Cyber risk assessment in commercial shipping

Anastasios Agaoglou

SID: 232754576033

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

Master of Science (MSc) in Cybersecurity

February 2024

Cyber risk assessment in commercial shipping

Anastasios Agaoglou

SID: 232754576033

Supervisor: Dr. Dimitrios Baltatzis

Supervising Committee

Members:

Dr. Nikolaos Serketzis

Dr. Konstantinos Rantos

SCHOOL OF SCIENCE & TECHNOLOGY

A thesis submitted for the degree of

MSc in Cybersecurity

February 2024

Abstract

This study constitutes a comprehensive review of existing literature on the vulnerability of commercial vessels to cyber-attacks, with a particular emphasis on the susceptibility of ship automation systems.

Due to the high dependence on automation systems, the danger of external interference in automated systems, devices and tools of ships is significantly exacerbated. This means that attackers have the opportunity to interfere in an easy way in navigation systems of a vessel, interrupting the ship's external communication or extracting useful and fairly confidential information.

The present study underscored the significance of conducting risk assessments and implementing preventive measures, while also emphasizing the adverse outcomes that can arise from neglecting such risks.

Anastasios Agaoglou

23/08/2023

Table of Contents

Abstract 3

1. Introduction 5

2. Background Work 9

2.1 Assessment of Cyber Security, Safety Administration and Measures for Protection Against Cyber Threats 9

2.1.1 CYBER SAFETY OCCURRENCES AND CYBER RISK MANAGEMENT 9

2.1.2 GUIDELINES FOR CYBER SECURITY AWARENESS 11

2.1.3 IDENTIFY THREATS AND VULNERABILITIES 14

2.1.4 EVALUATION OF RISK EXPOSURE 19

2.2 MEASURES FOR CYBER THREATS *23*

2.3 ADOPTION OF CONTINGENCY PLANS *26*

2.4 EFFECTIVE RESPONSE AND RECOVERY FROM CYBER-SECURITY INCIDENTS *28*

3. Theoretical Perspectives on Maritime Cybersecurity Risks 31

3.1 CYBER RISK MANAGEMENT AND THE SAFETY MANAGEMENT SYSTEM *31*

3.2 ***THEORIES OF BRIDGE HAZARDS*** *33*

3.2.1 HISTORICAL CONTEXT 34

3.2.2 IMPLICATIONS 34

3.3 THE CASE OF CYBER-ATTACKS TARGETING SHIP AUTOMATION SYSTEMS *35*

3.3.1 Description 35

3.3.2 ASSESSMENT 41

4. My Proposed Solutions 48

4.1 Global Navigation Satellite Systems (GNSS) *48*

4.2 Automatic Radar Plotting Aids (ARPA) *50*

4.3 The Electronic Chart Display and Information System (ECDIS) *51*

4.4 Automatic Identification System (AIS) *52*

4.5 Voyage Data Recorder (VDR) *53*

5. Conclusions 54

Appendix 57

References 60

1. Introduction

'Cyber risk' means any danger of contingencies regarding economical damage, business corruption or harm to the reputation of an organization in shipping industry through bipartite failure of its operational systems to the point or by the employees who are utilizing those systems. In a shipping framework, a cyber danger might represent the impairment or inadequacy particularly of an onboard GPS receiver aforehand due to a failure concerning the mechanical equipment, the targeting system or the functional technologies, expanding through to catastrophe scenarios of vessel systems being attacked with the precise outcome of the ship being deactivated or taken over by malicious third parties.

Although these catastrophe scenarios are strongly potential the possibility of such a contingency for most shipping companies is poor due to safety administration. The danger concerning electronic operational equipment faults is in general well identified by experts and crucial machinery will often be required, spares will be carried out and manual functional operation will be extremely possible should the electronic systems fail. What has been less well acknowledged these days is the threat of these systems being subject to arbitrary access or malicious attacks – well known as 'Cyber Vulnerabilities'. Recently, there has been a focus on this field by the shipping industry itself and the increments that should be followed to safeguard shipping companies from arbitrary approaches or malicious attacks. The defences taken to safeguard operational systems are widely known as 'Cyber Security'.

There are three significant discoveries specified by IMO Resolution MSC.428 (98) in compliance with the compatibility compare report between the contexts generated by the "Guidelines on Cyber Security Onboard Ships" and ISO/IEC 27002 which are represent by the below sentences:

1. The two frameworks possess a significant common area and are significantly compatible as researched and observed. Moreover, there are some technological fields of interest where it is indicated the way that they supplement each other in advance to any impairment. Furthermore, the introduction, integration and

comprisement of a sustainable type model between these two is in the interests of the maritime industry.

2. Although the risk administration approach is phenomenally suggested in the shipping industry, the relative maritime statutory context does not demand any accredited evaluation or credential about safety administration by independent bodies on cybersecurity and security incidents as usual. The ongoing compulsory prerequisite is in practise the existence on board ships and ashore on the vessels communication of an "autonomous" Cyber-Security Manual (without assuring for credential or endorsement by any corpus or principle) or for an Integrated Security Management System Manual that encapsulates the envisaged prerequisites for cyber safety on board the vessels.
3. With the acquirement and involvement of ISOIEC 27001 (which is a typical of accredited credential manners and reports) in the best practices of MSC-FAL.1 / Circ.3 it can be reenforced that accredited credential according to ISOIEC 27001 is imminently advised. Therefore, it persists solely on a voluntary basis.

The regulatory framework for shipping and the EU described above along with the emerging standards applied to industries for protection against cyber risks and business continuity, are seen as a "de facto" necessity for shipping companies to implement management systems that comply with international standards such as ISO/IEC 27001: 2013 (Information Security Management Systems) and ISO 22301: 2019 (Business continuity management systems).

Today's era, which is characterized by the development of technological science has brought about digital transformation in numerous industries, including shipping industry. More specifically, the shipping industry has been faced with a number of challenges out of which our focus will be on cyber security. The present thesis aims to provide an in-depth look at this critical aspect, the challenge of automation systems in cyber-attacks. To-day's era as mentioned above has led to a significant reliance on technological means and automated systems in the businesses operating in the shipping industry. Thus, a thorough understanding and imminent mitigation of cyber risks is now an imperative for everyone involved in this field.

In general, studies about the cybersecurity in the maritime field are many and all of them have enormous research interest. So as to proceed to the description and analysis of the cyber-attacks in the shipping sector, we will refer to particular information

systems and technological devices of ships. As a result, the dangers of cyber threats will be quite conspicuous.

The main purpose of this study is the investigation of cyber-attacks on ships and especial-ly on their automation systems, which are more vulnerable to such attacks. Also, effective measures for the protection against these cyber-attacks will be proposed as part of this work. The study of cyberattacks on ship automation devices is particularly interesting and important and this is the reason why it was chosen as a topic in this thesis. Thus, this work is of great importance and aims through a thorough literature review to contribute to providing answers to critical research questions and to better understanding the issues that need attention and are related to cyber threats in the field of shipping and ship systems.

Due to the huge evolution of technology and the maritime industry's great dependence on technology and automated systems, the vulnerability of these systems to cyber-attacks and cyber threats is a vital issue, which requires further study to be undertaken within the framework of this work. These attacks are important to a greater extent, as they have significant negative, even catastrophic effects, on the operation of the ship's systems, on its communication, but can also lead to more dangerous situations, such as a collision.

The basic research questions that we will attempt to answer in this thesis are the following:

1. What degree of danger have the cyber-attacks on ships' automation systems?
2. Is cybersecurity in the maritime sector at a low level?
3. To what extent are the measures taken to protect against attacks effective?

Every study and research effort must explicitly and comprehensively state the importance of its conduct. For this reason, the importance of the present study is found in the use of its findings which can greatly affect maritime safety and upcoming operations. As soon as we are talking about the shipping industry, i.e., a critical industry that contributes globally with its activity in trade, the need to ensure cyber security is absolutely imperative and necessary. Either from the point of view of operational efficiency or international safety and environmental protection.

Particularly, in order to achieve the objectives of this thesis, the following structure will be followed:

- In the first chapter there is an introductory approach, which refers to the subject of the work, its main objectives and the importance of studying the issue of cyber incidents in the shipping sector.
- In the second chapter, a thorough literature review and a detailed report about the background work, which is related with the cyber-threats in the shipping industry, as well as the significant preventive and protective measures to safeguard the ship's automation systems are attempted.
- In the third chapter, we based on the theory and the main approach about the most important practices of Cyber-security Framework in order to outline the most significant phases for the effective management of cyber-attacks on ship’s devices.
- In the fourth chapter, we tried to express our point of view and add our own contribution to this work in the best possible way regarding the most important cyber-attacks on ship’s automation systems, which are crucial for its effective operation and for the reason that such systems are more vulnerable to these dangers, given that their functionality depends on the use of technology and on computer networks. Of course, this was done with the help of bibliographic review and after the study of various cases of cyber-attacks.
- In the fifth chapter, the main results follow regarding the importance and the negative effects of cyber-threats on ships and their operational devices.

2. Background Work

2.1 Assessment of Cyber Security, Safety Administration and Measures for Protection Against Cyber Threats

2.1.1 CYBER SAFETY OCCURRENCES AND CYBER RISK MANAGEMENT

Cyber security and cyber safety administration are both of major significance because of their potential effect on private staff, the owner, the ship, the company and cargo and mainly the environment. Cyber security is concerned with the protection of IT, OT, information and data from arbitrary access, handling operation and manipulation and mainly disruption disturbance and impairment of many kinds. Cyber safety administration encompasses the risks from the detriment of availability or rectitude of safety critical data and OT (Mannadiar, 2020).

Many cyber safety occurrences can emerge as the result of:

- A cyber safety contingency, which has an effect on the availability and rectitude of OT, for example the destruction of chart data which is spanned in an Electronic Chart Display and Information System (ECDIS).
- A failure arising during software sustenance and repairing.
- Damage of or malign operation of external sensor or probe data, crucial for the operation of a ship – this comprises but is not entirely restricted to Global Navigation Satellite Systems (GNSS).

As long as the reasons and roots of a cyber safety occurrence might be separately distinct from a cyber security one, the substantial reply to both is based upon educating, training and mindful awareness.

Cyber risk management should:

- Specify the competence, roles and liabilities of users, key staff, and management whilst both ashore and on board.

- Specify the systems, merits, components, information data and abilities, which if and when corrupted, could incapacitate risks to the ship's operations, general structural functions and safety.
- Deploy technical and structural moderations to protect against a cyber occurrence and secure cohesion of operations.
- Implement aims and activities to initialize for and respond to cyber occurrences.

Some facets of cyber risk management though may preclude commercially sensitive or strictly confidential information data. Ship owners, ship managers and companies should, therefore, examine and act by protecting this information data in the proper way, and as far as possible, not include confidential data in their Safety Management System (SMS).

Deployment, appliance, implementation, preservation and upkeep of a cyber security management program in compliance with the approximate in figure 1 is a major undertaking for the operation firm. It is, therefore, significant that all presbyter administration remains ventured throughout the procedure to secure and ensure that the safeguard, probability of emergency and responding plans reassure the equilibrium in relation to the menaces, dangers, vulnerabilities, risk exposure and consistencies of a prospective cyber incident (The Guidelines on Cyber Security Onboard Ships, 2022).

So, from all the above we can fully understand that cyber risk in maritime field is directly related to threats to the ship's systems, which may lead to loss or alteration of useful data. Cyber risk management which we have studied in this subsection refers to the procedure of identification, analysis and evaluation of a cyber-related risk. The main purpose however is to support safe conditions in the shipping sector, which will involve a high degree of durability to serious cyber risks (https://www.imo.org/).

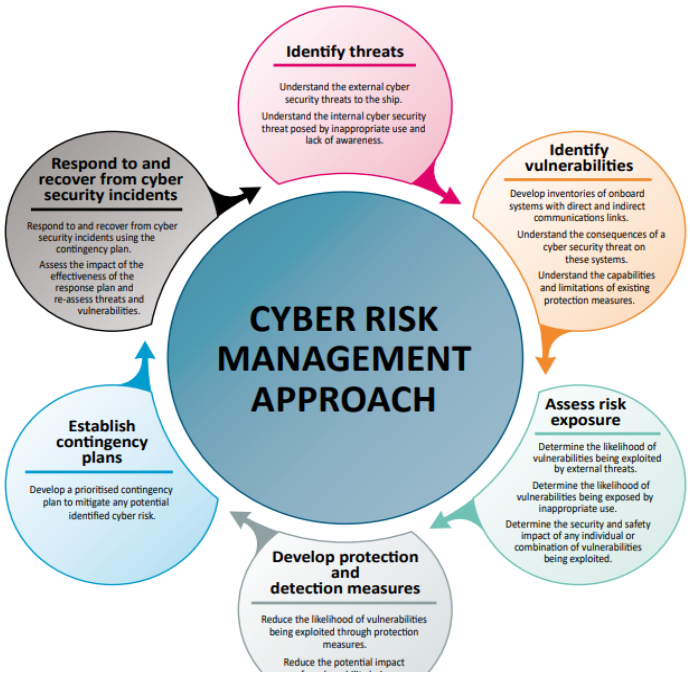


Figure1. Cyber risk management approach as set out in the guidelines

2.1.2 GUIDELINES FOR CYBER SECURITY AWARENESS

In so much the obvious and same way as contingency and emergency plans are already in place for the vessels, plans will have to be deployed in taking into account various scenarios. The accurately important guidelines have specified a list of some of the critical elements related to ships, some of them are the following:

- Knowing what to do in the case of disabling, malign handling or manipulation, of all types of electronic navigational equipment and technologies;
- Cognition of how to handle the case of disabling, or manipulation, of industrial control systems for propelling, adjuvant and auxiliary systems and some other crucial systems;
- Total awareness of how to verify that information data is integer in cases where intrusion is suspected but not yet confirmed;
- Processes for handling ransomware occurrences;
- Operational emergencies for ships in cases where land-based information data is lost when onboard.

