Maersk.

V. Conclusion

The maritime transport sector grew exponentially from 1980 resulting in the most used mean of transport, currently around 90% of international goods are transported by sea[215].

Today the maritime sector is of crucial importance to modern societies, and for the development of welfare of States therefore its maintenance must guaranteed. The disruption of a strategic port or maritime checkpoint could have devastating effects[216]. Among other risks that exists in the maritime framework, cybersecurity is a raising issue that requires immediate attention.

Indeed, the increasing dependency of the maritime sector on software-based technologies brought together with numerous advantages, in term of competitiveness, costs saving, sustainability also new types of threats, namely cyber-threats.

If from one side, it is difficult to understand their impact and potential, from the other it is fundamental to be aware of the risk and be prepared to respond.

Cybersecurity is the collection of tools and policies used to protect the cyber environment from cyber-attacks[217]. It is also the prevention of damage, the protection and restoration of computers, electronic communication systems, wire communication and information, able to ensure their availability, integrity, and confidentiality (from CNSS glossary)[218].

Cybersecurity is an ever-expanded fields that try to keep up with the evolution and sophistication of cyber-attacks. It can be seen as a security barrier that impedes the success of cyber breaches.

In the maritime sector, cybersecurity became fundamental in the last decades when cyber-criminals started targeting this important engine of the supply chain.

[215] "Review of Maritime Transport 2016" UNCTAD, November 2016

[216] "A vulnerability centric system of systems analysis on the Maritime transportation sector most valuable Assets: recommendations for Port Facilities and ships" C. Kapalidis, S. Karamperidis, T. Watson, G. Koligiannis, October 2022

[217] "Series X: Data Networks, Open System, Communications and Security – overview of cybersecurity" Recommendation ITU-T X.1205, 18 April 2008

[218] Committee on National Security System Glossary" CNSSI No. 4009, April 2015

Many attacks to port or ship IT/OT systems happened; among them the South Korean spoofing attack in 2017, the cyber-attack to Barcelona port that paralyzed operation in 2018 or the NotPetya attack in Ukraine.

Currently, there is a broad set of frameworks, guidelines, legislation, and recommendations regarding cybersecurity that serves as a baseline for companies and organisation to create proper cybersecurity strategies.

But focusing on the maritime transport sector, although steps forward have been made, it seems to be slow in addressing cyber breaches[219].

Among the most important documents on maritime cybersecurity, the ENISA good practices and guidelines give a complete picture of the cyber world, introducing definitions and a four-phase cyber risk management approach composed by the identification of threats, the evaluation of risks, the identification of possible security measures and the assessment of cybersecurity maturity. It is a model that all port operators can use to protect their systems.

Then, of significant importance are also the NIS directives that allowed to create a unique European strategy among Member States and enhanced cyber resilience and cooperation.

Moreover, the IMO resolutions provide high-level recommendations for port operators and a framework to support cyber risk management to "support safe and secure shipping"[220].

Among numerous types of cyber breaches, there are some that constitute serious threat for organizations, for example Ransomwares, as we analysed, they can be seen as a form of cyber extortion but in some case their aim is just destruction.

This is the case of NotPetya ransomware, a powerful malware that was aimed at causing damages to Ukraine and its infrastructures but then spread worldwide.

NotPetya caused around $10 billion estimated damages of which $300 million just to A.P. Moller Maersk, the Danish shipping giant[221].

[219] "Cybersecurity in the maritime industry: a literature review" C. Park, W. Shi, W. Zhang, C. Kontovas, C. Chang, 2019

[220] "Guidelines on Maritime Cyber Risk Management" IMO, June 2022, MSC-FAL.1/Circ.3/Rev.2

[221] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History" M. Mcquade, August 2018, Wired

What we can summarize after this tremendous attack is that, for one side what seemed to be an attack against a nation State, turned in a global attack, hitting numerous countries and international companies, and from the other, that everyone can be a potential target.

Thanks to the combination of two powerful tools, EternalBlue and Mimikatz, NotPetya was able to infect machines, encrypt data and spread in the network causing damages in all devices connected to it.

Even if it is impossible to achieve a completely cyber-secure environment because there is no absolute solution against cyber threats[222], this case study demonstrate how important is to have planned an efficient cybersecurity strategy to mitigate cyber threats and vulnerabilities. It is not just a matter of contrast but, as the European Port Strategy (EU-Resolution 2023/2059) as well as the ISPS code or the NIST Framework suggest, it is a matter of prevention.

Prevention means training of personnel and staff; it means awareness and development of skills that allow organisation to create cyber resilience. NIS 2 Directive states that Member States shall "promote and develop education and training on cybersecurity, cybersecurity skills, awareness raising and research"[223].

Applying all those factors allow to achieve a more cyber resilient and secure environment. The precise aim of this study was to raise awareness and create a complete framework of existing documents, legislative text, guidelines to increase awareness and improve cybersecurity understanding.

[222] "Global Challenges in Maritime Security" P. Kapalidis, 2020, chapter 8, Springer Editor

[223] Directive EU 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation 910/2014 and repealing Directive 2016/1148

BIBLIOGRAPHY

Akpan, Bendiab, Shiaeles, Karamperidis, Michaloliakos, February 2022 “Cybersecurity Challenges in the Maritime Sector”

Alcaide, Llave, 2020, “Critical infrastructures cybersecurity and the maritime sector”

Aslam, Serkant Aktug, Ozkan-Okay, Asim Yilmaz, Akin, March 2023 “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions”

Beaman, Barkworth, Akande, Hakak, Khan, December 2021 “Ransomware: Recent advances, analysis, challenges and future research directions”, Science Direct

Baldoni, De Nicola, Prinetto, gennaio 2018 “Il futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici”, Cybersecurity National Lab

Bevilacqua F., 2024, “cybersecurity e informatica forense”, Università Giustino Fortunato.

Bialas, August 2021 “Maritime Cyber Attacks”, Vessel Automation

BIMCO, Chamber of Shipping of America, Digital Containership Association, Intercargo, Intermanager, Intertanko, ICS, IUMI, OCIMF, World Shipping Council, 2021 “The Guidelines on Cyber Security Onboard Ships”

Boyes, Isbell, Luck, 2020, “Cyber Security of Ports and Port Systems”, The Institution of Engineering and Technology

Borys, July 2017 “The day a mysterious cyber-attack crippled Ukraine”, BBC

Brookson, Cadzow, Eckmaier, Eschweiler, Gerber, Guarino, Rannenberg, Shamah, Gorniak, December 2015 “Definition of Cybersecurity – gaps and overlaps in standardisation”, ENISA.

Caban, Brumerčik, Vrabel, Ignaciuk, Misztal, A. Marczuk, 2017 “Safety of Maritime Transport in the Baltic Sea”, MATEC Web of Conferences

Carrazana, December 2018 “The Economics of Cybersecurity and Cyberwarfare: A Case Study”

Cichonski, Millar, Grance, Scarfone, August 2012 “Computer Security Incident Handling Guide”, revision 2, NIST

Clough, 2014, “A World of Difference: the Budapest Convention on cybercrime and the challenges of harmonization”, Monash University Law Review

CNSSI No. 4009, April 2015 “Committee on National Security System (CNSS) Glossary”

Columbia University, January 2022, “NotPetya: A Columbia University Case Study”, School of International and Public Affairs

Corato F., 2024, “Gestione operativa dei sistemi e delle reti informatiche”, Università Giustino Fortunato.

Corradini, D’Alessandro, June 2016, “Sensibilizzazione e Formazione in materia di Cyber Security” AIIC

Council of Europe, November 2001 “Explanatory Report – ETS 185-Cybercrime (Convention)”

Council of the European Union, June 2014, “European Union Maritime Security Strategy”, 11205/14

Craigen, Diakun-Thibault, Purse, October 2014, “Defining Cybersecurity”, Technology Innovation Management Review

Drougkas, November 2019 “ENISA Report on Good Practices for Port Cybersecurity”, ENISA

Drougkas A., Sarri A., P. Kyranoudi P., December 2020 “Cyber Risk Management for Ports – guidelines for cybersecurity in the maritime sector”, ENISA

Drougkas, Sarri, Kyranoudi, December 2020 “Cyber Risk Management for Ports, guidelines for cybersecurity in the maritime sector” ENISA

ENISA, March 2024 “Foresight cybersecurity threats for 2030”

European Parliament and of the Council’s Directive EU 2022/2555 on measures for a high common level of cybersecurity across the Union, amending Regulation 910/2014 and repealing Directive 2016/1148

Federal Trade Commission, NIST, SBA, Homeland Security, (www.ftc.gov) “The NIST Cybersecurity Framework”

Gazzetta Ufficiale, Law n. 90, 28 June 2024, “Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici”, GU n.153 del 02-07-2024