IMO Resolution MSC.428(98) identifies cyber risks as specific menaces or cyber dangerous activities which companies should try to directorate as much as possible in the same manner as any other common risk that may affect deteriorating the

safe operation of a vessel and most of all protection of the marine environment. Additionally, there can be more guidance on how to incorporate and integrate cyber risk management and can be found into the company's SMS.

The aim and purpose of the SMS is to supply safety on the working environment by introducing proper practices and processes based on an evaluation of all specified risks to the ship, onboard and offboard key personnel and staff but also the marine environment. The SMS must comprise directives, guidelines and procedures to assure the secured function of the ship and protection of the marine environment in accordance with related international and flag state prerequisites. These processes and guidelines should examine threats, dangers and risks emerging from the use of IT and OT on board, taking into consideration prevailing passwords, guidelines and proposed patterns.

When encapsulating cyber risk management security issues into the company's SMS, attention must be exponentially acquired as to whether, in addition to a generic risk assessment of the ships it operates, a particular ship needs a particular threat evaluation. The company should examine the need for a particular threat evaluation based on whether a specific ship is unique within their fleet. The factors to be examined involve but are not constrained to the degree to which IT and OT are used on board, the complexity of system incorporation and the nature of all functions (The Guidelines on Cyber Security Onboard Ships, 2022).

Accordingly, cyber risk security management must be an intrinsic and innate part of the safety and security culture auspicious to the safe profitable and effective function of the ship and be regarded and perceived at several plans of the company, concerning senior management ashore and onboard key personnel and general staff. In the general structural framework of a ship's operation, cyber occurrences are foreseen to lead in corporal effects and dynamic safety or pollution incidents. This thoroughly means that the company needs to reassess risks and dangers flowing from the use of IT and OT onboard and offboard ships and mainly enact proper assurances against cyber contingencies. Company patterns and special crucial processes for cyber risk security management must be integrated into already existing security and safety risk management prerequisites included in the ISM Code and ISPS Code.

In accordance with chapter 8 of the ISPS Code, the ship is obligated to carry out a security evaluation, which comprises identification and assessment of key shipboard operations and the correlated dynetic threats. As recommended by Part B, paragraph 8.3.5 of the ISPS Code, the assessment must refer to radio and telecommunication

systems, including computer systems and networks. Therefore, the ship's security plan may need to comprise proper moderations for protecting both the technological equipment and the connection. Due to the rapid uptake of intricate, evolved and digitalised onboard OT systems, attention and caution must be given to involving these processes by reference to the SMS in order to help secure the ship's safety procedures are as up-to-date as possible. Systems like Tanker Management and Self-Assessment (TMSA) demand contingency plans to be integrated.

Finally, cyber security awareness is crucial for the proper operation of a ship's systems, which ensure the general safety on board. Cyber security strategies include many kinds of risks, such as information integrity, as well as system availability. A lot of incidents may be as a consequence of the below:

- Problems with the delivery of information from the shipping business to the vessel.
- Problems with onboard systems, which entail negative results on the overall operation of the ship.
- Interception of sensor and confidential information by hackers, which is important for the effective operation of a vessel (The importance of cybersecurity in the maritime industry (marine-digital.com).

Figure 2. Cyber security awareness.

2.1.3 IDENTIFY THREATS AND VULNERABILITIES

The guidelines generally will have to specify four groups, who may cause a substantial threat to arise. They are the activists (including disaffected employees), criminals, opportunists (who usually are interested for the challenge of breaking in) and states or terrorists. Each and every one of them has different motives, targets and objectives. The following table could describe some potential incentives and objectives. The usual procedure is that every company will have to take into account the danger that flows from these different groups.

Group	Motivation	Objective
Activists (including disgruntled employees)	■ reputational damage ■ disruption of operations	■ destruction of data ■ publication of sensitive data ■ media attention ■ denial of access to the service or system targeted
Criminals	■ financial gain ■ commercial espionage ■ industrial espionage	■ selling stolen data ■ ransoming stolen data ■ ransoming system operability ■ arranging fraudulent transportation of cargo ■ gathering intelligence for more sophisticated crime, exact cargo location, ship transportation and handling plans etc
Opportunists	■ the challenge	■ getting through cyber security defences ■ financial gain
States **State sponsored organisations** **Terrorists**	■ political gain ■ espionage	■ gaining knowledge ■ disruption to economies and critical national infrastructure

Table 2: Motivation and objectives

The cyber risk certain times is specific to the company, shipowner, ship manager, operation or trade. When the company evaluate the particular danger, it should examine and deal with any facet of their operations and functions that is looming to

augment their vulnerability to cyber incidents and contingencies. In contradiction with other fields of safety management and assessment of security risks, where historic demonstration is widely disposed, cyber risk management and security is made more challenging when any conclusive information data lapses both about these specific occurrences and their repercussions. In the meantime, and until this substantial proof is acquired, the scale and prevalence of these attacks will be resumed as to be unknown. Any wide known experiences and records in any kind of industry such as mass media, financial establishments, public transport including the shipping one, have shown in the past that every successful cyber-attack might cause a significant loss of their services and in a very short time period. Assets and merits in their own way of fashion can also compromise safety rules and security in general. There are certain incentives both for individuals or companies/organisations that flow from lack of the essential services that can actually within a moment withdraw assets or data information and cause trouble or even harness cyber vulnerabilities within the company.

Furthermore, there is always the likelihood that company key personnel, both on board and ashore, could undermine in order to sabotage cyber systems and data information. In general, the company should entertain the notion that this may be caused by a human factor that concludes to an unintentional error when managing IT and OT systems or maybe scarcity to the system when failing to follow the necessary technical and procedural protection moderations. There is, however, the possibility that these particular actions may be malicious and are an intentional endeavour by a disaffected employee to harm the company and the ship (North, Cyber Risks in Shipping, 2022).

Overall, there are two types of cyber-attacks, which might have an impact on companies and ships:

- Untargeted attacks, where a company or a ship's systems and information data are one of many possible objectives.
- Targeted attacks, where a company or a ship's systems and information data are the anticipated objective.

Untargeted attacks usually use gears, instruments such as machinery equipment and techniques available on the internet, which formally are used to locate, explore and harness widespread vulnerabilities that may also exist in a company and onboard a ship

but also ashore as well. Examples of some tools and techniques that may be used in these particular circumstances involve**:**

- **Zero-day-Exploit**: attack when a weakness is discovered in the software, before the problem is fixed.
- **Phishing (electronic fishing):** way of deception the users with the aim of making them disclose personal information or financial information through a misleading email, SMS message, phone call or a misleading web site.
- **Attack man-in the middle**: in communication networks the attacker interferes with a communication between two parties who have relationships of trust between them.
- **Service denial attacks**: attacks against a computer, or a service provided, which are intended to render the computer or service incapable of accepting other connections and serving other potential customers.
- **Attack with addendum malicious SQL code**: a malicious attacker runs SQL commands against a target server and then extracts sensitive information (such as access codes, usernames, emails, credit card numbers, etc.)
- **Malware**: Malicious software which is designed to access and damage a computer in order of a failure without the cognition of the owner.
- **Water holing**: Enact a fake website establishment or harnessing a genuine website institution to avail visitors.
- **Scanning**: Raiding large sections of the internet randomly.
- **Social engineering**: Sometimes, a possible cyber attacker exploits by manipulating an inside individual into breaking security codes or by ignoring safety procedures for the company, usually through communication via social media in order to capitalize the company, formally labelled as a non-typically technical technique.
- **Brute force**: This is an attack where the hacker tries as many passwords as possible with the hope that eventually he will guess the right one. In this technique the attacker systematically tests and verifies all possible passwords until the correct one is found.

Obviously, before any prior management it is essential that every shipping company would perform under any circumstances an initial evaluation of any potential threats, menaces or vulnerabilities that may come across. This notion should immediately be followed by an accurate evaluation of the systems of the ship and various onboard and ashore processes to secure the soundness of these systems and to the fact that they can handle all along with the responsible key personnel the upper level of an undergoing threat or menace. This comes to a reassuring level with the responsible cooperation of internal and external technicians or experts of the subject with excelled cognition of maritime industry and mainly security and of course its fundamental procedures. Afterwards, there comes a complete strategy which its main purpose is to centre around the wrenching risks and dangers (Kennard, n.d.).

Systems that are of standing alone quality would be absolutely better concerning the vulnerability to any external or internal cyber-attacks if and only are to be compared to those who function only under uncontrolled systems and networks or instantly via internet. Extra focus and care must be given to comprehend how crucial shipboard systems should comply to uncontrolled networks. When this is done, the human factor must be taken into account so as to understand that many occurrences and contingencies are to be enabled by the key personnel's motives and actions. Onboard systems could involve:

- **Cargo management systems**: They include digital systems mainly used for the uploading and consignment of ships, the security management and control of cargo and including hazardous freight that mainly sometimes can interconnect with a range of diversity systems ashore, consisting of ports, marine terminals and basic marine facilities. These systems are the ones which involve shipment tracking average instruments and equipment disposed to the shippers via internet. However, in most of the cases, this tracking is usually connected via the company's systems which communicate to the ship and not directly between the shipper and the ship. Interconnection of this type usually make cargo management systems and data information in freight uploading lists vulnerable to cyber-attacks.
- **Passenger servicing and management systems**: These are digital systems that are able to hold passenger's information data used for property management occupation, boarding information and access control. Usually, they dispose

intelligent devices (tablets, handheld scanners etc.) which their main purpose is to ultimately transpass the collected data on to other systems and informatorries.

- **Passenger facing public networks**: These are mainly wireless networks which are connected directly to the internet, installed most of the times on board for the advantage of passengers, for example guest entertainment systems. These systems should retain their label as uncontrolled systems and should not be associated or attached to any crucial safety system on the ship.
- **Bridge systems**: Bridge systems tend to be absorbed from network navigation systems offboard designed to interconnect from emergency updates or suppliance of services, thus making them extremely vulnerable to cyber-attacks. These digital navigation systems that are not usually connected to other external networks may be equally fragile and susceptible to damage, as removable media are often used for the update of such systems from other either controlled or uncontrolled networks. A cyber-attack incident or a malign occurrence most of the times can expand to service denial, mistreatment or manipulation and, therefore, may influence all systems correlated with navigation, including ECDIS, GNSS, AIS, VDR and Radar/ARPA.
- **Administrative and crew welfare systems**: These onboard computer networks are specifically vulnerable to the extent they are mainly utilised for the governance of the ship and the welfare of the mechanic crew. This phenomenon can be easily availed by cyber attackers to gain access to onboard systems and information data. These systems should be worn off as uncontrolled and should not be connected to any crucial security system on board.
- **Communication systems**: Communication systems provide internet connectivity via satellite and/or availability of any other wireless communication that usually can augment the vulnerability of ships. The main cyber defence mechanisms applied by the service trader should be carefully taken into account but should not be exclusively or entirely underpinned upon to guarantee every onboard system and information data. Communications transformatives, occupations and links to public authorities for propagation of necessary ship reference information are included in these systems. Obviously, all along with these systems comes the complete and accurate compliance with access control security management obligations and prevailing authentication.

- **Propulsion and machinery management and power control systems**: The use of digital systems to follow up, track and test auditing monitoring and onboard technical machinery, propelling and coordinating steering is the fact that enhances such systems to be vulnerable to cyber-attacks. The vulnerability of these systems can rise when they are used in combination with remote condition-based auditing and/or are incorporated with navigation and communications technical equipment on ships using encapsulated bridge systems.
- **Access control systems**: Another combination of digital systems that are vulnerable to cyber-attacks are the access control systems that are used to support access control to secure physical security of the staff and safety management of a ship and its cargo, including surveillance, supervision systems, shipboard security alarms, and electronic "personnel-on-board" systems (The Guidelines on Cyber Security Onboard Ships, 2022).

Therefore, cyber threats and vulnerabilities are many in the field of shipping, endangering the safety of the ship and its systems. Certain frequent disadvantages and weaknesses in the systems of different types of ships are the following:

- Obsolete and outdated devices on ships that cannot be upgraded.
- Anti-malware software which cannot offer full protection against modern cyber-threats.
- Lack of effective security protocols (Ship Cybersecurity | Maritime Industry Cybersecurity (mitags.org).

2.1.4 EVALUATION OF RISK EXPOSURE

When the key members and specialists of a company are assessing the risks, it is significant that they take into considerable account the dangers and threats that might be posed to the company itself from cyber security moderations and how exactly these moderations are going to influence the business practises and the inner relationship with the clients. It is suggested that the National Institute of Standards and Technology (NIST) Cyber Security Framework can draw a major role in deploying and compiling the approach to cyber security. The phases NIST outline are Identify, Protect, Detect, Respond, Recover. An initial risk exposure assessment may be considered as a charting activity that should involve:

• Which of the IT systems and operational navigation business technology systems are vulnerable and the reason that they are vulnerable, including human delegations.

• Which schemes are positioned in order to secure the business systems and how exactly these encompass the threats and vulnerabilities.

• What controls and key shipboard operations are vulnerable and the way they are in order to meet the follow up instructions to resolve them

• The specification of potential cyber contingencies, the chances that they have in appearing and causing malign effects in the business and the repercussions that they might have on shipboard operations and functions in general. Mainly, it sounds like a plan for every company to carry out this practise, but most of the times those companies with lower pores must count upon third parties to help and assist them. The earlier a third party is identified, the merrier results it carries out for the company's business plan and security operational system. In that way, a company would have both IT security expertise and experienced navigation systems. When the risk exposure assessment ends a report should be filed, one that specifies all the threats, menaces, risks, vulnerabilities regarding their likelihood and effect. Rectifying measures should be recommended that will decrease the risk and threats opposed to the company (North, Cyber Risks in Shipping, 2022).

Generally, there is a pile of questions that should be posed such as the following that can be used as a foundation for a risk exposure assessment, when aiming to specific cyber threats and vulnerabilities onboard ships:

- What merits are in danger?
- What is the possible effect of a cyber contingency?
- Who undertakes the ultimate jurisdiction for the cyber risk security management?
- Are the OT systems and their functioning surroundings secured from the internet?
- Is there remote approach to the OT systems, and if so, how is it tracked and secured?
- In the same manner, are the IT systems secured and is remote approach of these systems rightly tracked protected and managed?

- What cyber threat or vulnerability security management best tactics are being used?
- What is the training degree of the key personnel managing the IT and OT systems?

The company based on the answers given should send representatives as an authoritative principle and distribute the financial required the budget to execute a full risk exposure assessment and deploy furthermore workarounds that are best fitted for the company and the function of their ships. The later should be appealed as:

- Specify precarious systems that are significant to operational function, safety and environmental security.
- Delegate the persons accountable for regulating cyber policies terms and conditions, outsource processes and enforce tracking and monitoring.
- Identify the necessities for the training of key personnel and staff. The guidelines on risk exposure assessment concerning the security management and safety onboard ships will illustrate the occasion when the company's operation, functioning and trade is in need and the information data retained and guarded. The maritime industry holds a scope of features and attributes, which influence its vulnerability concerning cyber occurrences:
- The cyber controls already applied and integrated by the delegation of the company onboard in its ships.
- The interested partied and stakeholders of the company usually are involved within the procedures of operations onboard and chartering of a ship will presumably lead in scarcity of accountability for the IT foundation and infrastructure.
- When the ship is online it influences how it interconnects with other parties of the united global supply chain.
- The technical equipment most of the times is being remotely accessed by the producers.
- The business-crucial, data information susceptible and commercially sensitive data information shared with ashore-based service traders, including marine terminals and ports and also to communal principles.

- The availability and usage of controlled and uncontrolled crucial systems for the ship's security and safety and for environmental safeguarding.

These evidences should be fairly examined and the rest associated parties integrated into the company's cyber security policies, safety management systems and ship safety patterns. All the users of these specific guidelines should indicate international, national and flag state rules, industry policies and shipping practises and regulations when deploying and incorporating cyber risk management processes. Concerning the IT and OT systems, software and preservation upkeeping can be delegated to third-party department traders as the company, itself, may not occupy a specific procedure of verifying the extent of safety measures and moderations, provided by them. Some of the companies globally tend to use different kind of traders worldwide accountable for software and cyber security and safety controls. The rising usage of big data information as well as the smart ships will ultimately augment the amount of information available for manipulation to cyber criminals and the potential risk of intruding by any kinds of cyber attackers. This makes essential the necessity for sturdy and potent approaches to cyber threat management which are significant both now and, in the future, (Axio, what is a Cyber Risk Assessment? 2022).

The confidentiality, integrity and availability (CIA) model confers in its premises a context for evaluating the impacting effect of:

- Clandestine access to and revelation of data information or data about the ship, mechanic crew, key personnel, freight and passengers.
- Detriment of rectitude, which would possibly lead to misused or destructed data information and data, which are essentially related to the effective and secure functional operation of the ship.
- Harm or damage of availability given the corruption of the information and data and/or the impairment of operational services of the major ship systems.

The associated significance of confidentiality, integrity and availability regulations are dependent most of the times on the usage of the information data. Vice versa, evaluating the susceptibility of OT systems onboard and ashore ships, especially crucial security systems, may emphasize on availability and/or integrity rather than confidentiality. Possible effects or influences may have impact on security-related, conformity related functional, economic and budgetary and environmental-related regulations. In the same manner, various evaluation procedures and methodologies

provide technical criteria that can assist determine the potential size or magnitude of the effect from a cyber-attack.

This means that marine companies must follow a risk exposure plan in order to identify and confront incidents of cyber-attack on its ships and evaluate the adverse consequences on the operation and safety of a vessel's automation and navigation systems (Ship Cybersecurity | Maritime Industry Cybersecurity (mitags.org).

Potential impact	Definition	In practice
Low	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on company and ship, organisational assets, or individuals	A limited adverse effect means that a security breach might: (i) cause a degradation in ship operation to an extent and duration that the organisation is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organisational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Moderate	The loss of confidentiality, integrity, or availability could be expected to have a substantial adverse effect on company and ship, assets or individuals	A substantial adverse effect means that a security breach might: (i) cause a significant degradation in ship operation to an extent and duration that the organisation is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organisational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
High	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on company and ship operations, assets, environment or individuals.	A severe or catastrophic adverse effect means that a security breach might: (i) cause a severe degradation in or loss of ship operation to an extent and duration that the organisation is not able to perform one or more of its primary functions; (ii) result in major damage to environment and/or organisational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

Table 3: Potential impact levels when using the CIA model

2.2 MEASURES FOR CYBER THREATS

The procedure that should be followed to decrease the dangers and cyber threats must be distinct to each company separately. Generally, there are two types of responsive reactions to encounter the situation; technical responses, those that respond directly and cope with technical equipment and operational systems; and processional responses, which are mainly emphasizing on how the systems are working and on the interconnection of them with the human factor. The technical responses are usually the ones that can afford outplay of each situation quickly. On the contrary, procedural responses take more time, because they surface the need to alter already existing practises and operations that usually include awareness training by their parts. The development of protection and detection measures and moderation is an integral part of the procedure, since most of the times it is looming that without them, vessel systems will be vulnerable to cyber risks in the immediate future, if and only they are not used correctly. For this particular purpose it seems inevitable that the guidelines suggest that emergency plans are able to tackle with the several threats.

It is of major significance how to specify and how to tide over with the administration of cyber security and safety on board and ashore and how to convey liabilities to the master of the ship, accountable officers and when necessary to the company security officer. The connected OT systems on board must demand plenty of technical and procedural protection measures. Usually, they are used circumference

defencing systems or advocacies, an example of which are the firewalls in order to impede unauthorised entrance into the systems, but most of the times this does not look adequate to tackle with the deterrence of insider attacks. This system of defense thoroughly stimulates a conjunction of:

- natural and physical safety of the ship in compliance with the ship security plan (SSP).
- safeguard of networks, involving efficient partition.
- invasion identification.
- recurring vulnerability detection, tracking and testing.
- software whitelisting.
- approach in accordance and user audits and inspection.
- proper processes concerning the usage of detachable media and password techniques.
- key personnel's outreach of the danger and intimacy with proper processes.

When deploying incorporation between systems, a custodian threshold model should be assumed, according to which systems are bundled into those between which confidence is implied and tacit and those between which confidence should be explicit. For the generally major and complex systems, this model should be utilised as a procedure to comprehend all the technical approaches and where they should be incorporated and applied between systems in order to enhance the support for defensive moderations in extent (JAPAN P& I CLUB, Cyber risk and Cyber security countermeasures, 2022).

Nevertheless, concerning onboard ships where the standards of incorporation between IT and OT systems may be upper levelized, profound defensive strategies only operate if technical and procedural safety moderations are implemented in levels across all vulnerable and already incorporated systems. This is "defence in breadth" and it is utilised to hinder any threats or vulnerabilities in one system that is being used to undermine safety moderations of another system.

Cyber threats or vulnerabilities security measures may comprise in nature either technical or processional moderations, with technical controls incorporated and implemented to enforce procedural monitoring and control; a combinational approach

on the matter that utilises appropriate measures proper can provide one of the most effective template models of security safeguard.

Cyber threat security moderations are well known as to be technical under any circumstances and clearly cantered on reassuring and confirming that the onboard systems of a ship are drawn and adjusted as to be persistent and refractory to any cyber-attack flowing mostly from cyber criminals.

Safeguard moderations may also be procedural and should be addressed by company policies and regulations, safety operational processes, security procedures and approach monitoring and auditing.

Extra attention should be focused on how to integrate technical monitoring and auditing that comply to practical policies and are efficient concerning the expenditure, specifically on existing ships. Implementation of cyber safety controls must be precedented and heralded, including major attention to those moderations, or conjunctions of moderations, which feature the greatest interest.

The technical and procedural measures are described below.

Technical protection measures are the following:

1. Restriction to and control of network ports, protocols and policies.
2. Physical security and safety.
3. Detection, foreclosure, notifications alarms and alerts.
4. Satellite and radio interaction.
5. Modulation of network apparatus, such as firewalls and routers.
6. Malware identification and locating.
7. Wireless access control.
8. Email and web browser safeguard.
9. Safe modulation for hardware and software.
10. Data information restoration capacity.

Procedural protection measures are the following:

1. Access for visitors.
2. Upgrades and software preservation and upkeeping.
3. Remote access.
4. Training and educational outreach.
5. Anti-virus and anti-malware instrument updates.

6. Use of manager prerogatives.
7. Equipment allocation, involving information data corruption (The Guidelines on Cyber Security Onboard Ships, 2022).

Undoubtedly, the most important measures against the cyber-threats in ship's systems are the antivirus protection, the training about the cyber-security awareness and the direct response and confrontation of these risks.

2.3 ADOPTION OF CONTINGENCY PLANS

When deploying contingency plans for realization and application onboard ships, it is of major significance to comprehend the importance of all the main cyber events onboard and ashore and set in priority every responding activity in accordance.

All the cyber events should be evaluated accordingly to assess the effect that may have on functions, features, merits etc. In most of these situations there comes a major case and with the exception of upload programming and administrative systems, a damage of IT systems on board, involving a data violation of insider data, will be a business consistency matter upon the business's operation and should not have any effect on the safety operational management of the ship. In the event of a cyber occurrence or contingency influencing IT systems only, priority should be given to the immediate investigation of the incident and to the construction of a recovery plan (North, Cyber Risks in Shipping, 2022).

The damage of OT systems may also have an instant effect of major importance which will influence the ongoing secure operation of the ship. Should a cyber event lead to the damage or malfunction of OT systems, it will be certainly necessary that efficient operations and steps are to be taken to secure the direct security of the mechanical crew, ship, freight, key personnel and safeguard of the marine environment. Generally, proper contingency plans which tend to focus on cyber events, involving of course the damage of crucial systems and the necessity to utilize fallback methods of operation, should be directed by the relative operational and contingency processes involved in the security management system.

There exist some processes concerning the ship's safety and security management that already encompass such cyber occurrences of this importance. Nevertheless, some of the cyber incidents may have the malicious effect on these cases and can result to major failure on these systems to close down at the same time. The contingency planning should take such events into account.

Contingency plans shall be deployed in a way that several harming scenarios will be taken into consideration, in much the same way as all the emergency occurrences patterns will be placed upon the ships. These specific guidelines have already specified a directory of some of the crucial components relevant to vessels:

- Knowing the exact emergency moves in any situation of deactivating, malign handling or manipulation concerning most of the types and formulas of electronic navigational and operational technical equipment;
- Keeping the awareness on how to testify that information data is integer in situations where intrusion is suspected but not verified;
- Operational processes for handling ransomware events; and
- Management contingencies for vessels in cases where land-based data information is lost or damaged.

Associations and links between shore and OT systems can be relative to an extensive scope of implementations like performance auditing, preventive preservation and upkeeping as well as remote support in a quite cite of a few. A common trait of these systems is that they are not rigorously necessary for the secure function of the vessel. Moreover, they represent a possible attack medium of relief to these specific systems that are to be required for the vessel's secure operational function. Therefore, it becomes quite relative to evaluate when these connections and associations between shore and OT systems are authorised and mainly under whichever circumstances. Plans and patterns should be introduced identifying when such OT systems should be provisionally segregated from the shore network linkage to secure the vessel's safety and well-functioning operation. Disconnecting will provide help in order to impede the attacker from being able to mishandle security crucial systems or take immediate control of the system. Disconnecting processes could also occur in order to deter malware disseminating between network divisions.

Also, the safety management system is already involving processes for referring accidents, malfunctions or hazardous cases and determine stages of interaction, interconnection and authority for resolution upholding. Where the judgment is proper,

such operational processes should be modified to depict intercommunication and upholding principle in the case of a cyber incident.

Moreover, it is significant to assist reassurance and security when damage or loss of a technical equipment or credible data information caused by a cyber contingency does not render the already existing plans and emergency procedures as well as the operations irrelevant or inefficient. Contingency plans and relative information data should be disposed in a non-electronic format or mould as some formulas of cyber events can discretionally involve the methodical erase of information data and obviously termination of intercommunication linkage (JAPAN P& I CLUB, Cyber risk and Cyber security countermeasures, 2022).

So, there is an imperative need for a contingency plan for the ensuring of security in the systems and devices of a ship from cyber-attacks, with the aim to offer an appropriate and proper response to these dangers and find effective ways to return to their initial operation (Ship Cybersecurity | Maritime Industry Cybersecurity (mitags.org).

2.4 EFFECTIVE RESPONSE AND RECOVERY FROM CYBER-SECURITY INCIDENTS

It is of major significance to comprehend that cyber events around the globe may not fade away or vanish by themselves. If for instance, in a specific situation the ECDIS has been infected with malware, initiating immediately the back-up process for ECDIS may trigger another cyber event. It is, consequently, suggested to allow a draft project in order to execute the cleaning, resetting and resuming of these infiltrated systems.

A trained team, which most of the times involves a conjunction of onboard and ashore key personnel and crew or external experts, must be generated in order to act properly concerning the actions given for restoration of the IT and OT systems and so that accordingly the vessel will finally proceed under regular operational functions. This expert team must be focused on accomplishing and realizing all levels of the backlash reply (JAPAN P& I CLUB, Cyber risk and Cyber security countermeasures, 2022).

An efficient response must at least comprise some of the below steps:

1. Original evaluation. To assist secure a proper and effective reply, the team of experts should figure out:

   • how the event emerged.

   • which IT and/or OT systems were influenced and how exactly.

   • the degree to which the trading, marketing and function information data is interfered with.

   • to what rank any risk, threat or menace to IT and OT still persists.

2. Retrieve systems and recapture information data. When the original evaluation is completed OT and IT systems as well as the information data must be cleaned and retrieved as meticulously as possible in order to achieve a functional mode by subtracting menaces from the systems and recapturing the initial software.

3. Examine the particular event. In order to comprehend fully the root causes, reasons and repercussions of a cyber incident, an examination of the event itself should be engaged by the company, with skilled backup from an external technician, if necessary. After this investigation, the information that is collected will arouse a major impact on hindering a possible repetition.

4. How to impede a repetition. Having already assumed the output of the investigation indicated previously, activities on how to introduce and tackle with any deficiencies or impairments concerning technical and/or procedural security moderations must be taken into account, in compliance with the company processes for integration of reconstructive effect.

In a way to assist the upkeeping of the response capability efficient, it is also of significant importance for the related key personnel to perform tactical cyber safety operations, exercises and activities. Cyber safety activities on the matter can, whenever it is proper, be drawn by actual life events or can be emulated by other events that spiral cascades to become a cyber crisis. This presents with an ongoing occasion to examine and resolve technical cyber safety incidents, but also to secure the rightful introduction of business operational sequence and crisis administration (North, Cyber Risks in Shipping, 2022).

When a cyber incident is intricate and complicated, a mere example of this is when IT and/or OT systems cannot be reformed and reimbursed to regular operational functions, rumour has it that it may be essential to launch the restoration pattern

simultaneously with onboard and ashore contingency plans. When this is the situation that should be dealt with, the team of experts must be capable of delivering counselling to the vessel on:

- whether IT or OT systems must be erased or held running to secure information data.
- whether some specific vessel interactional connections between the vessel and the shore should be wiped out.
- the proper usage of any sophisticated equipment provisioned in pre-installed safety software.
- the degree to which these events have undermined IT or OT systems beyond the competence and capacities of already present recovery patterns.

Contingency and restoration plans must be aligned in antitypes both onboard and ashore. The sole objective of these patterns is to assist the retrieval process of the systems and data information essential to recover IT and OT to a well-disposed and normal operational function. When the main purpose is to assist the reassurance of the security of onboard key personnel and equipment, the operation and pilotage of the vessel should be set as a priority in the original plan. The restoration pattern must be comprehended completely and exclusively by the key personnel accountable for cyber safety and alarm. The thorough analysis and complexity of a restoration pattern will remain credible based on the model of the vessel and the IT, OT systems installed both ashore and onboard.

The team of experts who are responsible for the incident's response must take into major account the prevalence of retrieval activities which might lead to the corruption of any kind of testament that would demonstrate remarkable briefing upon the reasons of an event like that. Whereas probable, the team of professionals occupied with cyber event response enhancement must be focus on the matter in order to secure the upkeeping and maintenance of elementary proof whilst retrieving operational function and capacity.

Restoration of OT systems may be more complicated specifically when there are no support systems countable and may demand relief from ashore. Detailed information of where this aid is disposed and exactly by whom is offering it, must be an integral section of the restoration process, for instance when progressing to a related port to

acquire help from a serving mechanical engineer (The Guidelines on Cyber Security Onboard Ships, 2022).

If trained crew are disposed on board, then comes the possibility of more expanding and far-reaching diagnostic and retrieving activities and effects that may be executed. Diversely, the restoration plan will be restricted in acquiring a relatively rapid approach to technical backup and support.

As a result, effective response to cyber-attacks must involve a plan for the detection of threats and a recovery plan for the restoration of the physiological function of the ship's systems (https://www.ics-shipping.org/).

3. Theoretical Perspectives on Maritime Cybersecurity Risks

3.1 CYBER RISK MANAGEMENT AND THE SAFETY MANAGEMENT SYSTEM

Modern commercial vessels are characterized as "Floating Digital Offices" as they host and interact with complicated, heterogeneous Information Systems and depend on many suppliers (e.g., navigation technological equipment suppliers, cloud service suppliers, telecommunications and interconnections suppliers, etc.). The information systems of commercial ships may be recited to several threats and vulnerabilities in cyberspace and any corruption or malign function of the vessel's crucial systems (e.g., pilotage systems and/or OT systems) that will have a major effect on office-ship interaction or on the smooth pilotage of the vessel or even on the rectitude of the commodities or freight. Cybersecurity is therefore a crucial fold of the smooth operational function of commercial ships and by expansion, the business continuation or sequel of shipping companies.

At the same time, commercial shipping determines a crucial part in the Maritime Environment, interconnecting with many entities such as Shipping Companies, Crew, Ship Builders, Port Authorities, Inspectors / Classification Societies, Cargo Owners, and any deterioration, corruption or failure of their Information Systems will have decisive aftermath on the appropriate operational function of the vessel and the activities and pursuits of the interconnecting entities, making safety administration one of the most significant matters onboard and ashore. In order to ameliorate security and prevent such occurrences, there are numerous guidelines, instructions and best practices

to be assumed and pursued, such as the IMO: MCS-FAL.1-Circ.3 "Guidelines on Maritime Cyber Risk Management", "OCIMF: Tanker Management Self-Assessment v3" and "BIMCO: Guidelines on Cyber Security Onboard Ships v4".

Additionally, a significant part for the safety of vessel information data systems is being enhanced by classification societies, international organizations such as Lloyd's Register, DNV and Bureau Veritas, which have deployed instructions and supply technical aid in order for shipping companies to be still secured and comply with the above moderations, norms and best practices, decreasing the danger of cyber threats. Classification societies designate the technical regulations on the basis of experience and best practices and have the ability to investigate vessels at tactical periods and publish credentials to secure compliance with statutory prerequisites:

1. Additionally, to cyber safety prerequisites, international organisations such as ENISA, UK DfT and IAPH have published extra requirements and best practices concerning port Information Systems, as they constantly interconnect with vessels and their systems are also susceptible to possible cyberattacks (Σπανός, 2021).
2. All the above suggested instructions, guidelines and requirements can be met by well-known international templates and norms such as NIST CSF, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 22301, SOC 2, GDPR, CCPA, etc., and the most efficient pattern in order to adhere with these complex prerequisites is to embrace and endorse a Cybersecurity Compliance Framework to constantly evaluate and ameliorate the plane of safety of Ship and Commercial Ports Information Systems.

Moreover, a proposed compliance methodology consists of the below stages:

Phase1: Definition of a safety group => Appointment of CySO, assignment of security responsibilities to key personnel (e.g. crew, department managers, security engineers).

Phase2: Mapping => Identification of information goods (IT and OT). This may include assets related to the Maritime Environment, etc. (Data, Software, Material), identification of their dependencies, identification of essential operational requirements, identification of critical suppliers.

Phase 3: Conduction of Readiness Assessment => Comparison of ISO 27001& NIST controls with best practices such as IMO, ISM code, TMSA, BIMCO, etc., identification of existing control elements and finding deviations.

Phase 4: Evaluation of critical suppliers => Evaluation of technical control notes (TFA, encryption, creation of technical security copies, remote access, etc.), evaluation of SLAs support services, DPA, compliance with the applicable regulation (e.g. GDPR, CCPA NERC CIP, etc.).

Phase 5: Risk assessment and risk management plan => Carrying out impact assessment, identifying potential threats, assessing vulnerabilities, proposed mitigation measures.

Phase 6: Development of technical and organizational audits => Security policies & procedures, SLAs with critical suppliers, DPA with data processors, cyber security incident plans.

Phase 7: Development of emergency plans => Determination of recovery priority, determination of dependencies, creation of communication lines (internally and with critical suppliers).

Phase 8: Monitoring, control and review => internal inspection, review of technical and organizational audits.

Through the Maritime Cyber Security Compliance Framework, members of the Cybersecurity Team are able to identify all cybersecurity requirements, identify their assets (IT and OT assets), assess targeted threats and vulnerabilities, define targeted cybersecurity audits, include specific measurements (KPIs & Metrics) and evidence in their internal audits and therefore know the level of compliance for each requirement. All these steps are necessary for the better treatment of cyber-threats in the shipping industry.

3.2 THEORIES OF BRIDGE HAZARDS

Bridge risks in cybersecurity refer to vulnerabilities and threats that arise at the intersection or 'bridge' between different network systems, applications, or data sets, (Aslan *et al.*, 2023). These risks emerge when disparate systems connect, interact, or share information, creating potential entry points for cyber threats, (Albakri, Boiten and De Lemos, 2018). These risks can be physical (such as hardware connections), digital (such as software interfaces), or operational (involving processes and people).

The primary concern with bridge risks is that they may allow unauthorized access, data breaches, or the spread of malware across interconnected systems, (Djenna, Harous and Saïdouni, 2021). For instance, a secure network connected to a less secure one can

inherit vulnerabilities from the weaker network, effectively 'bridging' the security gap between them.

3.2.1 HISTORICAL CONTEXT

The concept of bridge risks has evolved significantly with the advancement of technology. Initially, when computer networks were isolated and the internet was in its infancy, bridge risks were limited and mostly internal within organizations. These early risks were more about managing physical access to computer systems and ensuring basic network security. With the advent of the internet and the explosion of digital connectivity, bridge risks took on a new dimension, (Süzen, 2020). The introduction of cloud computing, IoT (Internet of Things), mobile devices, and complex supply chains expanded the cybersecurity landscape, increasing the points of intersection between different systems and networks.

The proliferation of cloud services and third-party integrations in the 2000s further amplified these risks, (Bhuyan *et al.*, 2015). Organizations began to rely on external services and platforms, creating multiple bridges between internal and external systems. This era marked a significant shift in bridge risks, where the focus moved from internal network security to the security of interconnected systems across organizational boundaries, (Bigdeli *et al.*, 2021). The latest phase in the evolution of bridge risks coincides with the rise of sophisticated cyber-attacks, advanced persistent threats (APTs), and state-sponsored hacking. These threats often exploit bridge vulnerabilities to infiltrate high-value targets indirectly. For instance, attackers might compromise a smaller, less secure entity that has a trusted connection to a larger, more secure organization.

3.2.2 IMPLICATIONS

Bridge risks in cybersecurity have significant implications for the foundational principles of information security, commonly known as the CIA Triad: Confidentiality, Integrity, and Availability. These principles are critical for maintaining the trustworthiness and reliability of information systems and data.

Confidentiality:

Information Leakage: Bridge risks can lead to unintended information exposure across interconnected systems. For instance, a breach in a less secure network can provide a pathway to access sensitive data in a more secure network.
Eavesdropping and Interception: Cyber adversaries might exploit bridge vulnerabilities to intercept data in transit between systems, leading to unauthorized access to confidential information.
Third-party Exposure: In an ecosystem where organizations heavily rely on third-party services, a breach in these external systems can compromise the confidentiality of shared data.

Threats to Availability

Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks: Attackers can exploit bridge vulnerabilities to launch DoS or DDoS attacks, overwhelming network resources and rendering them unavailable to legitimate users.
Resource Strain: Even without malicious intent, bridge connections can inadvertently strain resources (like bandwidth or processing power), impacting the availability of critical services.
Cascading Failures: In interconnected systems, a failure in one network due to a security breach can lead to cascading effects, disrupting services across multiple networks.

3.3 THE CASE OF CYBER-ATTACKS TARGETING SHIP AUTOMATION SYSTEMS

3.3.1 Description

The widespread integration of automation and information technology (IT) systems in contemporary vessels presents novel avenues for malevolent actors and hackers to execute diverse cyberattacks, which have the potential to result in catastrophic occurrences and significant safety detriments. The contemporary maritime industry has been the subject of considerable research endeavours by scholars seeking to uncover vulnerabilities, with numerous instances of successful cybercrime having been

documented in recent years (Akpan et al., 2022). The primary driving factors behind such attacks typically involve the acquisition of remote access to ships and vessels, the theft of sensitive and confidential data for the purpose of launching subsequent attacks or the intentional disruption of ship operations through the corruption of critical components and subsequent unavailability of automated systems. The majority of information technology (IT) systems utilized in contemporary vessels are deemed less critical to security and performance, rendering them susceptible to attack and insecure (Akpan et al., 2022).

The Automatic Identification System (AIS) is a widely used technology in the maritime industry for vessel tracking and identification. The AIS transponders lack authentication and integrity verification mechanisms, thereby rendering them vulnerable to exploitation by malicious actors for the dissemination of counterfeit messages. Attackers utilize software-defined radio to generate counterfeit "man-in-the-water" signals, rendering the vessel inconspicuous and disseminating fabricated meteorological updates. Relying on data that may be potentially inaccurate has the potential to result in unfavourable decisions and catastrophic outcomes. The public can access AIS data without charge through online platforms, such as Vessel Finder Limited and Marine Traffic. The International Maritime Organization (IMO) has expressed disapproval towards the divulgence of data pertaining to vessels and their routes, citing the potential utility of such information in the event of a focused assault.

In fact, certain researches, such as CyberKeel (2014a) and Mordechai et al (2014) have brought out some weaknesses in the Automatic Identification System. These vulnerabilities are referred to the modification of the vessel features and characteristics, to the creation of fantastic ships, to the formation of fake notifications and to important changes to the signal transmission. In Wagstaff (2014) it was referred that pirates from Somalia exploited online AIS information in order to detect and lead to manipulation many victims. They used also fake AIS data so as to push these victims to deception or obscure their position.

The Global Positioning System (GPS) is a satellite-based navigation system that provides location and time information anywhere or near the Earth's surface. It was developed by the United States Department of Defense and is now widely used for both civilian and military purposes.

The employment of GPS and navigational technologies in the maritime industry renders them susceptible to targeted cyberattacks, which seek to exploit inherent design

vulnerabilities with the intention of disrupting the services reliant on these technologies (Androjna et al., 2020). The aforementioned attacks present moderate to elevated levels of risk due to the potential for both data and service protocol breaches, as well as the potential for physical harm. Numerous instances of attacks have been reported, which aimed to exploit this particular set of technologies. As an illustration, the utilization of falsified GPS signals facilitated malevolent actors to redirect a watercraft without eliciting a warning or notification from the corresponding system in charge. A comparable occurrence took place in South Korea whereby the reception of GPS signals was disrupted, leading to over 1000 aircraft and 700 ships being affected for a duration of more than one week. The cyberattacks in question can be categorized as having a moderate to high level of complexity and are attributed to the inherent designs and standards of GPS and navigation systems. Satellite Communication Systems (SATCOMs) are prone to numerous vulnerabilities and critical security gaps. These include the use of unsecured or undocumented protocols, factory-set-up accounts, the potential to exploit the password reset function, and backdoors. These security concerns are particularly relevant for vessels that rely on SATCOMs to connect with each other and with the mainland via the Internet (Akpan et al., 2022).

The Global Navigation Satellite System (GNSS) is a space-based navigation system that provides location and time information to users worldwide. The Global Navigation Satellite System (GNSS) is widely recognized as one of the most intricately linked systems. Autonomous vessels that depend on enhanced satellite communications for the transmission of operational commands and sensor data are susceptible to cyberattacks, including but not limited to denial-of-service attacks, package alterations and man-in-the-middle attacks. In addition, the technical drawback of low-power satellite signals is primarily attributed to congestion. Spoofing and jamming are significant vulnerabilities that can potentially result in low-effort attacks with high costs. Furthermore, the reliance of numerous ship systems on satellite positioning renders them susceptible to malfunction in the event of Global Navigation Satellite System (GNSS) failure, thereby resulting in the potential breakdown of other ship systems, such as Automatic Identification System (AIS). It is imperative for autonomous transportation systems to possess the ability to establish communication with operational crews on the ground. Failure to do so may render these systems vulnerable to cyberattacks, which could potentially result in complete control of critical transport operations. This susceptibility to a wider range of attacks and the potential

incentives for intruders further underscores the importance of ensuring robust communication capabilities for autonomous transportation systems (Grant et al, 2014).

The Electronic Chart Display Information System (ECDIS) is a navigational tool that utilizes electronic charts to provide real-time information to mariners (Akpan et al., 2022). Electronic Chart Display and Information Systems constitutes a basic and important ship bridge and this system is connected directly with many other devices. However, ENC updates should be made to this system, on a weekly basis. The process of upgrading this system through Internet is subject to several serious vulnerabilities, providing opportunities for invasion to many attackers. More specifically, many studies, such as CyberKeel (2014b) have revealed that the ECDIS system has many disadvantages and for this reason it is not difficult for an attack to take place, which may even lead to the permanent deletion of ECDIS data. With the modifications of Maritime regulations, ships which have ECDIS systems, can use raster chart display systems instead of ECDIS. However, the last ones offer even less protection to cyber-attacks (ECDIS Info, 2014).

Numerous studies have extensively examined the security concerns associated with Electronic Chart Display and Information Systems (ECDIS). Indeed, there exists an extensive catalogue of deficiencies in the implementations of Electronic Chart Display and Information Systems (ECDIS) software. The system is often operated on outdated computer systems that lack available security updates. The maps can be obtained through online downloads or manual uploads via USB to the system. However, it is important to note that updating the maps in this manner may potentially compromise the system. This particular medium of update has the potential to create a significant vulnerability for potential attacks (Akpan et al., 2022).

Radio Detection and Ranging Radar helps to the detection of physical things with the utilization of radio waves. Nowadays, with quite modern techniques it is possible to observe interference to radar signals. It should, however, be noted at this point that radar signals are more vulnerable to noise-based jamming and to more complex spoofing attacks (Tam and Jones, 2018b). Despite the fact that the endeavor needed for a denial-of-service attack is in general minimal for an intruder, as a vessel has highly developed navigation tools, radar-based attacks can offer a relatively small reward for an attacker (Coffed, 2014).

Navigational Telex was designed with the main objective of providing serious warnings, urgent alerts, about security issues, as well as meteorological forecasts

(Offshore Blue, 2016). NAVTEX is not technologically advanced to a large extent and does not have the multiple capabilities as AIS or ECDIS. This is the reason why many jamming attacks could contribute negatively to the distortion of messages, as happened in Offshore Blue (2016) and Santamarta (2014b). Also, many attacks can lead to vessel delays or even to serious damage and destruction if the ship sent into a dangerous storm. The contemporary maritime industry has also extensively adopted VSAT technology. However, certain facets of the VSAT network, including transparent transmission and openness, necessitate enhancement to mitigate security risks, particularly unauthorized access and interception attacks. In 2014, IOActive conducted an assessment of multiple VSATs sourced from various vendors. The findings of the assessment indicated that the devices were susceptible at the implementation levels due to their utilization of plain text transmission without any authentication, encryption, security, or verification of personal information. Insufficient security measures may allow malevolent actors to transmit counterfeit signals or harmful code to the device, thereby disabling or compromising the system, impeding the vessel's ability to navigate safely (Akpan et al., 2022). Ship location data is typically provided by AIS aggregators. The primary concern lies in the fact that VSAT network interfaces are discoverable on the Internet through means, such as the Shodan Ship Tracker. The disclosure of certain information, such as brand names, product codes, and other data, may have significant implications, as it could potentially be exploited in cyberattacks. Vendors' websites typically provide standard information and numerous terminals persist in utilizing the unaltered factory settings, which encompass the username and server password. If an individual gains access to an open VSAT interface, they can potentially manipulate GPS coordinates and settings, as well as download malicious software. This could result in further network hacking and unauthorized access to critical management systems.

Despite being less vulnerable than satellites, radar signals remain susceptible to cyberattacks, such as interference and DDoS attacks. In the occurrence of a cyber assault, the radar system may generate erroneous data regarding proximate entities owing to spurious reflections induced by extraneous radar signals. Inaccurate information has the potential to result in maritime collisions.

Inaccurate data can lead to a collision between the vessel and an obstacle. It is noteworthy that although radar and other frequencies within the electromagnetic spectrum are vulnerable to interference caused by noise or sophisticated spoofing

attacks, the methods employed to achieve such an effect differ considerably across systems.

Video surveillance systems are electronic devices that are used to monitor and record activities in a particular area. These systems typically consist of cameras, recording devices and software that allow for the capture and storage of video footage. Video surveillance systems are commonly used in a variety of settings, including public spaces, businesses and residential properties. They are often employed as a means of enhancing security, deterring criminal activity and providing evidence in the event of a crime or other incident.

The utilization of Video Surveillance Systems (VSSs) is of paramount importance in ensuring the security and safety of crew, cargo and vessels across various contemporary ship types. The primary function of these systems is to oversee and monitor the crucial operations of the vessel, while also providing safeguards against potential threats posed by terrorists and pirates. Nevertheless, Vulnerability Scanning Systems (VSSs) have been discovered to be susceptible to various cyber threats, leading to the emergence of multiple security concerns (Akpan et al., 2022).

The majority of industrial control systems have been developed and coded without taking into account security considerations, and information is transmitted without encryption. The responsibility of ensuring component security should be jointly shared by vendors, who uphold secure development structures and operators who configure components in compliance with industry standards and optimal practices. Regardless of the situation, the approach frequently presumes culpability on the part of the adversary and fails to implement any countermeasures, thereby leaving numerous vulnerabilities for potential attackers to manipulate. Comprehension of the limitations of the system, along with the vulnerabilities of its components and protocols, is of utmost importance for ensuring the safety of the vessel, and therefore, it is imperative for the designers and operators of ICSs to possess this knowledge. The vessel's decentralized information technology infrastructure facilitates intercommunication among the aforementioned control systems. The establishment of uninterrupted communication between the IT network and the website facilitates remote monitoring, troubleshooting and debugging, thereby reducing expenses incurred in field travel and streamlining the process of data collection and evaluation. A significant issue within the shipping industry pertains to the tendency of operators and engineers to prioritize convenience and efficiency over safety, thus potentially resulting in widespread

ramifications. The aforementioned behaviour is a result of the commercial imperative to optimize time and bypass established security protocols (Akpan et al., 2022).

Various network configurations are employed within the maritime sector to facilitate the transfer of data that has been collected and analysed by interconnected information systems. Several technologies that fall under this category are SHIPNET, SAFENET, C3I system, RICE 10, SHIP system 2000, Smart Ship and TSCE. The existence of security vulnerabilities in these technologies can be attributed to the inadequate consideration given to authentication and encryption methods, during the design and configuration of communication links between IT networks. This has led to the availability of potentially vulnerable and outdated systems on the Internet. Shipboard information technology systems are commonly connected to onshore facilities, which can lead to an elevated susceptibility to persistent and systematic threats. The contemporary shipping industry is confronted with a mounting demand for IT systems and network connectivity due to financial constraints, legal obligations and the need for remote monitoring and management. Nevertheless, the implementation of these systems will inevitably augment the attack surface, thereby necessitating security teams to defend against potential threats. Additionally, the installation of these systems will create supplementary points of access that could potentially be exploited by hackers to gain unauthorized entry into the ship's system. Hence, it is imperative to conduct a meticulous investigation of the susceptibilities present in these automated systems. It is imperative to ensure that critical control networks are segregated from the vessel's IT and Internet networks within a secure location.

Furthermore, the human element poses an even greater challenge within the intricate and interdependent ecosystem of the maritime industry. Consequently, the absence of a culture that prioritizes cybersecurity may prove advantageous to an assailant seeking to infiltrate a vessel and its systems, exfiltrate sensitive information or impede the vessel's operations (Akpan et al., 2022).

3.3.2 ASSESSMENT

The cyber risk is contingent upon the unique characteristics of the company, vessel, operation and/or trade. In the process of risk assessment, it is imperative for companies to take into account any particular facets of their operations that may augment their susceptibility to cyber occurrences.

In contrast to other domains of safety and security, which benefit from the availability of historical data, the management of cyber risk is fraught with difficulties due to the lack of conclusive information regarding incidents and their consequences. The absence of this evidence precludes an accurate determination of the scope and recurrence of the assaults (The Guidelines on Cyber Security Onboard Ships, 2022).

Empirical evidence from the shipping industry and other business sectors, including financial institutions, public administration and air transport, has demonstrated that effective cyber-attacks can lead to substantial service disruptions. Assets may also pose a risk to safety.

The initiation of cyber risk assessment ought to commence at the senior management echelon of an organization, rather than being promptly assigned to the ship security officer or the head of the IT department. There exist multiple reasons for this phenomenon.

The implementation of measures aimed at enhancing cyber security and safety may have an impact on conventional business procedures and operations, resulting in increased time and/or financial costs. Hence, it is a decision that falls under the purview of senior management to assess and determine the appropriate measures for risk mitigation.

Several cyber risk management measures that pertain to business processes, training, ship safety and environmental safety are not directly associated with IT systems. Consequently, these measures should be institutionally embedded outside the IT department (The Guidelines on Cyber Security Onboard Ships, 2022).

The implementation of cyber awareness initiatives has the potential to alter the manner in which a company engages with its customers, suppliers, regulatory bodies and may necessitate the establishment of novel prerequisites for inter-party collaboration. The decision of driving changes in relationships is a matter that pertains to the senior management level and it is their responsibility to determine whether and how to proceed with such changes (The Guidelines on Cyber Security Onboard Ships, 2022).

The subsequent inquiries can serve as a foundation for conducting a risk evaluation concerning cyber hazards encountered on vessels:

- What are the assets that may be vulnerable to cyber threats?
- What could be the potential consequences of a cyber incident?
- What entity bears ultimate accountability for the management of cyber risk?

- Is the working environment of OT systems safeguarded against internet connectivity? Does remote access to the operational technology (OT) systems exist, and if it does, what are the measures in place to monitor and safeguard it?
- Are the information technology systems adequately secured, and is the remote access being effectively monitored and managed?
- Additionally, what are the best practices for managing cyber risks being employed?
- What is the proficiency level of the individuals responsible for operating the Information Technology (IT) and Operational Technology (OT) systems?

The findings suggest that the organization ought to assign responsibility and apportion the necessary funds to conduct a comprehensive risk evaluation and devise optimal remedies that align with the company's objectives and the functioning of their vessels (The Guidelines on Cyber Security Onboard Ships, 2022).

The following actions are recommended for ensuring effective operation, safety and environmental protection of systems:

1. identification of critical systems.
2. assignment of individuals responsible for establishing cyber policies and procedures.
3. implementation of monitoring measures.
4. determination of appropriate use of multiple defence lawyers for secure remote access.
5. disconnection of network protection from the internet.
6. Additionally, it is important to identify personnel training needs.

The degree of cyber risk is contingent upon various factors, including the company's specific circumstances, the ship's operations and trade, the IT and OT systems employed and the information and/or data retained. The maritime sector exhibits various attributes that impact its susceptibility to cyber events.

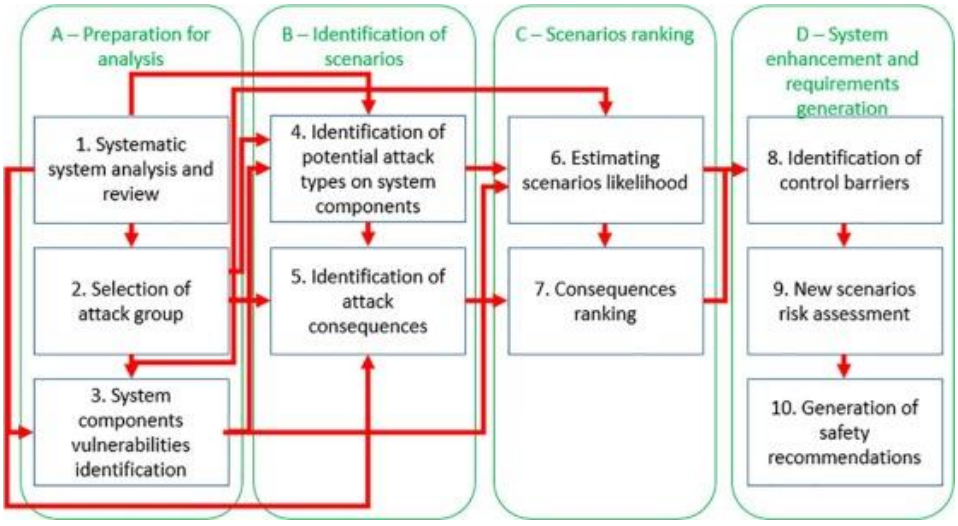
The ship's online presence and its interaction with other parts of the global supply chain are also important considerations. Additionally, ship equipment may be remotely monitored by producers, business-critical, data-sensitive and commercially sensitive information may be shared with shore-based service providers, marine terminals, stevedores and public authorities. Finally, the availability and use of computer-controlled critical systems for the ship's safety and environmental protection are crucial factors to be taken into account.

It is imperative to take into account these elements and integrate pertinent components into the cyber security policies, safety management systems and ship security plans of the company. It is recommended that individuals utilizing these guidelines consult distinct national, international and flag state regulations, as well as pertinent international and industry standards and best practices, in order to construct and execute cyber risk management procedures (The Guidelines on Cyber Security Onboard Ships, 2022).

Third-party service providers can be contracted to handle IT and OT systems, software and maintenance, with the company lacking the means to authenticate the security standards provided by these providers. Certain organizations employ distinct providers who are accountable for conducting software and cybersecurity assessments.

The proliferation of big data, smart ships and the internet of things (IoT) is expected to augment the volume of information accessible to cyber assailants and expand the potential attack perimeter for cyber malefactors. The significance of implementing strong strategies for managing cyber risks is crucial in the present as well as in the forthcoming times (The Guidelines on Cyber Security Onboard Ships, 2022).

The method proposed by Bolbot et al. (V.Bolbot et al. ,2020, 'A novel cyber-risk assessment method for ship systems') portraits in the following table a model way of risk assessment:



Phase 1 Pre-assessment activities.

Before commencing a cyber risk assessment, it is advisable to undertake the following activities:

- ✓ identify and evaluate the ship's essential functions and systems, as well as their potential impact levels, while considering the operation of OT systems. The CIA model may be utilized for this purpose.
- ✓ ascertain the primary manufacturers of crucial IT and OT equipment utilized on board ships.
- ✓ examine comprehensive documentation pertaining to essential operational technology (OT) and information technology (IT) systems, encompassing their network structure, interfaces, and interdependencies.
- ✓ identify the points-of-contact for cyber security within each producer and establish a collaborative working relationship with them.
- ✓ examine comprehensive documentation pertaining to the upkeep and sustenance of the information technology and operational technology systems aboard the vessel.
- ✓ define the contractual stipulations and responsibilities that the shipowner/ship operator may bear in relation to the maintenance and support of shipboard networks and equipment.
- ✓ supplement the risk assessment, as needed, by engaging an external specialist to formulate comprehensive strategies and involve manufacturers and service providers.

Phase 2: the evaluation of the ship.

The objective of evaluating a vessel's network, systems and devices is to detect any potential weaknesses that may jeopardize the confidentiality, integrity, or operational functionality of the equipment, system, network or the vessel itself. The aforementioned vulnerabilities and weaknesses may be classified into any of the subsequent categories:

Technical vulnerabilities, such as software defects or outdated and unpatched systems, and design vulnerabilities, such as access management and unmanaged network interconnections, can pose significant risks to information security. One potential cause of implementation errors is the misconfiguration of firewalls. Additionally, procedural or user errors may also contribute to such errors (The Guidelines on Cyber Security Onboard Ships, 2022).

The assessment process may encompass a range of activities, such as scrutinizing the setup of all computer systems, servers, routers and cybersecurity

mechanisms, which may comprise firewalls. The scope of the assessment may encompass evaluations of all extant cyber security documentation and protocols pertaining to interconnected information technology and operational technology systems and apparatuses.

One crucial element of on-ship evaluation involves the participation of crew members across all hierarchical levels, with a particular emphasis on the involvement of the master, chief engineer, and first mate. This procedure facilitates comprehension of the deployment of IT and OT systems aboard, including potential deviations from the specified design documentation, as well as the extent of cyber education provided to the vessel's personnel.

Phase 3: conducting a debrief and vulnerability review/reporting.

After conducting the assessment, it is necessary to assess each vulnerability that has been identified in terms of its potential impact and the likelihood of it being exploited. It is imperative to identify technical and/or procedural corrective actions for each vulnerability as per recommendations.

Ideally, the cyber risk assessment should encompass:

- The executive summary provides a concise overview of the evaluated vessel's security profile, recommendations and outcomes.
- The technical discoveries encompass an analysis of the identified vulnerabilities, including their likelihood of being exploited, the resultant consequences and the corresponding technical remedies and precautionary measures.

A prioritized list of actions should be developed, with priorities assigned based on factors, such as the measure's effectiveness, cost and applicability. The comprehensiveness of the list of options provided should be prioritized, ensuring that it does not serve as a means for the third-party risk assessor, if relevant, to promote their services and products.

The supplementary data comprises a supplement that encompasses the technical intricacies of all significant discoveries and an exhaustive examination of crucial shortcomings. The present section ought to incorporate exemplar data retrieved during the process of penetration testing, in the event of any, of vulnerabilities that are deemed critical or high-risk.

The appendices consist of documented records pertaining to the activities carried out by the cyber risk assessment team, as well as the tools utilized during the engagement.

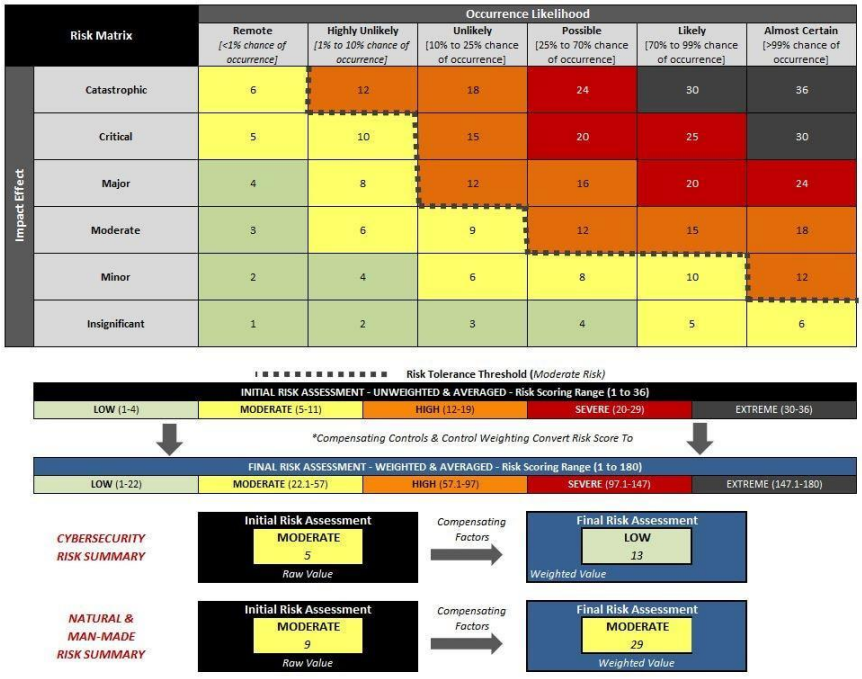
It is advisable to contemplate whether certain segments of the cyber risk evaluation ought to be regarded as confidential.

It is recommended that cyber risk management policies and procedures be incorporated into the safety management system of a company. However, it is important to ensure that such policies and procedures do not contain sensitive information that could potentially compromise the company's security if accessed by external parties (The Guidelines on Cyber Security Onboard Ships, 2022).

Phase 4: conducting a debrief with the producer.

Upon completion of the review, discussion and assessment process by the shipowner, it may become necessary to transmit a portion of the findings to the manufacturers of the impacted systems. Any discoveries that are authorized by the shipowner for dissemination to the producers may be subjected to additional scrutiny with the assistance of external specialists. These experts are expected to collaborate with the producer's cyber security point of contact to ensure a comprehensive comprehension of the issue's risks and technicalities. The purpose of this supplementary undertaking is to guarantee that the remedial course of action formulated by the manufacturer is all-encompassing and accurately identifies the appropriate resolution to eradicate the susceptibilities (The Guidelines on Cyber Security Onboard Ships, 2022).

Also, this table can be used as a measure of the risk (CRA, 2022):



So, an effective model for risk assessment should involve certain important steps, such as the identification of the vulnerabilities of a ship's systems, the consequences of a cyber-attack, the evaluation of negative results and the recommendation of preventive and protective measures.

4. My Proposed Solutions

The ship's bridge is equipped with a comprehensive set of advanced navigation technologies that are crucial for maintaining the safety and effectiveness of maritime operations. The Electronic Chart Display and Information System (ECDIS) serves as a digital navigation tool, offering current electronic charts and assisting in the process of designing routes. GNSS provides very accurate location, which improves navigation and increases situational awareness. The Automatic Identification System (AIS), Voyage Data Recorder (VDR), and Radar/Automatic Radar Plotting Aid (ARPA) collaborate to provide instantaneous data on neighboring boats, capture crucial voyage data, and give a complete radar overview to prevent collisions. These integrated technologies provide seafarers with the required tools for making educated decisions, guaranteeing a safe and secure journey on the wide seas.

4.1 Global Navigation Satellite Systems (GNSS)

Global Navigation Satellite Systems (GNSS) are essential for marine navigation since they provide precise location, timing, and communication services. Although GNSS systems are of great importance, they are susceptible to a range of safety concerns that may have an influence on ship operations. A major issue is the intentional disruption or falsification of GNSS signals, resulting in imprecise location or signal

deprivation. In order to tackle this issue, it is advisable to include sophisticated anti-jamming and anti-spoofing technologies into GNSS receivers. Additionally, it is advised to use numerous GNSS constellations for the purpose of redundancy (SAFETY4SEA 2019).

Vulnerability 1 & Solution

A further obstacle is the probable insufficiency of satellite coverage in some areas, leading to subpar GNSS performance (Engler, Noack, and Beckheinrich, 2008). To address this problem, one may use receivers that support several constellations and frequencies, upgrade the current GNSS constellations, and introduce new ones to enhance both coverage and accuracy.

Vulnerability 2 & Solution

The susceptibility of GNSS systems to cybersecurity attacks is an additional crucial problem. It is essential to deploy strong cybersecurity measures, such as encryption, secure channels, and authentication methods. Regular upgrades and fixes for Global Navigation Satellite System (GNSS) equipment are crucial in order to mitigate any vulnerabilities. Also, issues connected to receiver performance and compatibility might impair navigation (SAFETY4SEA 2019). It is important to use GNSS receivers that have excellent sensitivity and accuracy. Additionally, it is crucial to guarantee that these receivers are compatible with numerous GNSS constellations and signals.

Vulnerability 3 & Solution

The absence of redundancy in navigation systems poses a significant danger, particularly when depending only on GNSS. To address this issue, it is advisable to include redundant navigation methods, such as inertial navigation, radar, or optical navigation. It is essential to provide crew members with training on alternate navigation techniques to be used in the event of a Global Navigation Satellite System (GNSS) malfunction (SAFETY4SEA 2021). Attention must also be given to the problems related to regulation and standards. It is essential to establish global standards and rules for the use of GNSS in marine navigation to ensure uniform implementation and

adherence. Collective collaboration among regulatory organizations, industry stakeholders, and technology developers is vital to collaboratively tackle these difficulties.

4.2 Automatic Radar Plotting Aids (ARPA)

ARPA systems are essential for maritime navigation since they provide vessels immediate and accurate data on the location, trajectory, and velocity of surrounding ships. Despite its advantages, ARPA systems might confront safety concerns that demand care (Leite Junior, et al. 2021).

Vulnerability 1 & Solution

One major risk is the possibility for target over-reliance, where operators may completely depend on ARPA data without cross-verifying information from other sources (Leite Junior, et al. 2021). In order to reduce this danger, training programs should place strong emphasis on the significance of using ARPA as an additional tool rather of relying only on it as a reference. This will encourage operators to integrate visual observations and information from other navigational instruments.

Vulnerability 2 & Solution

Another safety concern arises from the inaccurate interpretation of ARPA data, which might result in potential collision hazards. This difficulty may be solved by extensive training that focuses on increasing operators' abilities in analyzing ARPA information appropriately. Consistent training exercises and simulations may enhance decision-making abilities in the context of dynamic navigation circumstances (Leite Junior, et al. 2021).

Vulnerability 3 & Solution

Cybersecurity is a problem due to the possibility of deliberate or accidental disruption of ARPA communications. Implementing comprehensive cybersecurity measures, such as secure communication protocols and frequent system security upgrades, may help prevent unwanted access and modification of ARPA data. Inconsistency in the implementation and interfaces of ARPA systems across several boats might result in misunderstanding and operational mistakes. Establishing

worldwide standards for ARPA systems, including uniform user interfaces and operational processes, may help to safer and more consistent utilization (Leite Junior, et al. 2021). The development and promotion of these standards need collaboration among industry stakeholders, producers, and regulatory organizations.

4.3 The Electronic Chart Display and Information System (ECDIS)

The Electronic Chart Display and Information System (ECDIS) is an essential element found on a ship's bridge, offering digital navigation charts for the purpose of route planning and immediate navigation. Nevertheless, ECDIS systems are susceptible to safety and cybersecurity issues.

Vulnerability 1 & Solution

An important safety issue arises from over dependence on ECDIS as the main method of navigation. In order to tackle this issue, it is crucial for sailors to get thorough training that highlights the significance of cross-verifying Electronic Chart Display and Information System (ECDIS) data with other navigational equipment and visual observations (Voyager Worldwide 2020). To minimize the possibility of navigating mistakes, it is crucial to use redundancy in navigation techniques, such as using paper charts as a supplementary measure.

Vulnerability 2 & Solution

The presence of cybersecurity attacks targeting ECDIS systems is a significant hazard to the safety of navigation. Illegitimate entry or alteration of electronic charts might result in dissemination of false information, which may pose a risk to navigation. To safeguard ECDIS systems from cyber-attacks, it is essential to establish strong cybersecurity measures, such as implementing frequent software upgrades, ensuring secure network setups, and enforcing user authentication processes. Consistent surveillance for irregularities and immediate action towards any security breaches are crucial elements of a complete cybersecurity plan (De Groot 2020). An further obstacle arises from the possibility of software faults or hardware problems occurring in ECDIS systems. Regular maintenance, software upgrades, and system inspections are essential

for rapidly identifying and resolving difficulties. Mariners have to get training in identifying and resolving typical ECDIS issues, guaranteeing the dependability of the system in crucial navigation scenarios. In addition, companies should plan to supply ships with 2 laptops, with one laptop serving as the main system and the other as a backup in case the main one encounters any issues. The laptops will be sent fully updated, and at each port the ship makes, a USB encrypted device will be sent from the office containing all kinds of updates from the software company (ECDIS) for offline use. The password should be communicated via telephone once the captain receives the equipment. The update will be done offline by unlocking the USB.

4.4 Automatic Identification System (AIS)

The Automatic Identification System (AIS) is an essential instrument aboard a ship, providing instantaneous data on the identity, location, trajectory, and velocity of neighboring boats. Nevertheless, AIS systems are not devoid of safety and cybersecurity problems.

Vulnerability 1 & Solution

An issue of concern related to AIS is the possibility of broadcasting inaccurate or deceptive information. This may result in ambiguity and undermine situational awareness, hence increasing the likelihood of crashes (Soner, et al. 2024). In order to alleviate this issue, sailors should get training to cross-check AIS data with other navigation instruments, remain alert, and quickly report any irregularities. Moreover, the use of more robust authentication techniques in AIS may augment the reliability of the sent data.

Vulnerability 2 & Solution

The increasing concern is in the cybersecurity risks posed to AIS systems. Illegitimate entry or manipulation of AIS data may have significant consequences for marine safety and security. To safeguard against cyber-attacks, it is crucial to establish strong cybersecurity protocols, such as encrypting AIS signals, configuring secure networks, and regularly updating software. Cooperative endeavors in the marine sector to define and comply with cybersecurity standards might enhance the security of AIS systems against possible attacks. Also, the act of generating fake signals in order to

imitate genuine boats, known as AIS signal spoofing, presents a substantial threat to the safety of navigation. To identify and limit the effects of signal spoofing, using advanced anomaly detection algorithms, continuously monitoring AIS signals, and utilizing secure cryptographic protocols may be very effective. It is crucial to provide regular training to mariners on how to identify and react to suspect AIS activity. Moreover, deliberate or accidental tampering with AIS signals may cause disruption to marine communication and navigation (Soner, et al. 2024). By using frequency-hopping and signal encryption techniques, the robustness of AIS may be improved in the face of interference. Furthermore, implementing educational and awareness initiatives targeted towards mariners might enhance their comprehension of the need of promptly reporting any atypical AIS activity.

4.5 Voyage Data Recorder (VDR)

The Voyage Data Recorder (VDR) is an essential element aboard a ship, responsible for capturing crucial data pertaining to the functioning of the vessel. This data is used for accident investigation and to improve safety measures. Nevertheless, VDR systems are susceptible to safety and cybersecurity issues.

Vulnerability 1 & Solution

An important safety issue is the possibility of the VDR malfunctioning at crucial periods, including as crashes or emergencies, which might impede accident investigations (Söner, et al. 2023). Consistent maintenance and rigorous testing of the VDR system are important to guarantee its dependability. Sailors should get training on the correct use of VDRs and the need of swiftly reporting any system problems. Introducing redundancy in data recording systems, where possible, may provide a backup solution in the event of a main VDR malfunction.

Vulnerability 2 & Solution

The integrity and confidentiality of recorded data are at danger due to cybersecurity attacks targeting VDR systems. Illegitimate entry or manipulation of VDR data might have a detrimental effect on accident inquiries and jeopardize the security of the vessel. In order to tackle this issue, it is necessary to install strong

cybersecurity measures, which include secure network setups, encryption of stored data, and access restrictions. Consistent software upgrades and thorough security audits may effectively detect and address any possible weaknesses in the VDR system (Söner, et al. 2023).

Vulnerability 3 & Solution

Another safety risk arises from the possibility for data loss or corruption resulting from physical damage to the VDR during accidents or harsh weather. To reduce the likelihood of bodily harm, it is advisable to install the VDR in a secure and conveniently accessible area, such as a specialized enclosure or protective housing (Söner, et al. 2023). Frequent inspections to verify the soundness of the tangible elements, such as sensors and recording media, are essential for the efficient operation of the VDR.

5. Conclusions

The integration of automation and information technology (IT) systems in modern vessels has created new opportunities for malicious actors and hackers to carry out various cyberattacks that could lead to catastrophic incidents and significant safety hazards. The emergence of digital and network-based navigation systems has resulted in a substantial metamorphosis in the ship's bridge. In the event that robust protective measures are not in place, these entry points may function as susceptible access points for malicious entities. Notwithstanding the adoption of network isolation protocols, the bridge infrastructure continues to be vulnerable to security violations. The use of removable media as a means for software updates has the potential to introduce a cyber-security vulnerability, as it may serve as an entry point for malware to compromise the network. If a cyber-attack were to occur on the bridge system, for instance, through service denial or data manipulation, it could have far-reaching consequences on all navigation-related systems. It is significant to note that outdated operating systems for bridges, even without any malicious intent, can hinder the vessel's functionality. The act of identity spoofing caused by malware possesses the capability to cause harm to both the infrastructure and individuals. The proper functioning of ship-based networks, which are integral to the vessel's operations, is highly dependent on the effective management of network devices such as firewalls, routers, and switches. It is crucial to establish a strong security framework for such systems.

Furthermore, it is imperative to exert authority over networks that provide vendors with remote entry to navigation and other operational technology (OT) software installed on vessels. The creation of such networks may be considered crucial in enabling suppliers to remotely offer system upgrades or perform maintenance services. Ensuring the security of external access points for shoreside connections is of utmost importance in order to prevent unauthorized access.

Also, it is crucial that the management systems pertaining to cargo stowage, load planning and overall management are subjected to rigorous control measures. The question of whether mandatory ship reporting systems to public authorities should be differentiated from other networks, such as guest access networks, merits consideration. The former may be regulated, whereas the latter may lack regulation, given their frequent association with passenger leisure pursuits or crew members' personal internet usage.

Therefore, from the study of the literature and the analysis of this work it is obvious that the risk of a cyberattack on a vessel's identification, navigation and automation system is huge and quite dangerous and this is the reason why fairly strict measures must be taken. So, to sum up, the most frequent types of cyber-attacks on ships can have unpleasant or even catastrophic effects. The most important attacks can lead to the above results:

- Modification of ship data.
- Creation of not real ships.
- Sending of incorrect meteorological information with the purpose of changing the course of a particular ship.
- Activation of incorrect collision warnings.
- The possibility to make an existing ship "invisible".
- Falsification of EPIRB warnings.

Finally, integrated navigation systems, such as the Electronic Chart Display and Information System (ECDIS), Global Navigation Satellite Systems (GNSS), Automatic Identification System (AIS), Voyage Data Recorder (VDR), and Radar/Automatic Radar Plotting Aid (ARPA), are crucial for ensuring maritime safety and navigation on a ship's bridge. Notwithstanding their significance, these systems have shared safety and cybersecurity obstacles. Significant issues arise from excessive dependence on

ECDIS (Electronic Chart Display and Information System) and the presence of cybersecurity risks. These concerns highlight the need for thorough training, frequent maintenance, and strong cybersecurity safeguards. It is essential to include redundancy in navigation systems, provide secure authentication for AIS, and preserve VDR data using physical measures and cryptographic approaches. Collaborative endeavors in standardization, including both operational and cybersecurity aspects, are crucial to strengthen the resilience of these systems, guaranteeing that the marine sector can traverse the oceans with assurance, effectiveness, and protection.

Appendix

Glossary

Access control is selective limiting of the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions.

Back door is a secret method of bypassing normal authentication and verification when accessing a system. A back door is sometimes created in hidden parts of the system itself or established by separate software.

Bring your own device (BYOD) allows employees to bring personally owned devices (laptops, tablets, and smart phones) to the ship and to use those devices to access privileged information and applications for business use.

Cyber attack is any type of offensive manoeuvre that targets IT and OT systems, computer networks, and/or personal computer devices and attempts to compromise, destroy or access company and ship systems and data.

Cyber incident is an occurrence, which actually or potentially results in adverse consequences to an onboard system, network and computer or to the information that they process, store or transmit, and which may require a response action to mitigate the consequences.

Cyber risk management means the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level by taking into consideration the costs and benefits of actions taken by stakeholders.

Cyber system is any combination of facilities, equipment, personnel, procedures and communications integrated to provide cyber services; examples include business systems, control systems and access control systems.

Defence in breadth is a planned, systematic set of activities that seek to identify, manage, and reduce exploitable vulnerabilities in IT and OT systems, networks and equipment at every stage of the system, network, or sub-component life cycle. Onboard ships, this approach will generally focus on network design, system integration, operations and maintenance.

Defence in depth is an approach which uses layers of independent technical and procedural measures to protect IT and OT on board.

Executable software includes instructions for a computer to perform specified tasks according to encoded instructions.

Firewall is a logical or physical break designed to prevent unauthorised access to IT infrastructure and information.

Firmware is software imbedded in electronic devices that provides control, monitoring and data manipulation of engineered products and systems. These are normally self-contained and not accessible to user manipulation.

Flaw is unintended functionality in software.

Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

Intrusion Prevention System (IPS), also known as Intrusion Detection and Prevention Systems (IDPSs), are network security appliances that monitor network and/or system activities for malicious activity.

Local Area Network (LAN) is a computer network that interconnects computers within a limited area such as a home, ship or office building, using network media.

Malware is a generic term for a variety of malicious software, which can infect computer systems and impact on their performance.

Operational technology (OT) includes devices, sensors, software and associated networking that monitor and control onboard systems.

Patches are software designed to update software or supporting data to improve the software or address security vulnerabilities and other bugs in operating systems or applications.

Phishing refers to the process of deceiving recipients into sharing sensitive information with a third-party.

Principle of least privilege refers to the restriction of user account privileges only to those with privileges that are essential to function.

Producer is the entity that manufactures the shipboard equipment and associated software.

Recovery refers to the activities after an incident required to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.

Removable media is a collective term for all methods of storing and transferring data between computers. This includes laptops, USB memory sticks, CDs, DVDs and diskettes.

Risk assessment is the process which collects information and assigns values to risks as a base on which to make decision on priorities and developing or comparing courses of action.

Risk management is the process of identifying, analysing, assessing and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level considering associated costs and benefits of any actions taken.

Sandbox is an isolated environment, in which a program may be executed without affecting the underlying system (computer or operating system) and any other applications. A sandbox is often used when executing untrusted software.

Service provider is a company or person, who provides and performs software maintenance. Social engineering is a method used to gain access to systems by tricking a person into revealing confidential information.

Software whitelisting means specifying the software, which is present and active on an IT or OT system.

Virtual Local Area Network (VLAN) is the logical grouping of network nodes. A virtual LAN allows geographically dispersed network nodes to communicate as if they were physically on the same network.

Virtual Private Network (VPN) enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network, thereby benefiting from the functionality, security and management policies of the private network.

Virus is a hidden, self-replicating section of computer software that maliciously infects and manipulates the operation of a computer program or system.

Wi-Fi is all short-range communications that use some type of electromagnetic spectrum to send and/ or receive information without wires

References

1. Albakri, A., Boiten, E.A. and De Lemos, R. (2018) 'Risks of Sharing Cyber Incident Information,' Research Gate [Preprint]. https://doi.org/10.1145/3230833.3233284.
2. Aslan, Ö. et al. (2023) 'A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions,' Electronics, 12(6), p. 1333. https://doi.org/10.3390/electronics12061333.
3. Akpan F, Bendiab G, Shiaeles S, Karamperidis S, Michaloliakos M. (2022). Cybersecurity Challenges in the Maritime Sector. *Network*. 2(1):123-138. https://doi.org/10.3390/network2010009.
4. Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering*, *8*(10), 776.
5. Bigdeli, A.Z. et al. (2021) 'Exploring the root causes of servitization challenges: an organisational boundary perspective,' International Journal of Operations & Production Management, 41(5), pp. 547–573. https://doi.org/10.1108/ijopm-08-2020-0507.
6. Bhuyan, B. et al. (2015) 'Security issues in cloud computing,' in Advances in information security, privacy, and ethics book series, pp. 1–29. https://doi.org/10.4018/978-1-4666-8387-7.ch001.
7. Coffed, J. (2014). The threat of gps jamming. Exelis.
8. CRA (2022). Stryke. Available at: https://strakecyber.com/product/risk-assessment/.
9. Cyber Risk in Shipping (clvaw-cdnwnd.com).
10. Cyber Risks & Shipping: Maritime Cyber Insurance (maritimecyberadvisors.com).
11. Cyber Risks In The Shipping Industry - Thomas Fenner Woods Agency Thomas-Fenner-Woods Agency, Inc. represents the most reputable and financially sound insurance companies in the world. (tfwinsurance.com).
12. Cyber security and cyber risks in the shipping industry (penningtonslaw.com).
13. Cybersecurity Risk & σημεία προσοχής. - Digital Entrepreneurship ecosystem SMB (instech.gr).
14. CyberKeel (2014a). Maritime cyber-risks. NCC Group Publication.
15. CyberKeel (2014b). Security risks and weaknesses in ecdis systems. NCC Group Publication.

16. De Groot, N. (2020) Human perception problems of ecdis electronic chart displays, Maritime ergonomics. Available at: https://www.maritime-ergonomics.com/ergos-hfe/articles/human-perception-problems-of-ecdis-electronic-chart-displays/ (Accessed: 11 January 2024).
17. Djenna, A., Harous, S. and Saïdouni, D.E. (2021) 'Internet of Things meet Internet of Threats: New concern Cyber security Issues of critical cyber infrastructure,' Applied Sciences, 11(10), p. 4580. https://doi.org/10.3390/app11104580.
18. guidelines-on-cyber-security-onboard-ships-min.pdf (ics-shipping.org).
19. https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/.
20. https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf.
21. https://www.dnv.com/expert-story/maritime-impact/Yards-and-vendors-must-act-promptly-to-comply-with-upcoming-IACS-cyber-security-requirements.html?utm_campaign=Ind_404_Cyber%20sec%20IACS%20reqs&utm_medium=email&utm_ source=Eloqua.
22. ECDIS Info (2014). ECDIS Regulations. http://www.ecdis-info.com/ecdis_regulations.html.
23. Engler, E., Noack, T. and Beckheinrich, J. (2008) GNSS based solutions for maritime “Safety of Life” application with ..., Research Gate. Available at: https://www.researchgate.net/publication/224990046_GNSS_based_solutions_for_maritime_Safety_of_Life_Application_with_increased_Accuracy_Requirements (Accessed: 11 January 2024).
24. Grant, A., Williams, P. & Basker, S. (2014). GPS jamming and the impact on maritime navigation. The General Lighthouse Authorities.
25. Kennard, D. (n.d.). CYBER SECURITY AND CYBER RISKS IN THE SHIPPING INDUSTRY. Available at: https://www.penningtonslaw.com/news-publications/latest-news/2019/cyber-security-and-cyber-risks-in-the-shipping-industry.
26. Leite Junior, W.C. et al. (2021) ‘A triggering mechanism for cyber-attacks in naval sensors and systems’, Sensors, 21(9), p. 3195. doi:10.3390/s21093195.
27. Maritime cyber risk (imo.org).
28. Mordechai, G., Kedma, G., Kachlon, A. & Elovici, Y. (2014). Airhopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies. Malicious & Unwanted Software Co.

29. Navigating cyber risk in the shipping industry - WTW (wtwco.com).
30. Offshore Blue (2016). A re-cap of the navtex system. Navigator's Newsletter.
31. SAFETY4SEA (2019) Study stresses major concerns on Ecdis safety, SAFETY4SEA. Available at: https://safety4sea.com/study-stresses-major-concerns-on-ecdis-safety/ (Accessed: 11 January 2024).
32. SAFETY4SEA (2021) Bridge procedure: GNSS failure while using the Ecdis, SAFETY4SEA. Available at: https://safety4sea.com/cm-bridge-procedure-gnss-failure-while-using-the-ecdis/ (Accessed: 11 January 2024).
33. Santamarta, R. (2014b). A wake-up call for satcom security. IOActive.
34. Söner, Ö. et al. (2023) 'Cybersecurity risk assessment of VDR', Journal of Navigation, 76(1), pp. 20–37. doi:10.1017/s0373463322000595.
35. Soner, O. et al. (2024) 'Risk sensitivity analysis of AIS cyber security through Maritime Cyber Regulatory Frameworks', Applied Ocean Research, 142, p. 103855. doi:10.1016/j.apor.2023.103855.
36. Süzen, A.A. (2020) 'A Risk-Assessment of cyber attacks and defense strategies in industry 4.0 ecosystem,' International Journal of Computer Network and Information Security, 12(1), pp. 1–12. https://doi.org/10.5815/ijcnis.2020.01.01.
37. Ship Cybersecurity | Maritime Industry Cybersecurity (mitags.org).
38. Tam, K. & Jones, K.D. (2018b). Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping.
39. The importance of cyber security risk management in shipping (shippingandfreightresource.com).
40. The importance of cybersecurity in the maritime industry (marine-digital.com).
41. The Guidelines on Cyber Security Onboard Ships (2022). Retrieved from: guidelines-on-cyber-security-onboard-ships-min.pdf (ics-shipping.org).
42. Top cyber concerns for the shipping industry | AGCS (allianz.com).
43. Wagstaff, J. (2014). All at sea: Global shipping fleet exposed to hacking threat. Reuters.
44. What is a Cyber Risk Assessment? | Axio.
45. Voyager Worldwide (2020) Ecdis: From problem to solution?, Voyager Worldwide. Available at: https://voyagerww.com/uncategorized/ecdis-from-problem-to-solution/ (Accessed: 11 January 2024).
46. Σπανός, Σ. (2021), Κυβερνοασφάλεια στη Ναυτιλία : Συγκριτική μελέτη! του Στέφανου Σπανού Director, CTO & Lead Assessor of ISONIKE Ltd, Retrieved

from: https://www.cyberinsurancequote.gr/news/kyvernoasfaleia-sti-naytilia-sygkritiki-meleti-toy-stefanoy-spanoy-director-cto-lead-assessor-of-isonike-ltd/.

47. V.Bolbot,G.Theotokatos,E.Boulougouris,D.Vassalos (2020), 'A novel cyber-risk assessment method for ship systems' Available at: https://doi.org/10.1016/j.ssci.2020.104908