Holmes K., PhD “What is National Security?”, the Heritage Foundation

IACS, April 2020 “Recommendation on Cyber Resilience”, No. 166

IMO, October 1998 “SOLAS: the international convention for the Safety of Life at Sea, 1974”

IMO, June 2022 “Guidelines on Maritime Cyber Risk Management”, MSC-FAL.1/Circ.3/Rev.2

IMO, December 2002 “International Code for the Security of Ships and of Port Facilities” (ISPS code) Annex to SOLAS 1974

IMO, 2003 edition, “International Ship & Port Facility Security Code and SOLAS Amendments 2002”

Institute of Data, 2023 “Confidentiality, Integrity and Availability – CIA in Cyber Security?”

Jensen, Valeriano, Maness, January 2019, “Fancy Bears and sigital trolls: Cyber Strategy with Russian twist”, Journal of Strategic Studies

Khammas, November 2020 “Ransomware Detection using Random Forest technique”, Science Direct

Kapalidis, Karamperidis, Watson, Koligiannis, 2022 “A Vulnerability Centric System of Systems analysis on the Maritime Transportation Sector most valuable Assets: recommendations for Port Facilities and Ships”, Journal of Marine Science and Engineering

Kapalidis, 2020 “Global Challenges in Maritime Security”, chapter 8, Springer Editor

Karamperidis, Kapalidis, Watson, November 2021 “Maritime Cyber Security: A global challenge tackled through distinct regional approaches”, journal of Marine Science and Engineering

Kapalidis, Maple, Bradbury, Farrel, Fisher, 2019 “Cyber Risk Management in satellite Systems”

Krasznay, January 2020 “Case Study: The NotPetya Campaign”, ResearchGate

Konig, Rass, Schauer, 2019, “Cyber-attack impact estimation for a port” Hamburg International Conference of Logistics

Mattioli, Malatras, March 2023 “Identifying Emerging Cyber Security Threats and Challenges for 2030”, ENISA.

Mcquade, August 2018, “The Untold Story of NotPetya, the Most Devastating Cyberattack in History”, Wired

Merico, Cesari, Gregoris, Gambaro, Cordella, Contini, 2021 “Shipping and Air Quality in Italian Port Cities: State-of-the-art Analysis of Available results of estimated impacts”, Atmosphere

NIST, April 2018, “Framework for Improving Critical Infrastructure Cybersecurity”, version 1.1.

OECD, July 2003, “Security in maritime transport: risk factors and economic impact” Maritime Transport Committee

O’Kane, Sezer, Carlin, May 2018 “Evolution of a ransomware”, The Institution of Engineering and Technology

Park, Shi, Zhang, Kontovas, Chang, 2019 “Cybersecurity in the maritime industry: a literature review”

Perwej, Abbas, Pratap Dixit, Akhtar, Jaiswal, 2021, “A Systematic Literature Review on the Cyber Security”, International Journal of Scientific Research and Management

Petrosyan, April 2024, “Number of ransomwares attempts per year 2017-2023”, Statistica.

Petta, January 2021 “The IMO 2021 Cyber Guidelines and the Need to Secure Seaports”, CIMSEC

Rodrigue, 2007 “Transportation and Globalization”

Schmitt, Biller, July 2017 “The NotPetya Cyber Operation as a Case Study of International Law”, Blog of the European Journal of International Law

Schimtz-Berndt, 2023 “Defining the reporting threshold for a cybersecurity incident under the NIS directive and the NIS 2 Directive”, Journal of Cybersecurity

Singer, 2014, “Cybersecurity and Cyberwar: What Everyone Needs to Know”, Oxford University Press.

Stilgherrian, April 2018 “Blaming Russia for NotPetya was coordinated diplomatic action”.

Swinhoe, October 2019, “Rebuilding after NotPetya: How Maersk moved forward”, CSO

Tailor, Patel, 2017, “A comprehensive survey: ransomware attacks prevention, monitoring and damage control” International Journal of Research and Scientific Innovation.

Tandon, Nayyar, January 2019, “A Comprehensive Survey on Ransomware Attack: A Growing Havoc Cyberthreat: Proceedings of ICDMAI 2018” chapter in Advances in intelligent Systems and Computing

Vipiana, 2024, “Introduzione al diritto della sicurezza pubblica” Giappichelli Editore

Yuchong Li, Qinghui Liu in Energy Reports, 2021 “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments”