Right on Course: Towards Cyber Secure Sailing?

Gunput, Stuart

Right on Course: Towards Cyber Secure Sailing?

Executive Master Cyber Security Thesis

Universiteit Leiden
Governance and Global Affairs

Name: Stuart Gunput

30th of January 2023

1st Supervisor: Olga Gadyatskaya
2nd Supervisor: George Smaragdakis

Acknowledgments

After two years of spending additional time on studying, I can proudly present my thesis. First, I would like to thank my wife, who supported me all those days of studying. Especially in the last days of submitting the thesis, coffee, food and support was within hands reach.

I would also like to express my gratitude to my thesis supervisor Olga Gadyatskaya for providing ideas and feedback on my thesis. Olga was always available and willing to help me and took the time to look through my material between her own deadlines. Furthermore, I would like to thank George Smaragdakis for being my second supervisor and taking the time to read my thesis.

I would like to thank all the interviewees who took the time and effort to provide the data for my research. Without their help I would not have any data to start with. Finally, I would like to thank my work as well as my colleagues for providing the opportunity to do this master's study and understanding that I was not always available during office hours.

Abstract

In the recent years, the maritime industry is applying Industrial Internet of Things devices, data trending and high-speed satellite connections. While these advances in technology make business easier for the industry, there are also drawbacks with these advances. In the past the maritime industry had an air-gap between the different systems. The probability of a cyber incident would be limited, let alone the probability of an incident propagating to a different system. Now, systems are interconnected and the risk of a cyber incident occurring is high, similar for the risk of an incident on one system propagating to another system. There are different academic studies, which have looked at maritime cyber threats as well as measures. However, there are not many qualitative studies in how the maritime industry is actually dealing with cyber threats.

For this thesis, first a literature survey was conducted on cyber security onboard ships. The survey showed that most of the literature is focussed on navigation and communication systems, where there are more systems which can be attacked, such as propulsion control systems and engine control systems. The literature study also shows that the focus on measurements against attacks are solved mainly in the governance domain. The main driver that is mentioned in the literature is IMO resolution MSC.428(98). The role of the shipyards and suppliers are equipment and systems are not mentioned in the literature, as these actors are not in the scope of the resolution.

Following the literature survey, semi-interviews were held with eight people working at different organisations in the maritime industry. The interviewees were selected using expert sampling and snowballing. The interviews took approximately 30-45 minutes and were held online via Teams. After the interviews were held, the interviews were transcribed and subjected to thematic analysis, where the interviews were coded and themed.

The combination of the literature survey and the semi-structured interviews provided the answer to what the maritime industry is doing to deal with cyber security on board ships. The conclusion is that while the maritime industry is lagging behind other industries, it is improving. The maritime industry is realising that cyber security is an important aspect of their daily business. Due to the many different actors involved in the maritime industry, there is a need for clear requirements and responsibilities. From top down, this starts with international organisations and classification societies in combination with owners enforcing requirements during the life time of a ship to the shipyards and suppliers of equipment and systems. To ensure that all parties are complying with the rules and regulations and that the systems on board the vessel work as intended, it is recommended to put one party in charge of cyber security on board ships.

Table of Contents

List of Acronyms

AMCS	Alarm, Monitoring and Control System
AIS	automatic identification system
BIMCO	Baltic and International Maritime Council
CCTV	closed-circuit television
CPS	cyber physical systems
CSAN	Cyber Security Assessment Netherlands
DPS	Dynamic Positioning Systems
ECDIS	Electronic Chart and Display System
EWS	Engineering Work Stations
GMDSS	Global Maritime Distress and Safety System
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HMI	Human Machine Interface
IACS	International Association of Classification Societies
IMO	International Maritime Organisation
IIoT	Industrial Internet of Things
ICS	industrial control systems
ICT	information and communication technology
IT	information technology
MITM	Man-in-the-Middle
NMEA	National Marine Electronics Association
NIST	National Institute of Standards and Technology
OT	Operational Technology
PCS	Propulsion Control Systems
PMS	Power Management Systems
UR	Unified rRules
VDR	Voyage Data Recorder
VHF	Very High Frequency
VSAT	Very Small Aperture Terminal

1. Introduction

In the recent years the trend of devices connected to the internet has increased significantly. Where in the early days of the internet interaction was between a limited number of devices and type of devices, we now see that not only the number of devices has increased but also the type of devices has increased and is increasing. Smart phones, tablets and wearables are just examples from devices that consumers started using in the last 20 years. The increase in connectivity of devices is not only for consumer electronics, but also for industrial devices. The recent trend in the industry is to have industrial devices which are interconnected in a smart manner, the Industrial Internet of Things (IIoT). Using smart sensors and actuators in the industry is often credited as the fourth industrial revolution or industry 4.0 and is seen as the next step in the industry (Mosteiro-Sanchez et al., 2020). With IIoT the traditionally hard separation between the operational technology (OT) network and information technology (IT) network disappears (Dhirani et al., 2021). These industrial developments are also occurring in the maritime industry and aboard ships (Sahay et al., 2019). Here networks of different systems are more and more interconnected and connected to the internet.

On one hand the increase of smart devices in the industry makes organizations more competitive, and it is making life easier (Dhirani et al., 2021). On the other hand, there is also an increase for risks in cyberattacks on IIoT devices, which are used in industrial control systems (ICS). Thus, a cyber-attack can have impact on physical systems as well as machine to machine communication (Dhirani et al., 2021). This is the case for control systems for critical infrastructures on land and similarly for this is the case for control systems on board ships.

1.1 Importance of Cyber Security for the Maritime Industry

The European Union (EU) Directive 2022/2555 (2022), which is better known as the NIS 2 Directive, will become effective in 2024 in the EU and contains measures for cyber security. According to the NIS 2 Directive (2022), the maritime industry as part of the transport sector is considered a critical infrastructure. Maritime trading is responsible for responsible for 90% of the word trade according to Kechagias et al. (2022). They also state that many ships have not incorporated cyber security by design due to their age and that legacy IT and OT systems make the maritime industry susceptible to cyberattacks by cybercriminals (Kechagias et al., 2022). This means that there are cyber security risks for the maritime industry, which can have an impact on the operability of ships.

A cyber incident on a ship can have far-reaching consequences, depending on the ship's systems involved and the ship's location at the time of the attack. When the ship is in a busy sailing area and the ship's navigation and propulsions systems are involved in an incident, the impact can be severe.

As an example, which is not related to cyber incidents, blocking of the Suez Canal by the Evergiven has had a huge economic impact (Lee & Wong, 2021). If a similar incident occurred with a different ship in the Suez Canal, however now triggered by a cyber incident, the economic impact would be as severe as it was with the Evergiven.

Although the impact of a cyber incident on a vessel that is not sailing is less, the economic impact can be still substantial. The Baltic and International Maritime Council (BIMCO) (2021) has reported a case where the bridge systems of a dry bulk carrier where infected with a virus, and as a consequence the vessel could not leave the port for days. The damage was estimated in the hundreds of thousands of dollars (BIMCO, 2021).

1.2 Research Question

Although cyber security threats in the maritime industry are known and mapped (Grispos & Mahoney, 2022), there is little literature on how the maritime industry deals with these threats in practice. This thesis aims to provide more insight into the question: *What is the maritime industry doing to deal with cyber risks on board ships?*

The thesis will be exploratory and to answer the research question a literature survey will be done as well as qualitative research by interviewing different actors in the maritime industry.

As a theoretical framework, the cyber harm model of B. van den Berg and Kuipers (2022) as well as the three-layer model of cyberspace of J. van den Berg (2018) are used. The cyber harm model is used to show how the industry is dealing with threats, which may be intentional or unintentional and physical or informational. The cyberspace model of J. van den Berg is used for the division of technical measures, socio-technical measures or governance measures, which may highly depend on the type of maritime actor.

By using the cyber harm model, we identify which threats the maritime industry foresees. In this thesis the focus will be on the harm to humans and society. The following sub-questions are discussed.

RQ1: *Which intentional harm is foreseen for physical damage and information damage and what are the vulnerabilities, attack vectors and main adversaries?*

RQ2: *Which unintentional harm is foreseen for physical and information damage and what are the vulnerabilities and causes?*

From the three-layer model the following sub questions will be answered.

RQ3: *For the technological layer, which technological solutions are mainly used in the industry or are upcoming to achieve a cyber secure ship?*

RQ4: *For the socio-technical layer, what are the policies that organisations use or are going to use to achieve secure networks?*

RQ5: *For the governance layer, which classification rules, industrial standards and applicable cyber security regulations (national and international) are used?*

The scope of the thesis is the maritime industry, which can be quite a broad definition. For the scope of the thesis first owners of ships are considered. Secondly the ships are built at a shipyard, which is also considered. Onboard a ship there are different systems, which are supplied by suppliers of systems and equipment. These are the third category of actors which are considered. As fourth, there are the classification societies, which play an important part in approving designs during building of ships and during the life time of a ship. Finally, there are the authorities which can provide additional requirements for the maritime industry.

1.3 Theoretical Framework

This section will elaborate the theoretical framework used for this thesis. For this thesis two theoretical frameworks are used. The first framework is the Cyber Harm model of B. van den Berg and Kuipers (2022), while the second framework is the cyberspace model of J. van den Berg (2018).

1.3.1 Cyber Harm Model

The cyber harm model is a model, which is developed by B. van den Berg and Kuipers (2022), with the goal of mapping the complex world of cyberspace, the threats from cyberspace and the reach of potential issues. The model is depicted in Figure 1 and shows the different distinctions that the model makes. Firstly, the model makes a distinction between harm to society that occurs in cyberspace and harm to society that occurs via cyberspace (B. van den Berg & Kuipers, 2022). Harm to society in cyberspace is in the core of the model and accounts for the damage that is done on the technical side of cyberspace, including networks, software, hardware and stored data and is considered indirect harm to humans (B. van den Berg & Kuipers, 2022). The harm in cyberspace can either be accidental (e.g., system errors, configuration errors) or intentional (e.g., ransomware, DDoS attacks). The model also considers harm to society via cyberspace, where harm can either be intentional or accidental, as well as physical and direct harm or informational harm (B. van den Berg & Kuipers, 2022). Physical harm is harm which occurs to physically in the world outside of cyberspace (i.e. the physical world) (B. van den Berg & Kuipers, 2022). An example of intentional

physical harm is the case of the attack on the power gird of Ukraine in 2014, where Russian state actors had the goal to cause disruption of the supply of electric power (Whitehead et al., 2017). According to B. van den Berg and Kuipers (2022), accidental physical harm is underestimated and can form a threat to cyber physical systems. On the other side of physical harm there is harm that occurs not physically and is considered informational harm. Informational harm is not harm to data (i.e., the bits and bytes) but rather harm caused on the content layer of data, such as disinformation or data theft for intentional informational harm and misinformation for accidental informational harm.

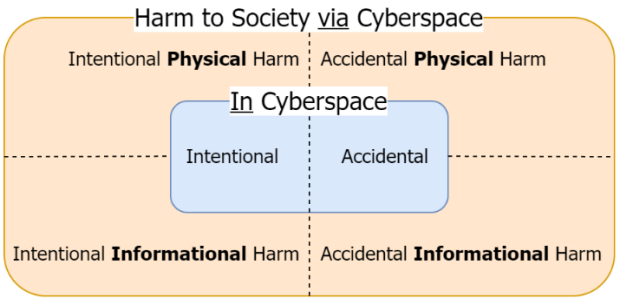

Figure 1: The cyber harm model (taken from (B. van den Berg & Kuipers, 2022)).

The reason this model is chosen is for this thesis that cyber incidents on ships are not limited to informational harm. A disruption in certain systems may lead to physical harm. Furthermore, this model takes into account that some incidents are accidental as well. The combination of these two factors, thus the separation in informational and physical harm as well as the separation in accidental and intentional harm, make this model suited for this thesis. The focus of the model for this thesis will be the harm to society via cyber space. Harm to society in cyberspace in the maritime industry is similar to harm to society in cyberspace for other industries, while harm to society via cyberspace can be different between the maritime industry and other industries. For example, if a computer on a ship becomes infected with malware and is used as a zombie in a botnet, the harm is comparable to when a computer in another industry becomes infected with the same malware. However, when the same malware is causing a navigational computer on a ship to crash and in turn causes the ship to collide with the shore, the harm that is inflicted on society via cyberspace is unique for the maritime industry.

1.3.2 Cyberspace Model

The second model that is used for this thesis is the model of cyberspace as developed by J. van den Berg. In this model cyber space is divided into three layers: the technical layer, the socio-technical layer and the governance layer (J. Van den Berg, 2018). The technical layer is in the heart of the

model and this represents information and communication technology (ICT). Here the technology that enables cyber space is represented. The middle part of the model represents the socio-technical layer, where the interaction of users with technology, or cyber activities, takes place. Cyberspace is an environment, which is governed and this is represented in the model as the final layeResearcher: the governance layer. Figure 2 illustrates the three layers and the interaction between these layers. The layers are divided into different sub-domains, which represent different sectors in society such as health, finance and transportation (J. Van den Berg, 2018). This is not illustrated in Figure 2, as there are many sectors which can be represented (J. Van den Berg, 2018), making it difficult to illustrate a complete picture. However, the focus of this thesis is the transportation sector (the maritime industry).

This model is chosen because it categorises actions, which are taken in cyber space into three distinctive groups, with their own characteristics and limitations. These three categories are considered separately, with a dedicated research question.

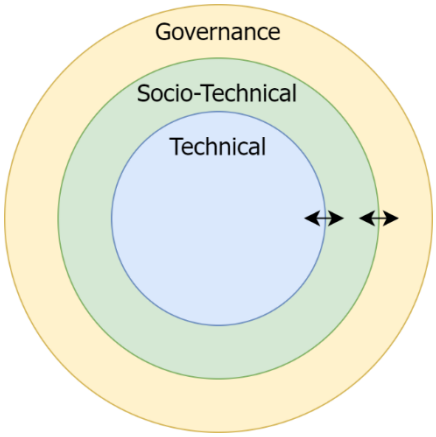

Figure 2: Simplified illustration of the 3-layer model where the arrows indicate interactions between the different layers. Taken from (J. Van den Berg, 2018).

1.4 Thesis Structure

The thesis is organised as follows. This chapter, Chapter 1 has given an introduction on the topic and has illustrated why cyber security for the maritime industry and society. This chapter has also presented the research question. The following chapter, Chapter 2, will start with the literature review regarding cyber security in the maritime industry. Subsequently, Chapter 3 will discuss the research methodology used for this research, the interviews and the data analysis of this thesis. This chapter is followed by Chapter 4 which will contain the actual analysis and will provide the results of the research. The thesis is finalised with the discussion and conclusion in Chapter 5.

2. Cyber Security Onboard Ships and in the Maritime Industry

This chapter contains the literature review of this thesis. The literature is set up int the following manner. First a typical network architecture of a ship is discussed along with the vulnerabilities for cyber incidents. Next the different threat vectors are discussed, and finally the different threat actors.

2.1 Vulnerabilities

On board a ship there are various networks, which can be targeted by cyber incidents. This section will provide some ship specific examples of the different vulnerabilities on board ships and at ports. Figure 3 shows different networks, which can be found on a ship based on literature (Akpan et al., 2022; BIMCO, 2021; Hatteland Technology, 2022; Meland et al., 2021). Modern ships are equipped with navigational systems such as a Voyage Data Recorder (VDR), Global Positioning System (GPS), radar, Electronic Chart and Display System (ECDIS), amongst others. These systems are usually interconnected into bridge networks. Besides the navigational systems, there are also various communicating devices such as Very High Frequency (VHF) radio, Global Maritime Distress and Safety System (GMDSS) and the automatic identification system (AIS) connected to the bride network. Usually there are closed-circuit television (CCTV) systems, which are on a separate network due to the high amount of data that is transmitted and stored. There are also systems which are related to the industrial platform of a ship such as the Alarm, Monitoring and Control System (AMCS), Propulsion Control Systems (PCS), Dynamic Positioning Systems (DPS) and Power Management Systems (PMS). Finally, there are IT networks, which are used for the office network for email and data exchange, or welfare networks (i.e. networks dedicated for personal communication and entertainment) such as IPTV and 4G connections. The different systems are shown in Table 1. The table also shows the use of the different systems and therefore importance of the systems for ship operability.

As stated in Chapter 1, port authorities, and thus ports, are a part of the maritime industry. Gunes et al. (2021) and De La Peña Zarzuelo (2021) identified various port vulnerabilities. Due to the transition to Industry 4.0, the main vulnerabilities identified by Gunes et al. (2021) as well as De La Peña Zarzuelo (2021) are cyber physical systems (CPS).

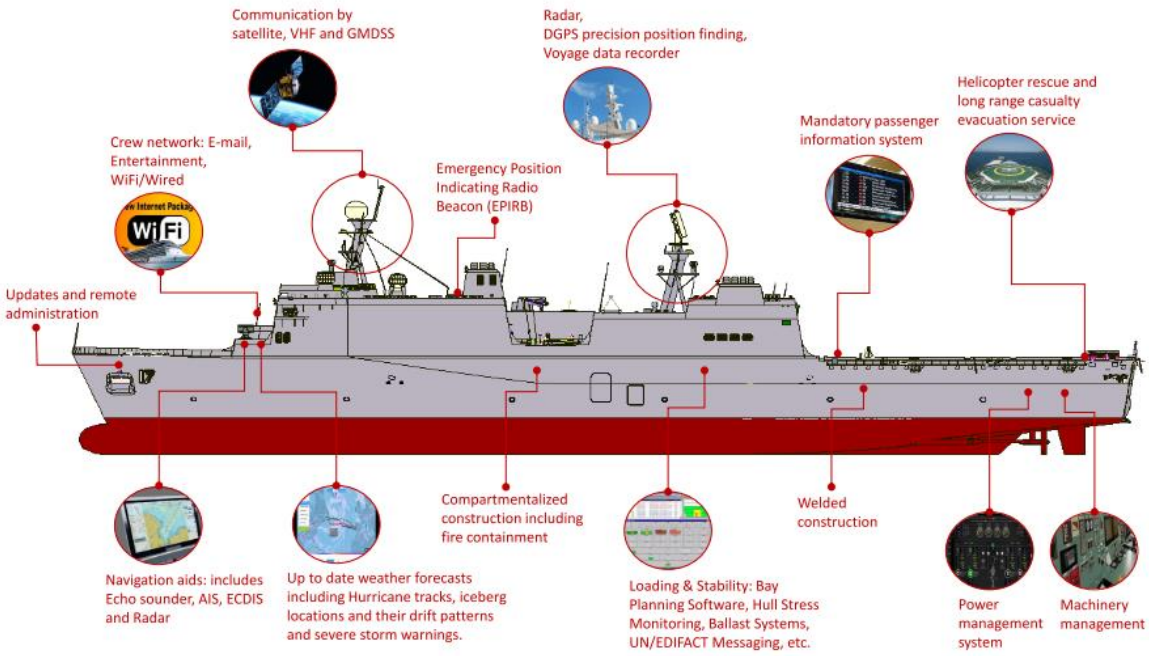

Figure 3: Typical automation systems onboard a ship (Akpan et al., 2022).

Table 1: Summary of automation systems on board of ships (Akpan et al., 2022).

System	Use
Automatic Identification System (AIS)	AIS is used for vessel traffic monitoring and assistance. With AIS the location and direction of a ship are transmitted. The main purpose of AIS is to avoid collisions between ships. Ships can see if other vessels are nearby and port and maritime authorities know the location of ships. AIS can assist with accident investigation and search and rescue operations.
Electronic Chart and Display System (ECDIS)	The ECDIS collects and combines data from different navigational sensors and displays the position of the ship on a map in real time. When a ship has paperless navigation, two independent systems are required.
Global Navigation Satellite System (GNSS)	A GNSS such as GPS is used to determine the position of a ship and calculate the speed. It can also be used to determine the time.
Radar	The radar provides information about the ship's surroundings. It is used for the detection of other ships and objects.

Global Maritime Distress System (GMDSS)	The GMDSS is used to broadcast distress messages regarding safety issues as well as for sending and receiving critical safety alerts.
Alarm, Monitoring and Control System (AMCS)	The AMCS displays alarm information and statuses of different equipment aboard a ship. With an AMCS is it possible to control various equipment from the AMCS status. The AMCS assists in reducing human errors and increases resource productivity. By having alarms prior to emergency situations, the life of the equipment will be extended.
Very Small Aperture Terminal (VSAT)	VSAT is used to transmit and receive data over a satellite communication link. VSAT can be used for internet connections while at sea.
Propulsion Control System (PCS), Power Management System (PMS)	The PCS is used to control various equipment in the propulsion line of the ship such as engines, gearboxes and propellors. The power management system ensures that there is enough (electric) power available for ship's operation.
Video Surveillance System	Ships often have video surveillance systems or CCTV. The system is used for monitoring the actual situation on board the ship such as in the engine room or cargo holds as well as the situation around the ship.
IT Network Systems	There are different IT networks onboard a ship. These are used either as an office network, used for crew or passenger welfare as well as crew or passenger devices (BYOD).

Most of the literature related to cyber security on board ships and in the maritime industry is related to the navigation systems and mainly the ECDIS (BIMCO, 2021; Erstad et al., 2022; Svilicic et al., 2020). With paperless navigation becoming more common, sailors rely on the ECDIS to navigate (Erstad et al., 2022; Svilicic et al., 2020). With an attack on the ECDIS, the charts become unavailable

or the information the charts display is incorrect. Other vulnerabilities in the navigation networks are the use of industrial protocols which are not secured such as the National Marine Electronics Association (NMEA) 0183 protocol (Longo et al., 2022). The same can be said for the industrial network onboard ships, where systems such as the PMS, PCS and AMCS are connected to. These systems also rely on industrial protocols, such as Modbus, which are relatively simple and not secure by design (Knapp & Langill, 2015). The research of Gunes (2021) and De La Peña Zarzuelo (2021) showed that the vulnerabilities of the ports are mainly the cyber physical systems, caused by the transition to Industry 4.0.

2.2 Threat Vectors

The previous section has discussed the different vulnerabilities on board a ship and ports. This section will elaborate on the common threat vectors and how they are affecting the different systems onboard a ship. Common attacks on industrial networks are Man-in-the-Middle (MITM) attacks, Denial-of-Service attacks, social engineering and compromising the Human Machine Interface (HMI) and Engineering Work Stations (EWS) (Knapp & Langill, 2015). Grispos and Mahony described altering navigational charts by hackers, jamming or spoofing of radar signals, tampering AIS data and spoofing of GPS signals amongst others as threat vectors (Grispos & Mahoney, 2022). As navigational systems on board ships are important, most of the literature is focussed on attack vectors affecting these systems as well.

2.2.1 Man In the Middle attack

In case of a Man-in-the-Middle (MitM), the attacker positions itself between communicating devices and snoops the communication traffic (Knapp & Langill, 2015). The attacker intercepts messages from the transmitting devices and alters the data and transmits the altered data. On the receiver side the devices receive the altered data and do not know that this data does not originate from the transmitter. A MitM attack is easier to implement and more successful when communication is unencrypted or when the attacker can make the regular devices trust that the data is transmitted correctly, which is the case in most of the industrial communication protocols (Knapp & Langill, 2015).

Because the maritime industry also relies on industrial communication protocols, MitM attacks are a threat as well. Longo et al. (2022) have demonstrated that it is also possible to alter radar data by performing a MitM attack. This study focussed specifically on the NMEA and ASTERIX protocols, which are used by many navigational systems (Longo et al., 2022). With the attack the Longo et al. researched, this type of attack sensory data is altered. Meland et al. (2021) have described a cyber

security incident, where emails were intercepted and bank account details were altered to make payments to wrong bank accounts.

2.2.2 Denial of Service

Knap and Langill (2015) define a Denial of Service (DoS) attack as an attack which is malicious and makes a service unavailable. Jamming of GPS signals can be considered a DoS attack, as with GPS jamming, the signal becomes unavailable and the position of the ship cannot be determined. Signal Jamming is described by Oruc et al. (2020) and has occurred on several instances, mainly by state actors.

2.2.3 Social Engineering

Social engineering is often used to gain access to networks. With social engineering attackers use the human factor to execute their attack (Kechagias et al., 2022). Many attacks are exploiting the human factor and expert often argue that humans are the weakest link within cyber security (Kechagias et al., 2022). A commonly used method of social engineering is phishing (Beaman et al., 2021). Meland et al. (2021) have described several incidents where phishing was used to deliver malware to organisations in the maritime industry. Jo et al. (2022) have described a case where the attacker has used pictures of a crew member on social media which showed the password to the ballast water management system. This can also be considered to be a form of social engineering.

2.2.4 Compromising Human Machine Interfaces and Engineering Work Stations

By elevating privileged in HMIs and EWSs, an attacker can easily obtain command and control privileges in industrial networks (Knapp & Langill, 2015). Compromising of these work stations is via malware that is send to the work station using phishing emails or by using infected storage devices (Meland et al., 2021).

2.3 Threat Actors

Looking at the literature, three different actors as defined in the threat matrix of the Cyber Security Assessment Netherlands (CSAN) can be distinguished. First there are the incidents which are unintentional, followed by criminals and finally there are the states and state-actors.

2.3.1 Unintentional Actors

First there are the actors which are responsible for unintentional acts. These are actions performed by actors who unknowingly cause disruption of the systems on board. BIMCO has reported two incidents which are accidental (BIMCO, 2021). In the first case BIMCO that reports, navigational computers with the ECDIS crashed due do a software update performed previously by a service

engineer on outdated operating systems (BIMCO, 2021). Not knowing that the operating system could not support the new software, the service engineer installed the latest version of the navigational software, thinking it would be beneficial for the client. At sea the ECDIS computers crashed and navigation had to be done with one radar and back-up paper charts (BIMCO, 2021). In the second case of an incident in the report of BIMCO the ECDIS and navigational computers were crashing as well due to outdated software (BIMCO, 2021). The pilot and crew had to navigate visually and by using the radar. The main difference with the previous example is that this time the problem of the outdates operating system was known for a prolonged time by the crew of the ship and reported to the owner of the vessel, however no action was taken by owner to update the system (BIMCO, 2021).

2.3.2 Cyber Criminals

The other type of threat actors which are contributing to cyber incidents onboard ships are cyber criminals. The goal of these actors is to get money from their victims by using ransomware, threatening to leak sensitive information or social engineering by sending fraudulent invoices or stealing user accounts (Meland et al., 2021). BIMCO (2021) has reported a case in the whitepaper of infected office networks onboard a ship with ransomware, where the owner of the ship paid the ransomware sum in at least one of the cases.

2.3.3 State and State Actors

The last type of actors which are seen in the maritime industry are state and state actors. These actors are usually politically motivated and are behind espionage (including commercial and industrial) as well as financial gains and commercial gains (BIMCO, 2021; Meland et al., 2021). A well-known example of a cyber incident involving state actors in the maritime industry is the NotPetya campaign. Initially targeted at Ukraine, the NotPetya worm reached Maersk via an Ukrainian port and the attack resulted in losses for more than $300 million (Akpan et al., 2022; Jasper, 2020, p. 100). The NotPetya malware is considered pseudo ransomware due to the way it was made. It looked like ransomware, however the way payments where handled and deletion of the encryption key, showed that the goal of the malware was more to disturb services within Ukraine. The NotPetya attack is attributed to groups connected to the Russian intelligence agency GRU and in 2018 the United State held the Russian military responsible for the attack (Jasper, 2020, pp. 101, 123). Lesser known examples of state sponsored attacks are related to GPS/GNSS as described by Oruc (2020). Oruc has described five instances of GPS spoofing or jamming by Russia, Turkey and North Korea (Oruc, 2020). Furthermore port authorities are also high value targets for state actors as indicated by Oruc (2020).

2.4 Maritime Measures

2.4.1 Technological

In order to detect attacks on the radar system, Longo et al. (2022) proposed an algorithm, which according to their research can detect anomalies with a high accuracy. The cases presented by BIMCO where aging hardware and software were causes of cyber incidents were solved by having up-to-date hardware and operating systems onboard the vessel.

2.4.2 Socio-Technical

Cyber-MAR is a research project that was funded by the European Union as part of the Horizon 2020 project (Canepa et al., 2021). As part of the project, research was done on cyber security and awareness training. The result was that most of the participants agreed that the training raised their awareness of cyber threats in the maritime industry. From the training case studies and counter measurements against the threats from the case studies were appreciated the most (Canepa et al., 2021).

In their qualitative research, Erstad et al. (2022) have concluded that attacks on the ECDIS may cause unavailability of that system, where the impact of unavailability of the ECDIS was compared to sailing in extremely foggy weather. One of the main measures against cyber-attacks mentioned in the research is training of navigators for situations where cyber threats may occur (Erstad et al., 2022). By having training Erstad et al. (2022) argued that cyber-attacks would be recognised and cyber resilience would be achieved.

2.4.3 Governance

Cyber activities in the maritime industry are governed trough international organisations, domestic rules and private sector protocols (Wilson, 2022). This section will elaborate on some of the most common organisations involved in governance of cyber activities and cyber security.

One of the main drivers for cyber security on ships driven from a governance point of view and is the International Maritime Organisation's (IMO) Resolution MSC.428(98) (Grispos & Mahoney, 2022; Hopcraft et al., 2021; Karim, 2022). In this resolution from 2017, the IMO strongly encourages to have a cyber risks recorded in a security management system from January 1, 2021 (International Maritime Organization, 2017b). Apart from this, the IMO has guidelines on maritime cyber risk management which provides recommendations and best practices (International Maritime Organization, 2017a; Wilson, 2022).

On the basis of this resolution and the National Institute of Standards and Technology (NIST) Cyber Security Framework Version 1.1, different maritime organisations, such as BIMCO, the International Chamber of Shipping and the Super Yacht Building Association, have combined contributed to formulate guidelines in a whitepaper. In the latest version from 2021 of this white paper different threats, actors and how to deal with the cyber incidents are mentioned (BIMCO, 2021).

A cyber security systematic approach based on an anonymised ship management company has been studied by Kechagias et al. (2022). In this study incorporation of a cyber security systematic approach by a shipping company was described. The company had a Plan-Do-Check-Act approach for a safety management system as well as their cyber security strategy (Kechagias et al., 2022).

2.5 MITRE ATT&CK Framework

An attack can be analysed using the MITRE ATT&CK framework (MITRE, 2021). Jo et al. (2022) have given examples of cyber-attacks using this framework. The framework is depicted in Figure 4 shows this model and the various steps in this model. This section the framework is discussed and examples are given from the maritime industry.

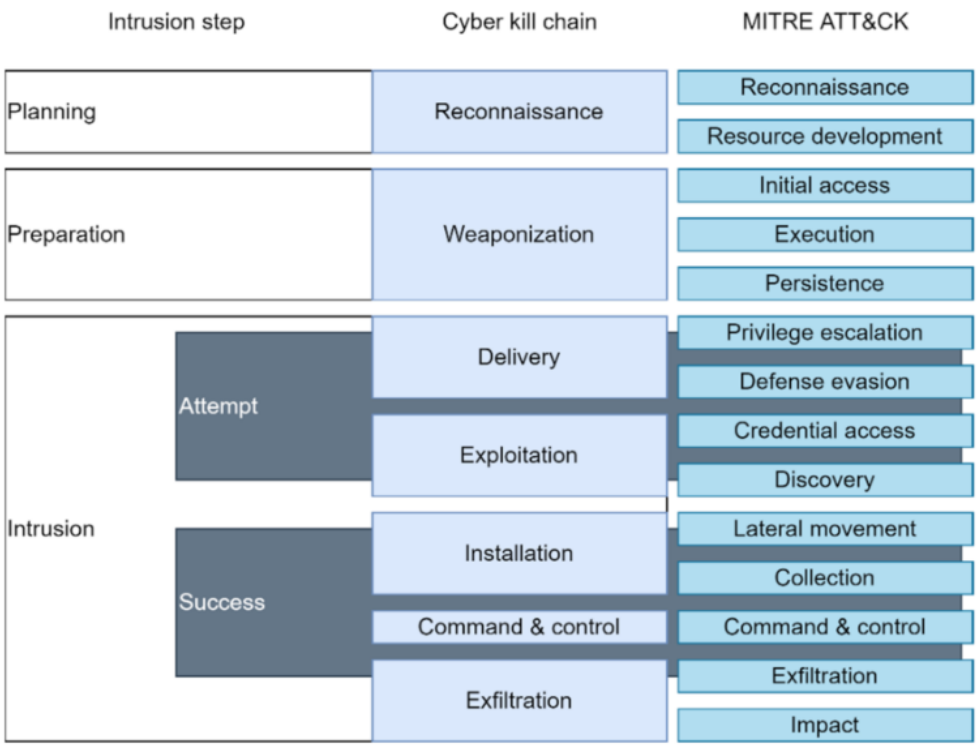

Figure 4: MITRE ATT&CK Framework (Jo et al., 2022).

2.5.1 Planning

In the **Reconnaissance phase**, the attacker is looking for entry points into the system, as an example the attacker can look at different equipment commonly used on ships or extract information of systems used from pictures social media (Jo et al., 2022).

During the **Resource Development** phase, the attacker goes further and looks for vulnerabilities in the systems that are used on board a ship. Examples of such vulnerabilities are standard administrator passwords.

2.5.2 Preparation

For **Initial Access**, the attacker uses the information gathered in the planning period and accesses the network on board the ship (Jo et al., 2022). This step is followed by the **Execution phase** where the attacker runs malicious code on the accessed machine, which could be network scanning tools to find vulnerable points in the network. In the **Persistence phase** the attacker has identified vulnerabilities in the OT system and exploits these vulnerabilities or tampers with the firmware. As an example, Jo et al. (2022) have indicated that some suppliers deliver an ECDIS with a standard password of “0000”, which the attacker can use in their advantage.

2.5.3 Intrusion

During **Privilege escalation**, the attacker tries to obtain higher-level permissions, which can be achieved by sending phishing to crew members. At the same time, the attacker always tries to avoid detection, which is **Defence Evasion**. With **Credential Access**, the attacker aims to get a hold of the credentials of different users and these credentials are in turn used for privilege escalation.

At the same time during the **Discovery** phase, the attacker tries to find different vulnerabilities in the system. With **Lateral Movement**, the attacker tries to manoeuvre through the systems and influence other machines. As an example, Jo et al. (2022) explain that attackers used the satellite communication terminal to gain access to the ballast water management system.

The next step which is described in the model is **Collection**. Here the attacker collects relevant information and data which is of interest for their goal. With **Command and Control**, the attackers try to communicate with their targeted system, which can be the ECDIS, the BWMS or any other system on board the ship.

By **Exfiltration**, the attacker obtains data from the targeted system. This can be process information from the OT network, which can be used by the attacker (Mohammed et al., 2022). The last step in

the MITTRE ATT&CK framework is **Impact**, where the attacker performs the intended attack (Jo et al., 2022).

2.6 Conclusion Literature Review

The conclusion on the literature review is although there is much written on cyber security for the maritime industry, to the best of our knowledge, there is a limited amount of data and experiences from the maritime industry. Most of the literature is focussed on intentional attacks on informational systems such as manipulation of the ECDIS. The role of physical damage caused by attacks or the role of accidental incidents is not highlighted in the literature. Furthermore, there is limited research done for different organisations involved in the maritime industry. While Kachagias (2022) has examined a case study, this was limited to a single shipping company, whereas the maritime industry is broader that shipping companies. Similar can be said from the study of Erstad (2022), which was focussed on navigators and ship's navigation systems. Although navigation systems are vulnerable systems onboard a ship, there are more systems which can be attacked, such as propulsion control systems and engine control systems.

The studies of Meland et al. (2021) and Jo et al. (2022) give examples of attacks that have happened in the maritime industry and provide a good reference for the possible impact of different attacks. However, although these studies give a good example of the attacks, they do not elaborate what the maritime industry has learned from these attacks and implemented as measures to prevent future attacks.

The literature study also shows that the focus on measurements against attacks are solved mainly in the governance domain. The main driver that is mentioned in the literature is IMO resolution MSC.428(98), which is more a recommendation aimed at operators of ships. The role of other players in the maritime industry is mentioned in the white paper of BIMCO (2021), however, the actions to be taken are guidelines and the main target group of the white paper are ship owners as well.

In conclusion, in order to have a broader idea on what the views of the maritime industry and which onboard systems are vulnerable, literature research is lacking. Therefore, interviews with different players in the maritime sector would be necessary.

3. Research Design and Methodology

This chapter discusses research design and methodology to answer the research question. The main research question is: what is the maritime industry doing to deal with cyber risks on board ships? To answer this question first a literature study was done. Subsequently, the exploratory nature of the research question was suited for a qualitative analysis using semi-structured interviews, which were conducted for specially for this thesis. The interviews were transcribed, which was followed by thematic analysis on those interviews. For the thematic analysis the transcripts were coded, after which the resulting codes were themed and subsequently the themes lead to the results and answer to the research question.

3.1 Research Design

The introduction of the chapter mentioned that qualitative research was done. Qualitative research originates from social studies (Creswell & Creswell, 2018). Additionally Galetta (2013) indicates that with qualitative research it is possible to provide answers for exploratory research. The research question of this thesis has an exploratory nature, therefore qualitative research has been chosen as the research methodology. Quantitative research methods focus on objective numerical data, obtained via a systematic approach, whereas on the other side qualitative methods focus on descriptions and words from a subjects perspective (Palmer & Bolderston, 2006). According to Palmer and Bolderston (2006), qualitative analysis allows the researcher to build theory via asking questions such as “why”, “how” and “in what way”.

3.2 Semi Structured Interview

The reason semi-structured interviews are used is mainly due to the lack of data from the maritime industry for this topic. Semi-structured interviews are a balance between structured interviews, where the researcher processes answers to pre-defined questions and script and unstructured interviews, where there is are not pre-defined questions nor is there a script. Due to the explorative nature of the research question, a structured interview would lead to answers which are too limiting. On the other hand, with an unstructured interview it would be difficult to find a red thread and convergence between the different stories. With semi-structured interviews, the researcher typically defines a set of open ended questions prior to the interview (Passer, 2017, p. 178). The order of the questions is not fixed and during when an answer needs further elaboration during the interview, the researcher can ask more questions to dive deeper into the topic. Semi-structured interviews therefore give the possibility to relate the research questions more directly to the research data, while still providing the own explanation or interpretation of the interviewee.

3.2.1 Sampling Technique

As described in the introduction the maritime industry contains different types of organisations and is divided into five groups for this thesis. The first group are the ship owners and operators of ships, and it can be considered the most noticeable stakeholder of the maritime industry. This group is involved in the day-to-day business of the shipping industry, exploitation of ships and use of ships. The second group are the shipyards, which in general build, convert or refit ships according to wishes and specifications of the owner. This group is also a major contributor which can be directly related to the maritime industry. The third group which is considered are the suppliers of equipment and systems. This group usually provides shipyards with equipment which in turn will be placed on board. This may be suppliers of radars, electronic charts, communication equipment and equipment for other systems. These suppliers are often, but not necessarily always, dependent on other suppliers, which deliver basic equipment, such as routers, PCs, etc.

The fourth group are the classification societies, which ensures that ships are built according to a certain standard. Classification societies set minimal rules which the owners, shipyard and suppliers have to comply with. In case a ship does not comply with classification rules, insurance of a ship will be difficult (i.e., expensive) if not impossible. The final group are the authorities such as the flag states, coast guard and port authorities. This group is focussed on safety of people and sailing areas and imposes rules and regulations to the shipowners. The different groups and the interaction between these groups are depicted in Figure 5. The arrows indicate which parties imposes rules and requirements to whom.

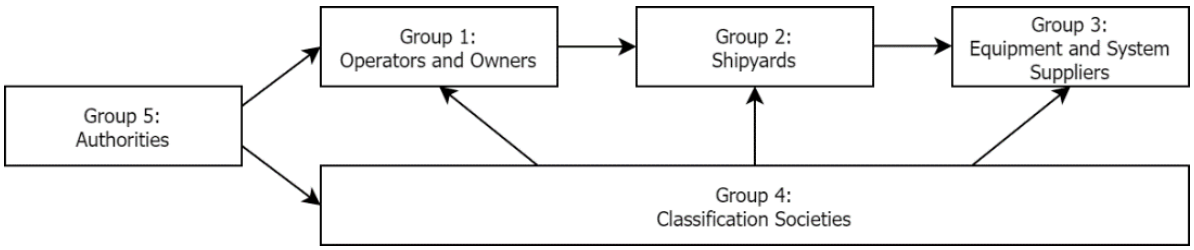

Figure 5: The different groups of actors in the maritime industry and their interaction.

The sample for the interviews is actors from different organisations that are part of the maritime industry. The sampling techniques used for this thesis is expert sampling. In expert sampling researchers identify experts themselves and ask them to participate a research (Passer, 2017, p. 219). For this thesis, experts were chosen by the author, to consider as many as possible of the different types of actors from the maritime industry.

Another sampling method that was used is snowballing. With snowball sampling, people which are contacted to participate are also asked to provide contact details or forward the invitation to other people who meet the requirement for the survey (Passer, 2017, p. 219). For this research, some participants were contacted to forward the request to other experts from their network in order to cover as many as different actors as possible.

3.2.2 Questionnaire

The following questions were considered for the semi-structured interview. The first questions were to establish the demographics of the interviewee and organisations.

1. Can you explain what your organisation does, and how it is related to the maritime industry?
    a. What is the size of the organisation?
2. Can you explain what your role in the organisation is?
    a. How does it relate to cyber security?
3. How long you have been at the organisation at the current role.
    a. What was your previous role at the organisation?
    b. Did you have the same role at a different organisation

These questions were followed by questions related to cyber security in the maritime industry. The questions were based on findings from the literature review. First general cyber security views of the interviewee were asked with the following questions.

4. How would you describe the cyber security landscape for the maritime industry in the last five years.
    a. How have you seen the cyber security landscape change in the last years?
5. What would you consider to be a cyber incident aboard a ship?
    a. Which unintentional cyber incidents would you consider in the maritime industry?
    b. And which intentional cyber incidents would you consider?
6. What are the main challenges for cyber security on ships?

The next questions were questions which are related to cyber security views within the own organisations.

7. Which cyber security strategies are used within your organisation?
8. How would you compare your organisations cyber security strategy to other organisations?
9. What do you consider the major (top 3 / top 5) threats for the maritime industry?
    a. Which systems are the most vulnerable for cyber incidents? (Vulnerabilities)

    b. Which are the main causes for cyber threats? (Attack Vectors)
    c. Which actors are causing the threats? (Adversaries)
10. What does your organisation do to adapt against these threats? (Which solutions, policies, standards etc. are enforced/used)
    a. Which technological solutions does your organisation uses or foresees in the near future?
    b. Which policies does your organisation promotes?
    c. Which classification rules, industrial standards and applicable cyber security regulations (national and international) are used?
11. In case budget would not be a limiting factor, which actions would be taken to enhance the security of a ship?

The last questions of the interview were questions which were a comparison between cyber security on ships and other industries.

12. In which ways are cyber incidents on critical infrastructures on land similar or dissimilar to cyber incidents on a ship?
13. How would you describe the maturity level of cyber security within the maritime industry and how would you compare the cyber security maturity level in the maritime industry compared to other industries?

3.2.3 Location and Interview Set-up

The interviews were held remotely on Microsoft Teams. This has the advantage that the interviews can be held at the moment of convenience for the interviewees. For the interview a timeslot between 30-45 minutes was reserved, however the time was not limited.

Table 2 shows on which date the interviews with which interviewee where held. The table shows also which type of organisation the interviewee represented, and which background the interviewee had at other organisations.

Table 2: Schedule of interviews.

Interviewee	Date	Organization Type	Other Background
No.1	6 December 2022	Classification Societies	
No.2	12 December 2022	Equipment and System Suppliers	
No.3	14 December 2022	Equipment and System Suppliers	
No.4	14 December 2022	Shipyards	Operators and Owners
No.5	15 December 2022	Equipment and System Suppliers	
No.6	16 December 2022	Shipyards	Operators and Owners
No.7	16 December 2022	Classification Societies	
No.8	21 December 2022	Equipment and System Suppliers	Operators and Owners, Authorities

3.2.4 Transcription

The interviews are recorded using Microsoft Teams, after which the recording is then used to transcribe. The way transcribing is done can be represented on a scale with naturalised on one end of the spectrum and denaturalised on the other end (Nicholas et al., 2019). With naturalised transcribing all what is said is transcribed, including hesitation words and grammatical errors. Furthermore, with natural transcribing, the transcriber also adds actions which are taken such as pausing, laughing and sighing. While on the other hand with denaturalised transcriptions, only the essence of what is said is transcribed, meaning that all stop words are deleted and grammatical errors are corrected. Additionally, there are no indications of actions that are occurring, so no indications of pauses, sighing or laughing.

For this thesis the transcription which leans more towards denaturalised transcribing is chosen. The reason is that what is said is more important than the manner on how it is said to answer the research questions. Another reason to choose this manner of transcribing is that denaturalised

transcriptions also match with thematic analysis, which is part of the next step of the research (Nicholas et al., 2019). During transcribing the interviews were anonymised. The names of the interviewees and organisations were replaced with descriptions. For example a the name of an organisation specialised in providing cyber security solutions was replaced into: “cyber security company from the Netherlands”.

3.3 Thematic Analysis

The next step after having the interviews is analysing the obtained data. For this thesis thematic analysis has been chosen to analyse the interviews. The reason for choosing thematic analysis is that it is presented as a structured method of analysing qualitative data as well as a relatively easy manner to interpret this data (Braun & Clarke, 2021; Guest et al., 2011). The thematic analysis that will be done in the six phases of reflective thematic analysis as described by (Braun & Clarke, 2021).

The first phase is familiarising with the dataset, which is in this case the transcripts of the interview. During this phase the transcript will be read and reread, while note may be taken on analytical ideas. The second phase is coding, where interesting parts of the transcript are highlighted and an analytical description, also called a code, is applied to the text. In phase 3, shared patterns are recognised and codes are clustered in themes. This is followed by reviewing and developing the themes in phase 4. Here the relevance of themes is assessed and grouping of themes is done when necessary. In phase 5 themes are refined, defined and named. Each theme is clearly demarcated, and a synopsis is written on the theme. In the last phase, phase 6, all the writing that has done previously is finished and an analytical narrative is formulated.

After the transcripts were completed, ALTAS.ti was used to code and analyse the data. Each interview was represented by a document and each document was assigned codes. After the codes were assigned, the codes were grouped into code groups, which are themes for the thematic analysis.

3.4 Validity and Reliability

According to Leung (2015), the quality of quantitative research can be quantified in terms of validity, reliability and generalization. Validity means that the research process is described, which is done in this study by providing the research methodology which discusses the sampling technique, methods and tools used for this thesis. Leung argues that in qualitative research, reliability refers to exactly replicating the results of the research. For this thesis, some interviews were checked as a form of triangulation and feedback was given to the researcher. Generalisation means whether the research can be duplicated. For qualitative studies generalisation requires the same criteria as validity,

meaning that the process should be replicable and described well. As with validity, generalisation in this thesis is achieved by describing the research methodology as well as checking of the interviews by the researcher's supervisor.

3.5 Limitations and drawbacks

The drawback of having interviews as a data collection method is that interviews have a potential for interviewer bias, and with interviews reliability of the collected data may be questioned due to the lack of structure (Palmer & Bolderston, 2006). With semi-structured interviews it is difficult to remove interviewer bias. On one hand semi-structured interviews are suited to ask in depth information on subjects that the interviewer think are interesting (Palmer & Bolderston, 2006). On the other hand, this introduces a bias towards what the interviewer deems interesting. The interviewer may not be triggered to ask in depth questions, which may be important for the research on subjects that are either trivial for the interviewer or subject that are unimportant to the opinion of the interviewer. The limitations of reliability are usually tackled by asking questions until saturation of the interview occurs (Palmer & Bolderston, 2006). The drawback of this is that saturation is not quantified in literature and could be subjective.

Besides limitation of the interviewing method, there are also limitation due to the sampling methods used. Due to the snowballing method used, the spread of the population is also limited to the network of the researcher. The maritime industry is globally present; however, the interviewees were from three countries in Northern and Western Europe as depicted in Figure 6. This means that the scope of the research is limited as well to organisations located in those three countries. This creates a bias towards socio-technical concepts, which can be expressed in organisational culture, and governance which can be shown in the influence of the European Union and classification societies present in Europe.

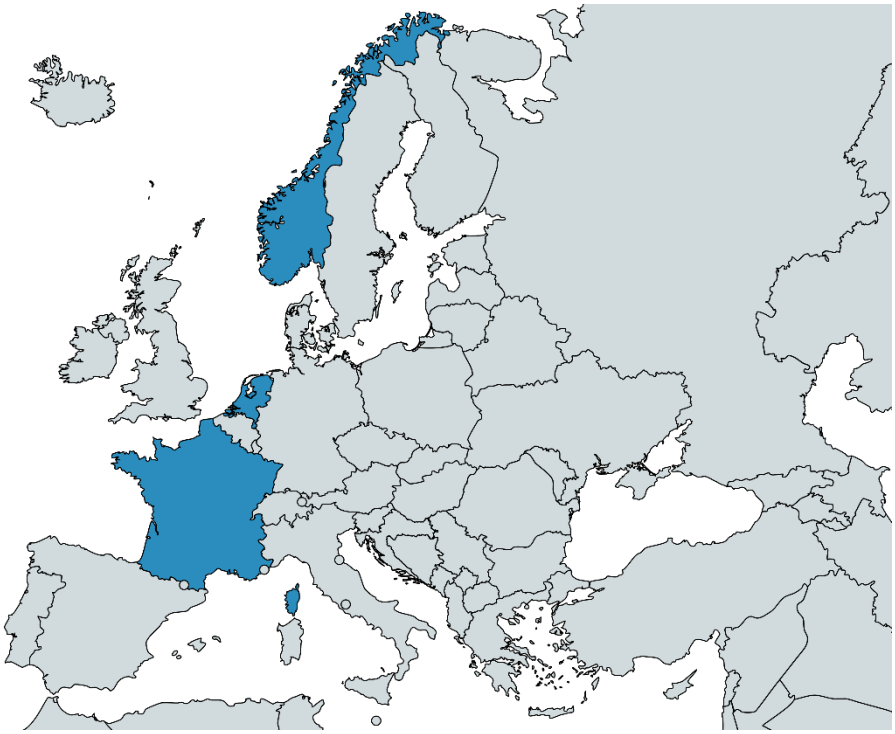

Figure 6: Location of interviewees in blue (created with mapchart.net).

4. Results

This chapter discusses the results of the interviews and thematic analysis. As indicated earlier ATLAS.ti was used for coding and analysis of the interviews. In total 143 different codes were assigned, which were subsequently grouped in 10 themes. On average each interview was coded with 53 codes.

The following themes were extracted from the analysis:

1. Trends in the maritime industry (6 codes) and cyber security characteristics (16 codes)
2. Comparison to different industries (10 codes)
3. Vulnerabilities (26 codes), threats (18 codes) and threat actors (5 codes)
4. Potential Harm (14 codes)
5. Technological Measures (30 codes)
6. Socio-Technical Measures (14 codes)
7. Governance Measures (12 codes)

In this chapter first general observations will be given. These general observations are related to the trends and cyber security characteristics in the maritime industry and comparisons with other industries. The chapter starts with this part to provide the maritime landscape the different interviewees have presented. Next vulnerabilities, threat vectors and threat actors within the maritime industry are presented, followed by measures which are taken.

4.1 Trends in the Maritime Industry and Cyber Security Characteristics

Before diving into the analysis of data related to research question, trends and cyber security characteristics are presented. The trends and characteristics are the views of the interviewees. According to the interviewees the maritime industry is shifting from a disconnected world on board ships, towards a connected world with data collection and remote connections, where highly automated and autonomous shipping is needed.

> *"… conventional ships have been designed to operate as an island, so without having a connection to the rest of the world. And at the same time in the last five years, each and every system provider has been automating and digitalising their products and by having that the opportunity comes to use that skills that capability of the system to get connected to other systems on board, but also to get connected to the shore. And the shore can be the supplier itself or the operator or any other entity." - Interviewee 6*

Although the maritime industry is evolving fast, there are some challenges associated with the industry. The first challenge for cyber security in the maritime industry is that the industry is a complex entity of different stakeholders with their interactions and own responsibilities.

> *"Because it is a complex system and it is okay to be responsible for your own deliveries to that system. But when you get all of these things connected and at different levels and so on, who is [responsible]? Everybody can say they are compliant, but when you can combine so many different systems are they all together compliant when you put it in a system? – Interviewee 8*

Not adding to cyber security in the maritime industry is that the awareness within the industry is low. Although some entities are promoting cyber security and have cyber security solutions, the impression that the majority of the organisations leave on the interviewees is that the level of awareness of cyber security is low.

> *"… the awareness … is shockingly low, with regards to cyber security. We formed … a strategic alliance with … an external company and we've launched some services and products … with regard to cyber security. And we've seen almost zero response to those propositions. Also, in RFQ's that we get from customers or technical specifications that we receive from customers or external parties, cyber security is almost never considered as an aspect in those requests. All those factors make me realize that the awareness about cyber security … is shockingly low." – Interviewee 2*

Although the awareness is low, there are signs that the awareness level in the maritime industry is increasing, perhaps assisted with the IMO regulations.

> *"… there is an increase in awareness that there is a high dependency and increasing dependency on the correct working of their operational technology on board of a vessel, which is also dependent and interconnected to other systems, instead of a standalone system, which they trusted a long time because it was physically separated from the rest so nobody could attack it. The awareness about the threat is only increasing." – Interviewee 5*

> *"In the last five years we really have seen the adoption going from the state of a plain antivirus to endpoint security and also adding unified threat management as well to the*

vessel. Especially for the last two years. That's a major leap and I think that it is especially coming from the IMO 2021 regulation that's in place." – Interviewee 3

Still one of the main characteristics is that there is a passive attitude in the maritime industry regarding cyber security.

"There is a passive attitude in the maritime industry regarding cyber security." – Interviewee 3

When the maritime industry is compared to other industries or critical infrastructures, there are differences as well as similarities observed. The differences have to do, among others, with the bandwidth available at ships as well as the knowledge available from the crew on the ship. There is usually only a single connection to the outside world, which is also limited in bandwidth. This means that solutions which work in other industries are not always applicable to the maritime industry.

"[Translating those requirements to a ship] is more a challenge than we can think. It's not something that we say, 'Okay, I've done it on shore, I have quite secure.' Of course, the level zero risk does not exist, but you say, 'Okay, onshore I have some solutions.' Well, they are not transposable to a ship because there is a challenge, there is the bandwidth issue that makes that the monitoring real time is not possible. As simple as that. You do not have on the field experience, you hardly have a cyber expert on board." – Interviewee 7

Due to the nature of a ship, which is a floating and moving object, a cyber incident on a ship has a different impact, compared to land-based industries which are much more static.

"For a land-based company, it would be more maybe getting access to information and so on. Or the disrupt operation of that company. But … a vessel is a moving object, and you can keep the vessel as a hostage, and you can also cause the vessel to cause damage to a third-party object."- Interviewee 8

Another difference is that the level of cyber security in other industries is considered higher than the level of cyber security in the maritime industry. This provides the maritime industry with the opportunity to learn from other industries and apply it to the maritime industry, as long as the differences are kept in mind.

"Nowadays you more and more see that there is a separate domain the cyber security for an operational technology, which is significantly different than an IT environment. But it also becomes its own expertise domain, which makes it a lot more easier to have the right

discussion for instance, also for us with our customers. I know now that maybe about three years ago when I just started over here, I had some discussions with customers. But I had a discussion with an IT security [expert]. So, then they come up with a lot of security measures, [for instance], that the system should lock after 50 minutes inactivity. That is perfectly fine for your desktop environment. However, the commander on the bridge looks at his radar, but he's not going to operate the radar system itself. So, from a system perspective, it's idle and if he loses his radar image after 50 minutes. … They didn't understand it and so that was a lot of discussion and struggle in the beginning. [While] nowadays you see, that they understand the difference in the systems on board of the vessel, and the discussions also become more easy and then you can also have much more a risk based security measure selection." – Interviewee 5

"What we did is that we involved companies from outside the maritime industry, because they are already at a higher level, so adopting their principles, their methodologies, their solutions make it much easier, faster to get on a good level of being becoming professional." - Interviewee 6

Although there are differences, there are still similarities that can be observed. The similarities are related to the threats and the technologies used on board ships and for critical infrastructures. In healthcare and for critical infrastructures, there the same protocols for OT equipment are being used. When the OT grid and the IT grid are connected, it would lead to similar vulnerabilities. There are similarities in threat actors as well, both the maritime industry and other industry have to deal with similar state actors with similar end goals.

"… for a naval ship, we are talking about a ship that's to be used in a war. So, the attacks are different. But when you're now looking to the Ukraine and see what the hackers has tried to disrupt, the energy centrals, it's similar, … that's … war as well. – Interviewee 4

"The similarities are that big that … it makes sense to make use of their knowledge, their expertise, and implement it in … maritime applications." – Interviewee 6

"All of the systems we know have caveats. … For instance, the healthcare architecture is also [a cyber security topic]. … In the US we saw recently that the critical infrastructure … were also not in his best shape and need investment." – Interviewee 7

There are similarities with the healthcare industry specifically. The similarity between the healthcare industry and the maritime industry is that both of these industries depend heavily on regulations.

Other than that, both of the industries have a slow adoption rate of IT and make use of legacy operating systems. In the healthcare industry there is a path for obsolescence and upgrading is more aligned with the provider of the operating system, while in the maritime industry this is not the case.

> *"They have a slower adoption in IT and they have the same, well, not the same, but the similar regulations as well, similar procedures." - Interviewee 3*

4.2 Vulnerabilities, Threats and Threat Actors

This section is focussed on the vulnerabilities, threats and threat actors which are present in the maritime industry.

4.2.1 Vulnerabilities

There are several vulnerabilities onboard ships which have been mentioned. The main vulnerability which is mentioned the most is the lack of awareness within the maritime industry. Lack of awareness of cyber threats is considered one of the most vulnerable parts of cyber security within the maritime industry.

> *"It all starts with awareness. I think that's the main challenge. To get the responsible crew of a ship or the management company of the ship to be aware of any cyber security risks and how to treat them in a proper manner." – Interviewee 2*

> *"The awareness is lacking a little bit on the implementation of remote monitoring, remote access." – Interviewee 6*

With lack of awareness being one factor, a related factor is lack of skills. The trend to have as much automated as possible aboard ships stems from the need to sail with less personnel. This is partly due to the higher complexity of ships, and the lack of personnel. This is the same for the lack of personnel with a cyber security background. On ships there is simply a lack of people with this specific background to tackle as the possible cyber security issues that may occur.

> *"One of the challenges … in the near future, is to sail with less manning. … [The goal of a current programme] is to think about [IT and automation], so you can sail with less crew." – Interviewee 4*

> *"Most of the time it's not about even money, but skills, and that is something that I think is still a challenge today." – Interviewee 7*

The lack of budget can also be seen as a vulnerability. Ship operators do not assign sufficient budget to for example perform relatively simple updates. By not assigning budgets, ships are sailing with outdated equipment and are therefore vulnerable for cyber incidents. This can also mean that ships are sailing with outdated operating systems.

> *"We have so many customers that don't have an IT budget. That just say: "We need that solution and we will mingle it in this budget somewhere." – Interviewee 3*

Another often mentioned vulnerability is the single connection to the outside world. Onboard ships, there are many systems which operate simultaneously and have different requirements regarding cyber security. Although networks such as the bridge equipment network, the propulsion network or the welfare network, have different requirements, they are usually interconnected with a single access point to the internet. Looking deeper into the different networks on board a ship, it shows that the welfare network is considered a vulnerability as well. The main reason the welfare network is considered a vulnerability is not only that behaviour on this network is unpredictable, on this network people often use their own personal devices.

> *"But as soon as there are users involved with their own applications or mailing and websites or media. Then it becomes unpredictable, so it becomes very hard to determine normal behaviour." – Interviewee 5*

The last vulnerability, which was mentioned, is that ships are built at a certain time, with certain technology that is available at that time. During the lifetime of a ship, technology in the world changes, however technology on board the ship stays the same. When a ship is being refit or updated during its lifetime there are design limitations to the systems which are related to the time of installation of the systems during building of the ship.

> *"The ships which … are now sailing, … are 15-20 years old or older and so it is very difficult to implement the cyber security requirements in those ships." – Interviewee 4*

> *"Because all the legacy systems were not built with security in mind. They were mainly built with a safety objective in mind and on the … assumption that they will never be interconnected with other systems. They lack any patching, they lack any form of authentication or whatever, so that they have pretty open systems. However, if they are standalone then they still stand alone. But I see that they are getting connected anyway, so that would be the most vulnerable system." – Interviewee 5*

"The conventional networks on board are not designed to deal with these kinds of threats. So, the communication is normally open, access to the systems is quite open. Which, was okay, because everybody on board was there with a permission. But that's changing. I think that's one of the biggest challenges. We have a little bit of legacy or maybe quite a lot of legacy of system developments which are becoming good and being smart and being interactive, but the companies which have designed and build them were not used to also take into account the cyber security risks." – Interviewee 6

4.2.2 Threats

The previous section has discussed the different vulnerabilities that the interviewees see in the maritime industry. These vulnerabilities can be exploited, which is a threat. The main threat recognised by the interviewees is people gaining unauthorised access to the ship's network, data or devices.

"Any unauthorized access to a network or a device could be considered an incident, I think." - Interviewee 2

"To me, when there is a cyber incident, it means that there would be access or access to data, access to ship systems without having wanted it to occur. So, if it's without any deliberate access accidentally or maybe a little bit more hostile, if there is an intruder." – Interviewee 6

"I don't like, somebody getting access physically through getting an open network port or something where they can get access to something that they shouldn't have." – Interviewee 8

Not only is gaining access to networks, data or devices a threat, making devices unavailable is seen as a threat as well. A common method of making devices unavailable is by overloading the network where the devices are communicating in. Because systems are dependent on communication of devices, this leads to unavailability of systems. Besides overloading networks, communication can also be disrupted by having interference of devices over communication lines.

"The worst scenario we experience is that we get a DDoS attack. And that brings the onboard systems down. So that is for us the most dangerous attack. … Military is about communication and data exchange. So, if you do a proper dumb DDoS attack, you bring the communication down." – Interviewee 1

"The problem is that when you have an infected machine it can just overload the connection and then you get timeouts." – Interviewee 3

"There could be already some interference between systems because the new way of communication has not yet been evaluated when it is fully integrated. So, systems can communicate more, but it can also make some interference between systems." – Interviewee 6

"There are probably access points, that could confuse the system, making it this whole system being crashed." – Interviewee 8

The final threat that is mentioned by the interviewees is malware. Malware can be introduced in many ways, where an infected USB stick is mentioned the most. The malware can be a virus, spyware, software which performs a firewall or network scan or even just software that broadcasts in the network and overloads the network.

"A firewall scan, that's an incident. …That can be just … a rogue application or an application broadcasting in a network." – Interviewee 3

"Because what has happened now, to update an ECDIS machine, they go with an USB drive from a ship's network … to the ECDIS machine; plug in the USB drive and if the USB drive is infected, it will infect the ECDIS machine." - Interviewee 5

Specifically related to the maritime industry are spoofing and jamming of GPS, GNSS and AIS signals. This threat is mentioned in the literature survey as well. Although, from the literature survey much emphasis is put on these threats. The interviewees consider it as a threat; however, they consider other threats more urgent.

"There is a common set of attacks that we always consider when assessing the risk. There is the well-known … spoofing and jamming of the various equipment onboard, [such as] GPS, GNSS, [and] AIS." – Interviewee 7

4.2.3 Threat actors

The interviews show that the threat actors of the maritime industry are no different from the threat actors in other industries.

When you talk about the actors, I see the state actors, the non-state actors like script kiddies, hackers and disgruntled employees/employers. That is top 3 of treats. And in

addition, any member or staff, regardless of rank or function intentionally or not, or unintentionally pose a threat by ignoring or circumventing cyber security measures procedures. So that makes you vulnerable for all your systems. – Interviewee 4

4.3 Harm

Harm caused by cyber incidents to society via cyberspace is divided into the four types of harm of B. van den Berg and Kuipers. The interviewees acknowledge that there is a distinguishment between intentional and unintentional threats. First there is unintentional informational harm in the maritime industry, the interviewees acknowledge that although unintentional, it can still be considered a threat. These threats are mainly caused by personnel which misuse the system to make their life easier. This includes bypass actions, where the user knowingly misuses the system, however unintentionally causes harm.

"There are a lot of events in the sense of that they are still misusing the system in a way which was not intended to be used… [That] becomes a cyber incident… [We] have for instance a staging system for deployment of our new update, but [the users] don't use it. They just walk around with the [organisation's] USB stick and because [the USB-ports are] still enabled, … they can just upload their own update locally. For me that's an incident…"

"They don't tend to abuse the system, to disrupt the system. They use the system to make their life easier." – Interviewee 5

There is also unintentional harm to systems, where users disrupt important systems for ship operation. Disruption can be due to misconfiguration of communication lines, but also due to overloading the satellite connection.

"The people on board made a mistake and actually hacked the ship themselves. They were not aware that they did that. They couldn't even control [the ship] locally anymore because everything got locked up… "

"If you swap T and S on the communication lines, you can lock up complete computer systems. Even redundant versions." - Interviewee 1

"For example, a customer was complaining about a slow connection and then we monitored the connection and there [was] nothing really special on it. But … [someone was] looking at a webcam back home. So that was slowing the connection." – Interviewee 3

Similarly, there is intentional informational harm as well as intentional system harm. Intentional informational harm can be related more to data theft. With intentional system harm, various systems on board the ship can be tampered with and can disrupt the safety of the vessel. Intentional informational harm does not have to be necessary on board a ship. By providing software that translates documents, a threat actor can receive data from naïve employee and process that data for its own needs.

> *"If you go on the darknet, then there is a facility where you can see all shipping, and you can see the interface on the ship and an IAS position coupled so you can check which ship it is. There is software on the market, if you use that, you have directly access to all the technical data transmitted over the lines." – Interviewee 1*

> *"Kingsoft is spyware plug-in and it's being used in translation programs. What does it do? You want to have your documents translated. The captain puts it in the software, the software sends it up to the Internet, and the servers are in China. You will get a nicely translated document back, but your document will be in that cloud. That's something that I don't really don't realize. They're giving all their information for free just to get it translated. That's something that the maritime industry still doesn't understand. 'But I get my translated document.' 'Yes, but you are giving them viable information which can potentially be used against you.'" – Interviewee 3*

The last category of harm is intentional harm to the physical world. According to the interviewees, this occurs when threat actors are intentionally tampering systems on board the ship.

> *But for a targeted attack, as a state actor would typically be doing, maybe the likelihood is slightly lower because we tried to protect the system from those type of actors. But the intent is much more hostile. So, they would typically disrupt the entire system if they want to." - Interviewee 5*

> *"If you succeed into achieving such a jump [from the IT space to the OT space], then having malicious attacks that could jeopardized the ship safety, it's quite easy." – Interviewee 7*

4.4 Measures

The measures which are derived from the interviews can be divided into four different types of measures. First there are the technological measures, which are related to different technologies used in the maritime industry. Next are the socio-technical measures, which describe measures to make the combination of people and IT-systems more cyber secure. Then there are the governance

measures, which relate to standards and rules. Finally, there are holistic measures which are related to the combination of the technical, socio-technical and governance measures.

4.4.1 Technological Measures

On a ship there are many different networks, which have different requirements for connectivity. The OT systems need less connections to the outside world compared to the welfare network. From a technological point of view the most mentioned solution is having proper network configurations and network segregation. With proper network configurations, the OT and welfare networks are properly segregated and the interdependencies are limited.

> *"That's one of the major things which often is still forgotten by the ship owner. If they have a proper IT network and correctly configure it, they will also lower the amount of threats that are entering the network." – Interviewee 3*

> *"[Proper system and network design starts] with having a good quality, robust network by itself, having the basic elements applied to make sure that interferences are handled and not possible. And, starting from the quality of network, building up the functionalities which needs to be running on the network and having a clear definition of responsibilities, accountabilities." – Interviewee 6*

After the network has been properly configured it is important to keep an eye on the state of the network and check whether there are no anomalies. The maritime industry incorporates network monitoring tools to fulfil this function. Not only should there be network monitoring, there should also be alarming and an advice for actions to be taken.

> *"Network scanning tools that expose any potential vulnerability with recommendations how to solve them but also real time monitoring of IP packets, packet inspection and monitoring when connections for any threats and alarming on them." - Interviewee 2*

Socio-Technical Measures

Socio-technical measures are mainly shown in different policies that organisations have. One of the most frequent mentioned measures is having a proper update policy. By keeping software up to date, bugs and leaks are fixed and the probability that threat actors will be able to pose a threat is reduced. This includes the use of the latest operating systems. As mentioned before, a ship contains different suppliers, with their own equipment. Which means that there is a possibility that there are different computer systems and even operating system on board. An important factor mentioned by

one of the interviewees is to make sure that there are as little different systems on board as possible to keep maintenance as easy as possible.

> *"Update all, make sure your IT equipment is standard. It's unmanageable to have like six different desktop systems. … [Update] all. HP, Dell, whatever brand, make sure they're updated." – Interviewee 3*

> *"It comes down to also the connectivity …, to have more patching and update frequently available on the infrastructure." – Interviewee 5*

On ships, there is crew turnover and there are shifts of different crew. A socio-technical measure to enhance cyber security in the maritime industry is to have proper user management. Preferably user management and access should be as simple as possible. Proper user management means that first a user should be validated prior to even gain access. Then, only access to certain parts of the network should be granted to users that need it. Furthermore, there should be reporting on which actions are taken by which user. Finally, when the user no longer need access, it should be revoked. Users are not fond of remembering different passwords for different systems, therefore, to make the life of the user easier and to limit security bypass actions by the users, user management should be user friendly.

> *"For instance, well what we did is, we centralized our whole user management and our account management. So instead of that they have to remember passwords for each system they have just one username, one password for all the systems. But still, it's a username password and they tend to hate that. I would like to make that a lot more easy for them." – Interviewee 5*

> *"First of all, whenever there is granted access to a ship in real life conditions, then I would call the captain if I'm allowed to go on board and then he will ask me to identify myself because before I accessed the vessel and I think in the cyber connection it's the same: Identifying whoever you are, getting permission to access the network and once you access the network, having restricted access to only those systems or those parts of the network where you have to do a job. And when you are finished with your job, normally you would report to the captain in real life, what did you do? What did you change? And I think this should also be done in the cyber security world, in the cyber security access. So, logging whatever is being changed, updated and reporting these changes and updates. And when you are finished, I think in the real-life world you will ask the captain to go off the ship. I think in this case it will be the same and if you are not active on the network, I think by*

default, your permission will be discontinued after some time of not using the connection and so these kinds of processes, needs to be in place." – Interviewee 6

As stated earlier, there is low awareness in the maritime industry and the appropriate budget is not always allocated. One of the interviewees has provided a method to raise the awareness and to keep the budget in mind for cyber security solution. The methods the organisation of the interviewee uses, is providing incident reporting, which shows what the impact of a cyber-attack might have been. By showing the benefits that cyber protection tools have, the organisations shows that the budget for cyber security tools are relatively low and that it is a must to allocate the budget.

"If a vessel can't sail away and have to stay at additional day in port, you will have earned it back. That's the thing. An additional port stay at the port of Rotterdam is somewhere between the $50,000 to $100,000 a day. … If you only have to stay an additional day, you will have your cyber security for the next three years free of charge basically. … That's one of the reasons why we have those reports saying: 'OK, we are saving money for you.' We're not calculating any additional port days that you have to have to have to do for this. But just giving them a ballpark figure, saying: 'this month you save $6000 because you had so many infections that they were blocked.'" – Interviewee 3

Governance Measures

In the maritime industry, different governance societies play an important part. From top down, it starts with the IMO, which provides rules for safe shipping. As stated in the literature study, IMO Resolution MSC.428(98) has been applicable since 2021. The IMO is followed by the IEC, which provides standards for electrical equipment. For cyber security IEC 62443 is applicable. Then there is the International Association of Classification Societies (IACS[1]), which in turn provide more details based on the rules of the IMO and the standards of the IEC, these are the unified rules (UR) E26 and E27 and will be mandatory from 2024. Finally, there are the classification societies, where in the recent years, classification societies have started to write rules regarding cyber security. Classification societies have combined IMO rules, IEC standards and IACS rules into their own rules and standards. The rules and standards that classification societies set up are a minimum a ship should comply with. Approval from classification societies play an important part in the maritime

[1] Note that IEC 62443 uses the acronym IACS for industrial automation and control systems (International Electrotechnical Commission, 2010). In this thesis, this acronym is only used for the International Association of Classification Societies. For industrial automation and control systems are referred as industrial control systems (ICS).

industry. A ship can receive the notation Cyber Secure when it is built according to the respective classification rules.

> *"So as such we have class notation for ships which match the IMO guideline. And then while we can speak about the IMO guideline, this is the first step. Of course, this is not sufficient because there are no technical requirements, but this is the first step and the goal of [organisation], is to provide a way for a ship owner to be compliant with that rules and certify This was the first step and then we have I would say in [our new rules from 2020] more advanced requirements for ship owners that want to tackle the cyber security issue at the design level and make some efforts into technical implementations [in the cyber secure class notation]. And in that requirement, we do include very demanding requirements on for instance the way you operate a remote access to the ship. Even at a system level. What does this remote access serve as a purpose? Is it telemetry, operation, management of the system? And depending on this mode of communication we define requirements that can go of some basic techniques such as VPNs to I would say very advanced technique with Bastion and Bastion host and DMZ implementation and to prevent malicious activities from those remote access and then of course a lot of network rules etc. And as you may know those requirements are evolving with the introductions in 2024 of the [IACS rules] UR E26 and E27." – Interviewee 7*

Shipyards and suppliers of maritime equipment have to ensure that the equipment that they put on board a ship compliant with the requirements from the customer as well as classification societies. The shipyards and shipowners do not only have to be compliant with classification rules, there are also rules from the owner, which are important.

> *"What we do is to make our products incorporate cyber security. We integrate cyber security measures in our products. … What do the different standards say and how can I translate that to cyber security functions that can be implemented in applications or can be provided as a common service to the applications or can be integrated in the infrastructure itself?" – Interviewee 5*

> *"The shipyards [and integrators] have to make sure that at the integration time, … the initial configuration in which the ship is delivered, is still in conformity or in compliance with regulations." – Interviewee 7*

Holistic Approach

In order to have a cyber secure maritime industry, it is not enough to focus only on one aspect of security from the layers. The combination of the different factors over all the different layers is equally important. Therefore, the holistic approach, meaning that cyber security for the maritime industry should focus on the combined measures from the layers of the model of cyberspace should be considered.

> *"… cyber security is much broader than technology alone. It has also a lot to do with awareness of the people using the systems. It has to do with the policies. It has to do with a lot of other aspects that are not directly technology related …." – Interviewee 2*

> *"You have to look at from the entire spectrum saying if you want to do cyber security, it's not only installing endpoint security, it is not only installing a UTM, it's also taking care of your workstation. Make sure that you have Windows 10 installed or Windows 8.1 with all the updates. Make sure that that's fixed and then apply your cyber security. Because if you have a boat and the engine represents cyber security and you're drilling holes in, it will still sink. That's what they basically are doing. Cyber security can only protect you up to a certain level." - Interviewee 3*

Analysis of the interviews have shown that not only should the different layers be considered. It is equally important to involve the different players in the maritime industry with cyber security aspects. Not only should the owner or end-used be involved, it is also important that the shipyard, classification and other parties are involved.

> *"… cyber security is a much broader aspect than only technology. To give an example we can secure a Wi-Fi network pretty heavily by using passwords and maybe even MAC address authentication and other technological methods to put in place. But if a boat does not have proper policies for crew turnover for example, and do not delete an account of a crew when the crew member leaves the boat, then you would still have a very high security risk, although the technology itself is in good order. So, we can only bring a piece of the puzzle, which can never be completed without the other aspects which also need to be considered. This starts, I think, with awareness which can be triggered by regulations like IMO and Lloyds. Since a year now there's basic cyber security aspects already considered in IMO regulations, and even then, still we do not get any, or almost any, proactive questions or inquiries from any of our clients or potential clients." – Interviewee 2*

Finally, an important aspect of the holistic approach is there is a need to assign the responsibility of cyber security to a single party. This single party has the responsibility to connect all the different systems together and ensure that the complete ship is cyber secure.

> *"If you had one entity responsible for this whole system, you can also do testing and you have somebody to point towards if something fails. If nobody is to have the total responsibility and you start doing testing and something fails and it fails in a kind of a grey area where it could be several stakeholder's fault, then the pointing game will start. And that was also an issue when we started getting more automation and so on board the ship. 'Something failed, we don't know why, it is probably you.' 'No, my system is okay, it is probably you.' So, when you don't have anybody having the total responsibility, you always get the finger pointing. … But I think it's important, and I think there is room for somebody to take that responsibility and the system integrator could be somebody that would take such responsibility. They already are connected to most of the ship systems, so it would be a good starting point to do." – Interviewee 8*

5. Discussion and Conclusion

This chapter contains the discussion and conclusions of the thesis. First the findings from the interviews will be summarised. This is followed by answering of the research questions. Next a conclusion will be made which discusses the limitations and recommendations for future work.

5.1 Findings Summary

In academic literature there are many examples on cyber security threats and measure on board ships and in the maritime industry. However, the literature does not indicate how the maritime industry is actually dealing with cyber security. The interviews have given an image of cyber security within the maritime industry. This section will briefly discuss the similarities and differences between the interviews and the literature survey.

5.1.1 Vulnerabilities

The interviewees have mainly indicated the same vulnerabilities as the literature study. In the literature, the navigation systems and mainly the ECDIS was mentioned as vulnerable system. In the interviews these systems were mentioned as well. The main difference between the literature and the interviews is the level of awareness in the maritime industry. The interviewers have indicated the level of awareness in the industry is relatively low. Only the previous research of Canepa et al. (2021) has mentioned awareness training. Another difference between the literature survey and the interviews is that in the literature survey there was much focus on IIoT devices as vulnerability. In the interviews IIoT devices were not mentioned.

5.1.2 Threat Vectors

The interviews have indicated the same threat vectors as the literature survey. Although not described in this thesis, the literature used for the survey went deeper into the different threats the maritime industry is facing. The threat vectors were mentioned in the interviews; however, they were described by the interviewees at a higher level.

5.1.3 Threat Actors

The interviews have shown the same threat actors compared to the literature survey. The interviewees distinguish between unintentional internal threat actors and by-pass threat actors, which are threat actors who are intentionally by-passing security, however unintentionally causing a cyber incident. In the literature survey this distinguishment for the internal threat actors was not made. By making the distinguishment, it shows better that although by-pass threat actors cause a threat unintentionally, they by-pass security intentionally.

5.1.4 Measures

As technical measures, the interviews mentioned network segregation often. In the literature survey, network segregation was not mentioned as a primary technical solution. The reason could be that the literature assumes incidents when proper network configuration is in place. Similar for socio-technical measures, in the interviews update of systems are mentioned, where in the literature survey this was not the case.

The literature study has indicated that the main driver for governance for cyber security in the maritime industry is are regulations from the IMO. In the interviews the IMO resolution was mentioned as well. The interviews went a bit deeper into other regulations that are emerging, such as the UR E26 and E27 from IACS.

5.1.5 Results

Looking at the interviews and the literature survey, it shows that in general these two have similar results. However, the interviews are going less deep into the cyber security issues and measures compared to the literature. The reason for this is that for this research a semi-structured interview with broad questions were chosen, which is linked to the broad nature of the research question.

5.2 Research Questions

The goal of the interviews was to answer the different research questions and the main question. In this section the answers to the various research questions following from the interviews will be elaborated.

5.2.1 Research Question 1

Which intentional harm is foreseen for physical damage and information damage and what are the vulnerabilities, attack vectors and main adversaries?

Intentional harm is mainly cause by state actors and non-state actors. State actors have the goal to disable ships, and are therefore more likely to attack the onboard OT systems. The goal of an attack for the state actors is more to ground a ship or disable communication. State actors would most likely use the navigation and communication systems and spoof or jam GPS signals. In order to ground a vessel, state actors would disable propulsion systems or other essential systems

For non-state actors, the goal is not necessarily to disable the ship, but to gain information or money. A cyber incident from non-state actors would mainly be for fraudulent purposes such as ransomware or to get data from crew, passengers or shipping companies.

5.2.2 Research Question 2

Which unintentional harm is foreseen for physical and information damage and what are the vulnerabilities and causes?

For unintentional harm, the contributors are mainly crew on board a ship, who bypasses security measures to make work easier. It may also be personnel who access systems they should not access which included uploading of documents for quick translation.

5.2.3 Research Question 3

For the technological layer, which technological solutions are mainly used or upcoming to achieve a cyber secure ship?

For the technologic solutions, many interviewees have indicated that they can use solutions which are available in the market. This means that they can use malware detection and hardened equipment for instance. However, the complexity of a ship's network comes with the combination of different equipment. The main technological solution is therefore to have a proper network configuration, with network segregation. On a ship there are different networks, where all these different networks have a single connection point to the outside world. It is therefore important to properly segregate the different type of network and make it for instance impossible for user on the welfare network to access the network of the propulsion systems or the navigation network.

Together with proper network configurations, it is important to monitor the network and raise alarms in case there are anomalies. This would require network monitoring tools and intrusion detection.

5.2.4 Research Question 4

For the socio-technical layer, what are the policies that organisations use or going to use to achieve secure networks?

The interviews have shown that awareness in the maritime industry is low, especially when compared to other industries. The first step into securing ships and the maritime industry is therefore to raise awareness with the crew and within the industry. By raising awareness, budgets for cyber security will increase as well as an increase of knowledge within the industry. Using expertise from other industries help in improving cyber security solution on board ships, however it is important to keep the differences between OT systems on board a ship and IT systems on shore in mind.

Another socio-technical solution is to have proper user management. The first step is to provide an easy way to access different systems such as by having single sing on for different users. By doing this, users do no longer need to share passwords for different systems and there will be less passwords written down at workstations, shared or saved in text files.

Other that these measures it is also important to have proper updates of computer systems. This means that during building of the ship, it should be taken into account that cyber security requirements can and probably will change. This means that there should be an update policy and systems on board should be kept as uniform as possible.

Looking at the socio-technical measures, it can be concluded that these are no different from measures in land-based industries. The difference in the maritime industry is that the industry is lagging behind other industries.

5.2.5 Research Question 5

For the governance layer, which classification rules, industrial standards and applicable cyber security regulations (national and international) are used?

From a governance point of view the most important driver in the maritime industry is IMO Resolution MSC.428(98), which forces ship owners to have a cyber risk management procedure. An important industrial standard is IEC 62443. Based on these two standards IACS has adopted two new requirements, UR E26 and UR E27, which will come into effect from January 2024. As a consequence of these rules and standards, classification societies have updated their rules as well and have incorporated notations related to cyber security.

Although there are governance rules which have been introduced for the maritime industry in the recent years and for the coming years, these rules are covering basics and are not too demanding. The reason for this is to enable a basic form of cyber security which can be implemented for all ship owners. If the requirements would be too strict, ships would not be able to comply and might lose their insurance.

5.2.6 Main Question

What is the maritime industry doing to deal with cyber risks on board ships?

Looking at the research questions, the main research questions can be answered. The main conclusion is that the maritime industry is lagging behind other industries. However, there are changes going on in the industry to change this. Slowly the maritime industry is realising that cyber

security is an important aspect of their daily business as well. Due to the many different actors involved in the maritime industry, there is a need for clear requirements and responsibilities. This starts with international organisations and classification societies, which have rules and standards the maritime industry has to comply with. Other than that, it is important that the ship owners enforce requirements during building of a ship. Finally, there is a need for a party to check whether all the systems on board delivered by the different suppliers are collaborating in a correct manner.

5.3 Limitations

As indicated previously the first limitation is the location of the organisations selected. Most organisations were located in the Netherlands, while one organisation was located in France and the other in Norway. The maritime industry is a global industry; therefore, the selected countries might give a North-Wester European approach to cyber security instead of a global approach.

The second limitation is that the sample sized studied in this work is limited (only 8 interviewees), due to the time limitations of the thesis schedule. To have more reliable data from the interviews, it would be desirable to conduct more interviews until the coding process is saturated, meaning that no new concepts emerge from new interviews.

The third limitation is that there were no people from organisations willing to cooperate in a recorded and transcribed interview from Group 1 (owners and operators) and Group 5 (authorities). Although there were interviewees which could give their experience from previous roles, the actual state of those groups might be different.

Although we attempted to limit bias as much as possible, interviews can never be considered completely unbiased. With verbal and non-verbal communication, the researched might have triggered certain answers from the interviewees.

Furthermore, the researcher has never performed semi-structured interviews before. Another researcher with more experience in semi-structured interviews would have used different interviewing techniques, and perhaps get more in-depth information from the interviewees.

Finally, the last limitation is related to validity, reliability and generalisation. The thesis is considered work of an individual, therefore although the research steps are described and some interviews have been checked, there is still bias from the researcher towards the topics discussed and the coding and themes applied to the interviews.

5.4 Conclusion

The conclusion is that cyber security measures in the maritime industry are lower compared to other industries. The maritime industry is lagging; however, the situation is changing and the industry is trying to keep up with other industries. The reasons that the maritime industry is changing to become more cyber secure can be found from the three layers of the model of cyberspace.

From a technical point of view, the systems in the maritime industry have changed significantly in the last few years. Where the systems on board used to be separated, now the systems are interconnected and sometimes even have high speed internet connections.

From a socio-technical point, awareness is increasing in the maritime industry. This has to do with the increase in cyber-attacks, as well as with the increase of security policies. The skills of people are increasing as well, where cyber security used to be for people with a purely IT background, it is now seen that the people have an IT and OT background and understand the maritime industry better.

The main driver for cyber security in the maritime industry comes from the governance layer. Be setting rules for 2021 from the IMO and 2024 from the IACS, ship owners are forced to deal with cyber security and risk management. In turn classification societies in combination with the ship owners force the yards and ultimately the suppliers of equipment and systems to have cyber security incorporated in their products as well.

In the end it is not sufficient to focus only on one part of cyber security or one actor within the maritime industry. The recommendation is to use a holistic approach, meaning that technological, socio-technical and governance solutions must be applied by all the players in the maritime industry, being the shipowners and operators, the ship yards, suppliers of equipment and systems, the classification societies and last but not least maritime authorities.

5.5 Future Work

For future research the following points from this research can be elaborated on:

- The research in this thesis was limited to parties in the maritime industry in Western Europe. For future research it is interesting to have views from other continents as well. It would especially be interesting to see how Asian port authorities or shipyards see cyber security in the maritime industry and in their organisation. By looking at interviews from other continents the number of interviews would increase as well, which improve the work and could lead to saturation of the coding process.

- There were no shipowner or operators of ships interested in participating in the interviews. Two of the interviewees, had a background as operators and provided information related to owners and operators. However, it would still be interesting to see how they view cyber security in the maritime industry, especially with the upcoming E26 UR E27 rules from IACS.
- The researcher had no previous experience with interviews as a research method. For future research, there would be fewer general questions, and more questions in depth on the different solutions that the industry needs or provides.
- In order to achieve better validity, reliability and generalisation, for future research looking at the problem with a team of researchers and perform the analysis of the interviews as a team would be recommended. By doing this, better triangulation is achieved.
- The last item which would be interesting for future research is focusing the interviews on an attack scenario using the MITRE ATT&CK framework. By focussing on each stage of the framework, the different measures might be prioritised differently by the interviewers.

References

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

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, *111*, 102490. https://doi.org/10.1016/j.cose.2021.102490

BIMCO. (2021). *The Guidelines on Cyber Security Onboard Ships* (Vol. 4). https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

Braun, V., & Clarke, V. (2021). *Thematic Analysis: A Practical Guide*. Sage.

Canepa, M., Ballini, F., Dalaklis, D., & Vakili, S. (2021). Assessing the Effectiveness of Cybersecurity Training and Raising Awareness Within the Maritime Domain. *INTED2021 Proceedings*, *1*(98), 3489–3499. https://doi.org/10.21125/inted.2021.0726

Creswell, J. W., & Creswell, J. D. (2018). *Research Design: Qualitative, Quantitative and Mixed Methods Approaches* (5th ed.). Sage.

de la Peña Zarzuelo, I. (2021). Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue. *Transport Policy*, *100*(October 2020), 1–4. https://doi.org/10.1016/j.tranpol.2020.10.001

Dhirani, L. L., Armstrong, E., & Newe, T. (2021). Industrial iot, cyber threats, and standards landscape: Evaluation and roadmap. *Sensors*, *21*(11), 1–30. https://doi.org/10.3390/s21113901

DIRECTIVE (EU) 2022/2555. (2022). *DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (E*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Erstad, E., Soldal Lund, M., & Ostnes, R. (2022). Navigating through Cyber Threats, A Maritime Navigator's Experience. *Human Factors in Cybersecurity*, *53*, 84–91. https://doi.org/10.54941/ahfe1002205

Galetta, A. (2013). *Mastering the Semi-Structured Interview and Beyond*. New York University Press.

Grispos, G., & Mahoney, W. R. (2022). Cyber Pirates Ahoy! An Analysis of Cybersecurity Challenges in the Shipping Industry. In *Journal of Information Warfare* (Vol. 21, Issue 3).

Guest, G., MacQueen, K., & Namey, E. E. (2011). Applied Thematic Analysis. In *Sage Publications*. Sage.

Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. *Computers and Security*, *103*, 102196. https://doi.org/10.1016/j.cose.2021.102196

Hatteland Technology. (2022). *An Introduction to Computer Networks*. https://www.hattelandtechnology.com/blog/introduction-to-computer-networks-on-ships

Hopcraft, R., Tam, K., Moara-Nkwe, K., & Jones, K. (2021). Enhanced Transparency: Improving Maritime Cyber Governance. *European Workshop on Maritime Systems Resilience and Security Conference (MARESEC 2021)*. https://orcid.org/0000-0003-2840-5715

International Electrotechnical Commission. (2010). *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program* (Issue IEC 62443-2-1).

International Maritime Organization. (2017a). *Guidelines On Maritime Cyber Risk Management - MSC-FAL.1-Circ.3*. *44*(0), 1–6. https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

International Maritime Organization. (2017b). Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems. *Web Site IMO*, *428*(June 2017), 2017. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution MSC.428(98).pdf

Jasper, S. (2020). *Russian Cyber Operations: Coding the Boundaries of Conflict*. Georgetown University Press. https://doi.org/10.2307/j.ctv2k88t3d.13

Jo, Y., Choi, O., You, J., Cha, Y., & Lee, D. H. (2022). Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework. *Sensors*, *22*(5), 1–18. https://doi.org/10.3390/s22051860

Karim, M. S. (2022). Maritime cybersecurity and the IMO legal instruments: Sluggish response to an

escalating threat? *Marine Policy*, *143*. https://doi.org/10.1016/j.marpol.2022.105138

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection*, *37*. https://doi.org/10.1016/j.ijcip.2022.100526

Knapp, E., & Langill, J. T. (2015). Industrial network security: Securing critical infrastructure networks for smart grid, scada, and other industrial control systems. In R. Samani (Ed.), *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems* (2nd ed.). Syngress. https://doi.org/10.1016/B978-1-59749-645-2.00024-0

Lee, J. M., & Wong, E. Y. (2021). Suez Canal blockage: an analysis of legal impact, risks and liabilities to the global supply chain. *MATEC Web of Conferences*, *339*, 01019. https://doi.org/10.1051/matecconf/202133901019

Leung, L. (2015). Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, *4*(3), 324. https://doi.org/10.4103/2249-4863.161306

Longo, G., Russo, E., Armando, A., & Merlo, A. (2022). *Attacking (and defending) the Maritime Radar System*. 1–16. https://doi.org/10.48550/arxiv.2207.05623

Meland, P. H., Bernsmed, K., Wille, E., Rødseth, J., & Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents. *TransNav*, *15*(3), 519–530. https://doi.org/10.12716/1001.15.03.04

MITRE. (2021). *Faq | Mitre ATT&CK®*. https://attack.mitre.org/resources/faq/

Mohammed, A. S., Reinecke, P., Burnap, P., Rana, O., & Anthi, E. (2022). Cybersecurity Challenges in the Offshore Oil and Gas Industry: An Industrial Cyber-Physical Systems (ICPS) Perspective. *ACM Transactions on Cyber-Physical Systems*, *6*(3), 1–24. https://doi.org/10.1145/3548691

Mosteiro-Sanchez, A., Barcelo, M., Astorga, J., & Urbieta, A. (2020). Securing IIoT using Defence-in-Depth: Towards an End-to-End secure Industry 4.0. *Journal of Manufacturing Systems*, *57*(October), 367–378. https://doi.org/10.1016/j.jmsy.2020.10.011

Nicholas, C. F., Clark, L., & Szauter, K. (2019). Transcription and Data Management. In D. Nestel, J. Hui, K. Kunkler, M. W. Scerbo, & A. W. Calhoun (Eds.), *Healthcare Simulation Research* (pp. 121–126). Springer Nature Switzerland. https://doi.org/10.1007/978-3-030-26837-4_34

Oruc, A. (2020). Claims of state-sponsored cyberattack in the maritime industry. *15th International Naval Engineering Conference & Exhibition*, *C4ads 2019*.

Palmer, C., & Bolderston, A. (2006). A Brief Introduction to Qualitative Research. *Canadian Journal of Medical Radiation Technology*, *37*(1), 16–19. https://doi.org/10.1016/s0820-5930(09)60112-2

Passer, M. W. (2017). *Research Methods* (2nd ed.). Worth Publishers.

Sahay, R., Meng, W., Estay, D. A. S., Jensen, C. D., & Barfod, M. B. (2019). CyberShip-IoT: A dynamic and adaptive SDN-based security policy enforcement framework for ships. *Future Generation Computer Systems*, *100*, 736–750. https://doi.org/10.1016/j.future.2019.05.049

Svilicic, B., Kristić, M., Žuškin, S., & Brčić, D. (2020). Paperless ship navigation: cyber security weaknesses. *Journal of Transportation Security*, *13*(3–4), 203–214. https://doi.org/10.1007/s12198-020-00222-2

van den Berg, B., & Kuipers, S. (2022). Vulnerabilities and Cyberspace: A New Kind of Crises. In *Oxford Research Encyclopedia of Politics*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.1604

Van den Berg, J. (2018). Cybersecurity for Everyone. In M. Bartch & S. Frey (Eds.), *Cybersecurity Best Practices* (pp. 571–583). Springer Vieweg. https://doi.org/10.1007/978-3-658-21655-9_40

Whitehead, D. E., Owens, K., Gammel, D., & Smith, J. (2017). Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. *70th Annual Conference for Protective Relay Engineers, CPRE 2017*. https://doi.org/10.1109/CPRE.2017.8090056

Wilson, B. (2022). Maritime Cyber Security. In J. Kraska & Y. K. Park (Eds.), *Emerging Technology and the Law of the Sea* (pp. 158–183). Cambridge University Press. https://doi.org/10.1017/9781009042178.007

Appendix I. Interview Transcriptions

Appendix I.I. Interview 1

Researcher: The first question I have is, can you explain what your organization does and how it's related to the maritime industry? So, it is just a short introduction on, how you fit into the maritime industry.

Interviewee 1: [The organisation] is the [one of the oldest classification companies]. We do it over [100 years]. And we basically set the minimum technical standard required to pass. And if possible, we also cover the flag [state] if the flag agrees to that, and otherwise the flag does it by themselves. Last us propulsion, steering and floating, that is the main topic. And the flag does the safety side. In the old days it was different, everything was done and set by class. But that's later pulled by the flags towards them. Because for small ships there were no requirements, because there was… Classification is a notified body status. And it's mandatory to follow. If you do not follow, then you can't sail the vessel. And that is actually above 24 meters. That's where the mandate starts. And we do not engineer, clients engineer, we only check out if it's appropriate and common-sense engineering is applied.

Researcher: If it meets the minimum standards.

Interviewee 1: It's a minimum standard requirement. You can always do more and the same with the flag. The flag deals with things like humans, certification of the humans or vessels, like the fire safety on the vessel. Procedures on the vessel, stuff like that.

Researcher: And ensuring that everyone has the same everybody has the same or the appropriate education to go on board or to work on a ship or…

Interviewee 1: Yes, that is set by the flag. That is not [done] by class. We expect that everyone is professional and

they got a valid certificate. That is our start point. And the flag decides if the person has sufficient knowledge and if he is obliged to get a certificate. It's called a STWC-Certificate.

Researcher: What is about the size of the organization?

Interviewee 1: We have about 3.000 people.

Researcher: So quite significant in the maritime industry.

Interviewee 1: Yes, world coverage.

Researcher: Can you explain what your role in the organization is and how does it relate to cybersecurity?

Interviewee 1: I'm the head of the electrical department in the Netherlands and Belgium. And we basically deal with all electrical aspects and control aspects including control air, control hydraulics. And a part of them is cybersecurity for when software gets adapted on board. And the latest step we have that people start interconnecting with ships to shore. It gives another challenge.

Researcher: Indeed. And how long have you been in your current role at the organization?

Interviewee 1: Over 25 years I'm doing it. More than 31.

Researcher: Okay. And did you have a previous role in the organization?

Interviewee 1: No, always in this area, territory. There's more energy and the latest technology as well normally often involved in. Because I know the core of the regulations, where it's based on. For me, it is easier to adapt to new technology than the other people. They have already problems in understanding the core.

Researcher: So, you know the core. You know where the interpretation comes from. When a new technology comes…

Interviewee 1: The majority. There is also history. Shipping is conventional, so its history goes electrical wires more than 120 years, 140 years. It is based on history and accidents. Marine basically tries to adapt nowadays with risk assessment, but it used to be with accidents.

Researcher: Like the Titanic for example. The most famous.

Interviewee 1: But the Titanic was actually a very good vessel. It was 200% above the minimum standard. In those days.

Researcher: Okay, only the life…

Interviewee 1: In principle it was not a requirement to have watertight bulk heads. That ship had. Only the way it was solved was differently than we do nowadays. Because it was not tied to up and it had lifeboats. It was in those days not a requirement on vessels. And it had lifeboats for all people on

board. That was the rumour. Later we found out there were more people on board than actually lifeboat positions.

Researcher: That was more an introduction on what [the organisation] is and what you are and now we're going to move to the cyber security aspects. So how would you describe the cyber security landscape, let's say in the last five years of the maritime industry?

Interviewee 1: The maritime industry thinks that if they can obtain the data from the ships live, or trend it, that they can make designs more efficient. And some company sees as an extra business model. Aid to support the technical departments of the ship owners. If additional information and things are deteriorating. But mainly is used to analyse behaviour. That is where the trend of the market goes and the ultimate step we have is a digital twin. That is our ultimate goal for any ship we have. Any type. And digital twin is a long time ago and the predecessor was condition monitoring. It never took of so much of then we actually in the past expected it should be done. And in the old days remote technology was expensive and actually not available. And now the technology is available. It is still a bit expensive, but it is actually everyday knowledge if you look in the Netherlands. And availability, so the technical side is no longer a limit. It is now more the functional side. The ethics with it and emotions.

Researcher: If you look at the security landscape, how would you say that it has evolved in the last years?

Interviewee 1: In the beginning they only focused on the tools of the service engineers. That is where we started. And that is where we started with cyber security and the way to control software.

Researcher: But it is more into what does engineer do with the software or?

Interviewee 1: Now often bug repairs. Or implement no issues. But the last thing; You should have a process to do that, design process. And not programming on board. And a lot of people in the marine market still do that. We find that basically immature. So classwide view. It should be properly designed to paper, then you test it and then you implement it on board. So you need to test it in the factory and that is a challenge. The marine market is not mature on that. We have different expectations and we have conflicts because of that. Or we find issues that there is no proper control.

Researcher: No, or delay of information that comes at the latest stage that you should have gotten earlier.

Interviewee 1: Yes, we have a profound opinion that the software cannot be 100% tested. And that not everybody in the world has that opinion, but they think it is not. So in the factory acceptance you can only touch a bit.

Researcher: Yes, indeed. If it comes together you have to...

Interviewee 1: If it comes to interfacing, then the world is poor. If they come in the factory and they say, “Can you show me the agreement for this on data on the serial link and demonstrate the serial links”, then it becomes a challenge.

Researcher: Yes, and it starts [with] staring.

Interviewee 1: Yes, it is very slowly improving not fast. And the problem is that cyber security goes much faster.

Researcher: Yes, it develops more rapidly than the people can keep up with.

Interviewee 1: Not necessarily that they cannot keep up, but the IT world has their own ISO 9001 approach. And in the marine world it's rather barely implemented. So, the way you should deal with software is not in the same level as they do in the real IT world. And here is where the challenge is then. Because people think if you have a link, then you can obtain the data. That is true, you can obtain the data, but there is a hell of a complete process behind it, what is needed for obtaining data. And how to avoid, that the ship has changed you due to the uplink. Technically it's not a problem anymore. At the moment we controlling ships from shore. We done trials in [the organisation] and then basically cyber and all these aspects get on your desk. For us, remote monitoring is almost the same as the remote control. It is only the direction that is different, but modern systems are bidirectional, and the interfaces are programmable from shore. And this is the achilles heel in all the designs.

Researcher: You would say that it is the main challenge for cyber security on ships at the moment?

Interviewee 1: Yes, and the software world invented a little thing for convenience and the convenience is where the price is paid. That convenience is called script. And by transmitting scripts, you can update software. Basically, not in-flight, because the system will shut down for the moment, but the next step is that we will do in-flight updating.

Researcher: If you look at the maritime industry, what would you consider the top three threats for cyber incidents?

Interviewee 1: Technically, we see that you get hacked. And that the system is changed on board. Either accidentally or on purpose. And at the moment you don't hear much because people are not transparent. And sometimes we test the systems, but the tests were devastating in the beginning. Because we've got links, they could not fight any attack. And then the worst scenario we experience is that we get a DDoS attack. And that brings the onboard systems down. So that is for us the most dangerous attack. Then the next step is updating software on board. And that's not properly tested and it is lesser quality. If you look from a safety point, then what is installed on the vessel. Because we assume the 1.000 reasons to update the vessel. And it is also a necessity to do that apparently. We say, that if the software is stable, then don't touch it. Don't update.

Researcher: One is getting external intruders going into the ship, or hacking the ship, And the other one is more how people deal with it by they accidentally altered the…

Interviewee 1: Yes. So now we are going for the unmanned ships. At the moment we have 6 phases where we identify the steps to do. The majority of the technology is now at AL3. If we look from zero to 6, that's the range. We have done tests till AL5. And at the moment we have no AL6 projects.

Researcher: No. And AL6 would be without anybody on board?

Interviewee 1: No active crew on board. I'm not saying nobody is on board. And no active crew.

Researcher: So that would be even more risky when there are people on board and there is no active crew, because then the risk would be, let's say a person getting under life threat.

Interviewee 1: That is the consequence, if things get out of hand. And if you look to all the drones flying around, that is exactly an in between AL3 and AL6. We have seen naval projects with AL6 sailing around with nobody on board, with weapons on board. And they are task driven. These experiments are happening. So you say, "Defend the harbour." And then they will take care of defending the harbour unmanned, there's nobody on board, there's nobody controlling the vessels, maybe the people looking on the distant, but actually all decisions are made by the ships themselves intercommunicating. I've seen experiments with that, with this rather quite advanced, because that's task driven projects, that's slightly different than sailing unmanned. In AL6 you can actually you can also separate things to that level. But actually, technology wise we are that far. We are now experimenting with the task driven versions. So you can say that if you look at naval where you need to defend this or you need to attack that or that you get from ships, commercial ships operations say, "You need to bring the goods from A to B." Now we have no automatic discharging systems yet on board. We did some experiments in the past, but till now it is not actually done or came in big

things, you see some in between steps in containers, and the cranes are automatic. Particularly in Rotterdam, and then the handling is automatic, but on the ship there's still parts done manually. And the ship needs to control itself. Partly manually and partly automatic.

Researcher: And also the mooring to the quay and things like that are of course…

Interviewee 1: Yes, that is also possible automatic, because we have done test with that, also in Rotterdam. Magnetic mooring. And then able to handle the tides. It is a consequence. And I also see ships automatic connecting to shore when they need electricity or for charging. And the fully automatic nobody touches it. That's for electrical people not so difficult because they say, “That is how we design systems.”

Researcher: Without the influence of...

Interviewee 1: It is a bit task object driven stuff. But to big systems like ships, it is not yet, but here are a lot of experiments going on in their test areas. Possible where complete ships are meant to tested, I think we have around 60 in the world. I think in the neighbourhood of the Netherlands we have 15 areas where you can test automatic. Even in the Netherlands, there are areas where you're allowed to go for automatic testing, but you need flag permission.

Researcher: Also the status too…

Interviewee 1: Yes, because in the Netherlands it's in the law. The shipping is in the law, so you need permission from the law to experiment. Because otherwise they detain your vessel.

Researcher: I was wondering about the cyber security views of the organization. So which cyber security strategies are used within the organisation?

Interviewee 1: If you look to the [organisation] in general, we have a heavy defence, because we get regularly attacked, people try to steal technical information. So that is why the first defence is for us that is operational, we have a heavy defence on that and that’s sometimes so tight that even the clients can't get through. That's the side effect of it and then we have what we do with the vessel, and we have legislation for it. That's why I submit that to you. So, you can read some stuff about it. And then you basically follow the American principle where you have 4 levels, so first: Able to detect. That you have a cyber problem and then: How to recognize it and then: Mitigation. And if you get attacked, how to deal with it? Whether I'm handing part. There is a world standard on that, and we basically follow that kind of world standard.

Researcher: Is it from the NIS or?

Interviewee 1: Yes. From the NIS. So that is basically what we follow as a concept. Because it is like military. It is a constant battle. We always say, “We have 100,000 entries to the software. So, we need to make from designer point are 100,000 entries tight. And the attacker needs one. So, it is not a comparable game. For the defenders it is very difficult. If you follow certain steps then you can make things very tight. And what we find very weak at the moment is, that they focus on the connection now, and they have good and bad ones, but they do not focus how they inside the company interconnect. Because technically, they would be very happy to go even in the cloud mode. But they have no clue what the cloud does with the information. Nor if it's true. For instance, if the data transmission gets done physically to the ship, you don't even see it, and the simplest version is checksums, but there is no data repair, there is no, repair block on uploading software if it's not incorrect. If the software is received, there's no check if the software is actually in total correct. File size is the same as the transmitted file size. There is no comparison check. Simple tools which would make your life easier, but sometimes if you start pinpointing on that level, it's a bit weak. And it takes some time that people get mature.

Researcher: Somebody could intercept the message, alter it.

Interviewee 1: Yes, but people think they are not so vulnerable between men in the middle attack, but if you go on the darknet, then there is a facility where you can see all shipping, and you can see the interface on the ship and an IAS position coupled so you can check which ship it is. There is software on the market, if you use that, you have directly access to all the technical data transmitted over the lines, in the seven levels of the of the ISO.

Researcher: It is quite deep.

Interviewee 1: I can even see the salaries. Anything you want, you can see. And it is freely available with that software.

Researcher: Many people are do not know about the consequences of the actions that they do that they don't expect the attack because…

Interviewee 1: Yes, so we understand you want to monitor the vessel. We can see the advantage there because it's for certain levels an advantage, but technically with the same link you can also be directional. There is no half duplex systems available anymore. We have to go 30 years back in time to get half physical hardware or duplex. Now everything is, even from [your organisation] you can

actually update the interface equipment and the uplink equipment at the ship, and then bring it to higher level and do what you want. They can change the access. If you have admin rights, then you can.

Researcher: You can do everything, yes.

Interviewee 1: Yes, but that is from the other side. And we would as the first thing say. “Do it from the ship side.” But everything is transparent nowadays, and tough interconnecting principles makes you less vulnerable. And here is the price we pay. Everybody wants it very convenient and easy interconnecting.

Researcher: Directly.

Interviewee 1: So you can do it, I can do it. And with no direct issue on the communication. But there is also the Achilles heel, because it makes you weak.

Researcher: Yes, indeed. It is convenient so…

Interviewee 1: Yes. It is the price you pay for convenience. The more convenient, the weaker you are. People are not aware, till they are exposed to it.

Researcher: When it is too late actually.

Interviewee 1: And then they go levels higher in security suddenly.

Researcher: But if the budget would not be a limiting factor, which action would you take to enhance the security of a ship?

Interviewee 1: I think first we would tackle the procedures.

Researcher: Okay. Procedures are the main.

Interviewee 1: And second, we would partly, at least better test the system that there are less vulnerable. In the cyber world you have all kinds of processes where you can check your vulnerability. Maybe you would actually indicate phases and level between A and Z where is your vulnerability. And regularly say, “Well, this is the goal, how vulnerable do you want?” And if you look now to present operations. Present operations is just in time. The example is when a vessel in Suez Canal blocked the world. One vessel completely blocked the world and it brought the transport from for months. And if you look to just in time then that doesn't allow that, so you get serious issues as a

result from that. So even cyber-attack would create exactly the same. And then you can see how vulnerable you are as a total society.

Researcher: Yes, all the shipping is based on arriving at the port at a certain time, unloading and continuing again another port at a time.

Interviewee 1: We had a case in the Netherlands where Maersk got attacked. And that was actually from a virus specifically for Ukraine. That they accidentally were vulnerable to that. And it brought the traffic down for in the waterway all the way to Switzerland for six weeks. Even the ships in Switzerland could not sail because they could not release the goods. So, everything was stuck. A fight for the distribution effects of it. And then we have seen people get in serious financial problems because the margin is too little to handle that

Researcher: Indeed, and just in time.

Interviewee 1: People are not aware how vulnerable you are and an extreme example was Speed II. I give that always to people the example movie to watch it's exactly technically a bit extreme because at the moment we still can locally take over so we can stop things locally, but you need crew on board to do that. But I see already the first steps. Where we had a hacker problem. What we call an indirect hacker. So the people on board made a mistake and actually hacked the ship themselves. And there were not aware that they did that. And they couldn't even control locally anymore because everything got locked up.

Researcher: Okay, so they really fixed something that shouldn't be fixed.

Interviewee 1: Yes, it is a very simple problem if you swap T and S on the communication lines, you can lock up complete computer systems. Even redundant versions.

Researcher: So sometimes it is not completely redundant.

Interviewee 1: Yes, that is the definition of redundant. I think it's a bit out of scope here, but it is cyber, it is the problem. Actually, nobody wants to be vulnerable for cyber-attacks. And the budget available for it is rather low because apparently the systems are quite good, so people don't get often the experience. But if you're in the naval world. Then that will happen extremely. It's one way to bring the enemy down.

Researcher: Especially if you if it is with a lot of automated decision making, automated shipping and if you can take over then you have control, or you can at least neutralize it.

Interviewee 1: Yes, but military is about communication and data exchange. So, if you do a proper dumb DDoS attack, you bring the communication down.

Researcher: Yes, then they put you in the blue or staring in the black.

Interviewee 1: And then it really hurts if you have no alternative which is not vulnerable to such a system. And the world is moving to data and data exchange. As [the organisation] we even if we think it's not okay, we cannot stop the world.

Researcher: No, they will find other ways.

Interviewee 1: That is what the world goes to, and we only need to properly deal with it. And part is to do the ethics side. In the rules, there is a specific ethic side where we can refer to and say, “We can stop basically technology like this where maybe feel the ethics come around if the software start killing people on board”. And for many that is the street too far.

Researcher: So it is making automated decisions and decides it's better to…

Interviewee 1: This is where people and certainly non experts are very cautious because they think this takes over my job, this takes over my life, it influences my life. And that is where people could be lying, where they don't accept anymore. But technology wise is everything possible now and I think there is technically no limitation anymore of interconnecting. This with technology and even money wise it become very cheap. Certainly, if you use the uplinks with Starlink. It is just a high-speed link rather cheap.

Researcher: Worldwide.

Interviewee 1: Yes. And if you use the technology and the encrypting they use for video exchange like we have now, then you can see an enormous amount of information get exchanged at a rather low bandwidth. For us, the ultimate side is holodeck where I can board the vessel. That is very far future still. But then we can board the vessel and say this is the problem or that is the problem. That is where we go to. In the electrical world, we already have digital twins operational. We don't do that with simulation of the reality. So, this is the first core steps where things go slowly in digital twins. And digital twin is requiring this cyber side properly done. I can ask you a simple question: If you are the ship owner, but you are allowed that the ship software is not on the ship but on the shore base and it talks to the ship by interconnection only.

Researcher: I would be a bit weary.

Interviewee 1: That is now technically possible, and the example is the mobile phone. The mobile phone is an example of how the purpose and what she can do extremely exploded in that capability. Because actually it is an advanced remote-controlled computer to the cloud, to the cloud system. Because you only see your screen acting and not the whole thing behind it. And if it's perfect and there is no vulnerability, then this is the step possible in shipping, but it's an ethics site if you would go that far.

Researcher: That is where the phone is. Yes, you can get a lot of data by having the user information, the position information and those things. The same for ships, of course.

Interviewee 1: What we normally do is kind of risk analysis and then we say. “What is the risk”, and try to pinpoint to the users who like to have it, “Are you aware of the consequences, what is possible?”

Researcher: And then they can get a better idea or at least think about it, about the risk and see how they will deal with it.

Interviewee 1: Yes, it is now selling a thing because the ships are now connecting to shore for monitoring purposes. Everybody wants it. So are [your organisation]. And here is where the advantages in the moment you start autonomous controlling ships, there is always somebody who likes to know the data from the vessel to oversee what is happening. I think that that station of overseeing somewhere by somebody, it will take a very long time before that is dependent. But some systems it is possible, and the military will use the long time overseeing signs if autonomous ships and the owners also. So, it takes some time, but the problem is it goes very rapidly now. Everybody dives in it, so the more people go in it, the faster the acceleration rate is for implementing technology. And many people have problems in understanding it and to keep track of it. What is happening. It goes so extremely fast now.

Researcher: And everybody brings in his own idea or its own principle on how to do it.

Interviewee 1: That is not wrong because, if you have started to experiment and you learn and to figure out from a blank piece of paper all directions is very difficult. Technology used to be the limit and that is no longer. So we go this route.

Researcher: Okay. Thank you for the interview. I got a lot of information

Interviewee 1: Is it useful?

Researcher: Yes it is.

Appendix I.II. Interview 2

Researcher: The first question is just to get some idea on what you are doing and how your organization fits into the maritime industry. Can you explain what your organization does and how does it relate to the maritime industry, and perhaps say what size your organization is?

Interviewee 2: We were a group of 125 people head quartered here in Amsterdam in the Netherlands and we have service offices in Antibes in France and in Fort Lauderdale in the US. And our focus is on integrating luxury technology on super yachts. So that that's our relation to the maritime industry. We've we're fully focused at the moment on yachts and we integrate audio visual on IT and physical security and communication technology on board yachts.

Researcher: OK, clear. Can you explain what your role in the organization is?

Interviewee 2: I'm responsible for technology and innovation and part of the management team. And within my department, we define technical standards and we are busy with the innovation. That's in a nutshell my role in the company.

Researcher: And how would you relate that to cyber security?

Interviewee 2: Well, cyber security I think is a very broad aspect. We of course are active in the IT domain. Any electronic system nowadays runs on an IT or IP backbone, and this is true also for our systems. Although we are not in direct contact with the mission critical systems on board like navigation, communication or engine room systems. Our systems are more aimed at entertainment and informational purposes. Audio visual systems and stuff like that. But also, there's a big IT component. And of course, what we try to do is to look at this aspect in a pragmatic and sensible way. When we designed these IT topologies and systems, we take cyber security and security in general into account as much as possible.

Researcher: If I would summarize, I would say that, because you work in IT that automatically brings you into the cybersecurity domain, because of the work that you do.

Interviewee 2: Part of it, because I think cybersecurity is much broader than technology alone. It has also a lot to do with awareness of the people using the systems. It has to do with the policies. It has to do with a lot of other aspects that are not directly technology related and we are involved only, at the moment, in the technology side of things.

Researcher: OK, clear. And how long have you been at the organization?

Interviewee 2: Almost 15 years. I would say 14 and a half years.

Researcher: And what was your previous roles in organization?

Interviewee 2: I started as a project manager and then I went on to be a program manager. I was leading various project managers. And then when I joined the MT like four to five years ago, I was operational responsible for all the all our new build projects and now for two years responsible for technology and innovation.

Researcher: The next questions are, about on what you think of the cybersecurity in the maritime industry in general. If you look at the maritime landscape, how would you say that the landscape has evolved in the last, let's say, five years?

Interviewee 2: With regards specifically to cyber security?

Researcher: Yes.

Interviewee 2: I cannot speak for the broad maritime industry because I only know yachts. We are only active on yachts. And then I must say that although regulators like IMO and Lloyds are starting to put together requirements in their regulations about cybersecurity, I feel the awareness in the yachting industry is shockingly low, with regards to cybersecurity. We formed three years ago a strategic alliance with the cyber security Company, an external company and we've launched some services and products in the yachting market with regard to cybersecurity. And we've seen almost zero response to those propositions. Also, in RFQ's that we get from customers or technical specifications that we receive from customers or external parties, cybersecurity is almost never considered as an aspect in those requests. All those factors make me realize that the awareness about cybersecurity in the yachting industry is shockingly low.

Researcher: And because you say it's low, but you internally [within the organisation] have your own opinion. Has it changed in the last five years or has [the organisation] always been into cyber security?

Interviewee 2: Well, of course that's changed because technology is constantly evolving. And I can say that within our company the awareness has increased and is still increasing. But also, as I said cybersecurity is a much broader aspect than only technology. To give an example we can secure a Wi-Fi network pretty heavily by using passwords and maybe even MAC address authentication and other technological methods to put in place. But if a boat does not have proper policies for crew turnover for example, and do not delete an account of a crew when the crew member leaves the

boat, then you would still have a very high security risk, although the technology itself is in good order. So, we can only bring a piece of the puzzle, which can never be completed without the other aspects which also need to be considered. This starts, I think, with awareness which can be triggered by regulations like IMO and Lloyds. Since a year now there's basic cybersecurity aspects already considered in IMO regulations, and even then, still we do not get any, or almost any, proactive questions or inquiries from any of our clients or potential clients.

Researcher: You have gone to pursue them actively and then the response is how would you say that?

Interviewee 2: Low.

Researcher: If you think about cyber security on ships, what would you consider a cyber incident? Which unintentional incidents would you consider and which intentional incidents do you consider?

Interviewee 2: In in broad sense or?

Researcher: Yes, in a broad sense, or specified for your situation, that’s also ok.

Interviewee 2: This is very hard to question for me to answer because in the end we are a technology provider, and although we have some cyber security offerings in our portfolio, this is almost never part of the scope of our projects. In that sense cyber security is the risk of our customer, because it's not something that they paid us for to provide for them. Still of course when designing our system for our customers we take security into account by implementing proper measures and configuration of equipment etc. However, this is nothing without also having proper considerations about policies and awareness at the client level. The propositions that I was talking about that we that we had with a partner, included a more let's say, active cyber security technology. Network scanning tools that expose any potential vulnerability with recommendations how to solve them but also real time monitoring of IP packets, packet inspection and monitoring when connections for any threats and alarming on them. But those kinds of systems we haven't deployed much, because customers are they just not willing to invest in them. Even though cybersecurity is not part of the scope of our projects, we still try to take the common-sense approach. When we design our networks for our clients and also in the configuration, we take, a more secure way of configuring for example access control lists on network switches. And in the designing the network topology we take the aspects of cybersecurity into account. That's about all we can do, when cyber security is not a direct aspect of our scope. And then, what would I consider

an incident, I don't know. Any unauthorized access to a network or a device could be considered an incident, I think.

Researcher: But anybody who gets into the network doesn't matter what purpose or task. As long as an authorized person accesses the network, then it's an incident.

Interviewee 2: Yes, I would say so.

Researcher: What would you say that are the main challenges of cyber security on a ship?

I think it all starts with awareness. I think that's the main challenge. To get the responsible crew of a ship or the management company of the ship to be aware of any cybersecurity risks and how to treat them in a proper manner. Often cybersecurity is looked at from the technology side of things, but I think that the biggest challenge is to convince people that there are many more aspects important, like awareness, like proper policies in place. Also, procedures by maintaining a network. I think that's the biggest, challenge to convince people of the fact that there's much more than technology involved in in cybersecurity.

Researcher: If I understand you, would you say that the people they think: “I've good technology on board so my ship is cyber secure, but they don't consider other policies and user policy that could cause actual incidents.

Interviewee 2: Yes, indeed. You can have a top-notch technology system that's fully considered with all cyber security aspects, really 100% secure. But then, if you gave out your passwords to crew, that leaves the boat and then they're still able to log in when they left the boat. Then you're still not secure and you have a very high risk. Or you could have this technology, this system in place, but then not actively, scan it for example, or monitor it. So, somebody could just plug in a different switch and connect all kind of other devices, and your network would still not be secure. I think the main challenge is to consider more than technology alone, because the technological systems and the technology out there is already [available]. I don't think that's the issue. It's a matter of, the responsible people and companies realizing that there's much more to cybersecurity than technology only.

Researcher: If you look at your organizations own cybersecurity strategy, I would how would you compare it to other organizations?

Interviewee 2: I've too little experience in the field to judge that. But my gut feeling is that a lot of companies active in this industry are taking it to narrow approach by either only considering

technology or only considered considering some other aspects and not taking a holistic approach that is needed I think in cyber security.

Researcher: OK,clear. Let me see this we already covered. Let's say you have a ship and the budget is no limitation. Which action would you take to enhance the cyber security on the ship?

Interviewee 2: This is an already existing vessel.

Yes, let’s say it's an already existing vessel or you will have a new vessel or you will upgrade the whole ship.

Interviewee 2: It starts, I think, with an assessment of the current situation and looking at what the client is actually looking for what they are requesting. Because a lot of times systems are made too complex and too big. Maybe it's not even needed for the customers requirements. First maybe an assessment and then downsizing until you reach something that the client is actually looking for. Then it starts, I think, by together with the client creating awareness for cyber security but also creating the necessary documentation and policies that are required to properly handle the aspect of cyber security. And then you start implementing your technological side of things. Start designing or redesigning a network, looking at all the interface that the network should or should not have. Defined the boundaries of a network and then put your network design in place, configure everything as secure as possible. Finding a balance between security and practicality, let's say. Then having what I would call passive and active scanning tools in place. So with passive scanning tool I mean a predefined scan at a predefined interval. Like every week you perform a full scan of the whole network and indicate any potential vulnerabilities with recommendation on how to fix them. And active scanning, I mean scanning all the end connections of the boats for any threats and vulnerabilities and putting alarming on them. Those aspects I would consider

Researcher: So find out what the real purpose of the client is and what they want to achieve.

Interviewee 2: That’s the plan yes.

Researcher: Make it as simple as possible. Make the policies and then put over the technology.

Interviewee 2: Yes, [the] cybersecurity plan starts with that.

Researcher: If you would compare the shipping industry. I don't know if [the organisation] is now focused only on the shipping industry. And it used to be, I think, on other industries as well or not?

Interviewee 2: Well, we focus exclusively on yachts and sometimes we do some residential projects. But this is really a small part of our work.

Researcher: And if you would compare those two, if you would compare yachting to [the] residential industry. Are there differences or would you say that the client approach is similar with respect to cybersecurity?

Interviewee 2: Residential is really a whole different story because it's a home. It's people's homes and I think cybersecurity is only considered by the ISP, providing Internet to the to the home. But on commercial and especially governmental projects, I think the aspect of cyber security is much more considered than in the, at least, the yachting industry. When you look, for example, at security certificates for equipment and stuff like that, it's much more considered in governmental and commercial projects than it is, I think, in the maritime industry or let me focus only on the yachting side of things. I think relative to other industries in the yachting market, it's under considered.

Researcher: And what would you think that would be the cause of this under consider?

Interviewee 2: If I knew that then… Maybe it's because there have not yet been big incidents in the yard industry with cyber security, or at least not published ones. Maybe we need to wait until the first boat is hacked and runs into shore because of it, and then people will consider it. Maybe it's also because it's considered as a place to have pleasure and not let's say a place where you work or keep a very secret data. It's guessing. I don't know.

Researcher: The maturity level you said it's less mature and mainly it's lack of awareness. Because if I would say I would compare it to other industries, then you just give that answer actually.

Interviewee 2: Yes. I think in in other industry, there's much more awareness. And maybe because I only know the yachting market. Maybe in other maritime markets like container shipping or of course oil tankers, I can only assume that the awareness is much higher. Maybe it's indeed because yachting is more considered a pleasure business that it's under considered.

Appendix I.III Interview 3

Researcher: First, I would like to talk about your organization and how the organization positions itself in the maritime industry. Can you explain what your organization does and how it relates to the maritime industry?

Interviewee 3: Sure. Well, [cyber security company from the Netherlands] is what you call a maritime cyber security specialist as some would say. But we focus on the on the cybersecurity maritime industry. With that, meaning that since the beginning of 2007 and we were one of the first parties actually to launch an antivirus service specifically to update via the satellite link. That that has evolved over the years, we now also offer endpoint security, unified threat management, network detection and response. So basically, a whole set of services, but one of the important parts that we do that is that we make our products compliant or how do you call it, that it's easier for the ship owner manager to get to that IMO compliancy. But also, the new IACS E26-E27 that will be a comic factor for January 1st, 2024. Those are the tools that we have in house, we can also assist the customer with that. That's focusing purely on cybersecurity detection response and with the Security Operation Centre, monitoring those vessels with those services to see if there are any threats. And if there are threats being detected, are they persistent, can we remove those threats, are they already removed and report those findings in a report. Because that's also parts for the vessel's audits that so that they can actually prove that somebody is taking a look into the security records. Because often people install antivirus or endpoint security, [and think] it's installed and they never check if it's updated, they never check if a virus is found or if it's being removed and so on.

Researcher: Are you only focusing on shipping or ships or are you also involved management companies?

Interviewee 3: We only focus on the ship. Everything basically that floats or is in the water. If a management company would knock on the door, we will not say: "We don't assist you." But nine out of ten times they really see the big difference in it; in their shore IT and in their vessel IT. So, we focus on the vessel alone and that's also made us, I think, market leader in it. We provide our services in an in a rebranded form to various parties, Speedcast, INMARSAT. So basically, the biggest satellite providers in the world are using our services and white labelled version.

Researcher: Can you explain what your role in the organization is?

Interviewee 3: Well, I'm the I'm the CEO, so I'm the owner. I'm responsible of getting everything up and running, getting all the teams...

Researcher: And have you always worked at this organization or did you have previous roles before?

Interviewee 3: Well, I have. I have previous roles before, but I founded the organization; I'm the founder of the organization. When it started, I was there. Before that I was active in the maritime industry as well. First as an engineer and basically responsible for e-mail platforms in the maritime industry, satellite system installations, communication, IT, networking, all maritime. I did a little small side step to medical, to hospitals. And then you actually see that hospitals and maritime are very much alike. They have a slower adoption in IT and they have the same, well, not the same, but the similar regulations as well, similar procedures. That was actually a good thing to see as well.

Researcher: Getting a different view and going back into the same market. Now the other questions are more about the views or how you see the maritime industry in in general. How would you describe the maritime industry over the last five years? How did it evolve?

Interviewee 3: Well actually, it's evolving faster for the last five years than the five years before that. So that's actually a good thing. I think that the regulations are also an important part of it and they are pushing ship owners or managers do to more, to quicker interact and to adopt new solutions and they find out that they can't do everything themselves. So, they are using a managed service providers actually to assist them with that stuff. In the last five years we really have seen the adoption going from the state of a plain antivirus to endpoint security and also adding unified threat management as well to the vessel. Especially for the last two years. That's a major leap and I think that it is especially coming from the IMO 2021 regulation that's in place.

Researcher: You see a big push from the governance side.

Interviewee 3: That's the thing. When they don't need to have to have it or need to invest in it, they won't do it. So now it is regulation pushing and then well, they need to do so.

Researcher: Have you encountered for example a cyber incident that caused some extra speed into the process?

Interviewee 3: What do you mean? We have detected multiple cyber incidents of course. For example, a customer was complaining about a slow connection and then we monitored the connection and there wasn't nothing really special on it. But there was just somebody was looking at a webcam back home. So that was slowing the connection. That's not really a cyber incident, but we have seen a Samsung television that was infected by a botnet. And that was broadcasting on the entire network. We could detect that in the network. And of course, we find thousands of infections

a day, which are being dealt with, with the endpoint security or threat management that we have installed. And what we do in our system and our web portals is that we give customers a cost savings report. So, it gives them an overview saying if you wouldn't have this solution, this would be your engineering costs to actually resolve that issue that you currently have adopted. So that gives them a more of a feeling: “OK, so I'm paying for my cybersecurity and now I'm paying, it's actually giving me this back if I would have made those costs.” So, it's making it more visible, because cybersecurity is something that everybody needs but nobody wants to have because it's an additional investment in top of their budget.

Researcher: So that also convinces them to get more products?

Interviewee 3: Some of them, yes. Some of them do actually get more products as well. But it really depends on the type of vessel. Some of them only have one PC because it's a short sea vessel or ship or a fishing vessel. But most of them really upgrade to the new version because they actually see the benefit of all the reporting of what's happening on their vessel, what type of threats, and so on. So, it gives them a more overview.

Researcher: So first you actually have that classification societies and IMO enforce them to have cyber security installed or to have cyber security measures and now they see more benefits from having cyber security measures and take more actions as well. It has a bit of a snow ball effect.

Interviewee 3: Yes.

Researcher: What do you consider incidents on board of a ship?

Interviewee 3: An incident can be… We only focus on network activity and malware that we find. Like a firewall scan, that's an incident. But that can be just like a rogue application or an application broadcasting in a network. Of course, the typical viruses, that's an incident. URLs that are being blocked. Those are incidents. We ourselves are not monitoring if a computer screen is locked or unlocked, for example. We're not dealing with that. That's something that the customer needs to do themselves. That's something that they've paid in their IT policy and they need to configure their systems for it.

Researcher: You focus more on the intentional...

Interviewee 3: The incident response part actually, that's where we focus on. Sure, we have some customers where we do it maintenance as well. So, then we monitor well but then we have correctly configured the entire network. That's one of the major things which often is still forgotten by the

ship owner. If they have a proper IT network and correctly configure it, they will also lower the amount of threats that are entering the network. If you if you block users from specific content, gambling websites, for example, then you will lower the chance of getting any infection on your vessel. If you don't allow users to install software on your PCs, then you lower the chance of any cyber incident. Networks that we manage actually do have that. Do have that installed or have that configured. That makes it very low on incident response on that part.

Researcher: And what would you say are the main challenges for cyber security on board ships?

Interviewee 3: Well, one of the main challenges that often a lot of PCs in the network are still Windows 7 for example. We develop our own software. At some point we have to say to the customer, we will not support Windows 7 anymore. Like Microsoft is not doing it for the last three years. You should really upgrade to a new system. And sometimes they still think it's costly to upgrade because then they need a new PC, for example. And that's something… That's… Why should a machine… In our office or maybe back at home, you replace your PC every three to five years, then you get your new PC. But on a vessel, it needs to work 9 to 10 years. Why is that? They work 24/7 on the machines. Please replace it the darn thing every four to five years. It's not that costly. It's like 800 bucks for a new machine. If you prep it correctly, it's not the end of the world. And then you have the latest operating system and make sure it's updated. But no, they try to keep on just to save like $300.00 on a yearly basis. It's just insane.

Researcher: It’s ridiculous, indeed. How do you deal with that?

Interviewee 3: Sometimes we just enforce the customer saying: “OK, now we're really, we don't support that anymore” and then then they have to. For example, Windows XP support has been dropped last year. If a customer comes [and says]: “But I still have Windows XP” “Sir, sorry man” “It's only five or six years ago.” We always say cybersecurity has to do… You have to look at from the entire spectrum saying if you want to do cyber security, it's not only installing endpoint security, it is not only installing a UTM, it’s also taking care of your workstation. Make sure that you have Windows 10 installed or Windows 8.1 with all the updates. Make sure that that's fixed and then apply your cyber security. Because if you have a boat and the engine represents cybersecurity and you're drilling holes in, it will still sink. That's what they basically are doing. Cyber security can only protect you up to a certain level.

Researcher: OK, clear. What would you say are the most vulnerable systems on board a ship for cyber security?

Interviewee 3: Most vulnerable systems are actually the ECDIS machines, because they're not installed with any security, because it's not allowed at the moment. At the moment it's not allowed. They're are going to change that. So that's at the moment is one of the most vulnerable machine. Because what has happened now, to update an ECDIS machine, they go with an USB drive from a ship's network with a chart to the ECDIS machine; plug in the USB drive and if the USB drive is infected, it will infect the ECDIS machine. So that's one of the issues now that they have with those things. Their SCADA networks, the OT, is often still not a big issue because it's often disconnected from the network. But that will in time be a problem when they are going to connect it.

Researcher: And other like the Radar systems or it's also a disconnected network?

Interviewee 3: That's often just disconnected so you don't have any issues with that as well. The main issues at the moment for shipping is their common IT network, their crew network and their communication system. Although the communication system is running and it's like a back at home switch and the satellite dish and so on. The problem is that when you have an infected machine it can just overload the connection and then you get timeouts.

Researcher: So you get more DDoS attacks?

Interviewee 3: Yes, it's something you can compare it with. You can compare it with that. That's the need to optimize that. They need to segment the traffic; they're still not doing that. And what is becoming more and more of an issue and that's something that we also said and advice to our customers is they get an engine control system from Kongsberg or Wärtsillä or anything of those suppliers. Those suppliers want to look into those systems remotely and some of them even have said: “We also want to control them.” But you as a ship owner are responsible for your ship. If they steer your vessel into the ground, you are responsible. You have to take care of that as well. The other thing is that, the issue that they have is that you need to assess that vendor; how they are dealing with their own cybersecurity. We have seen the biggest threats in the industry, not just maritime, but worldwide, Solar Winds and all those kinds of attacks were happening because a third-party supplier was actually attacked. You get the supply chain attack and that's something in shipping can happen as well. You can have all the security correctly done. You give access to one of your suppliers, they get attacked and they still breach your system because you opened the door for that supplier.

Researcher: The chain is as strong as the weakest link. Which policy do you promote against threats?

Interviewee 3: How do you mean the policy?

Researcher: What do you promote us as a company on what the shipping industry should do?

Interviewee 3: Well, what we always say, well, we start, always start with the basics, start with sanitizing, update all, make sure your IT equipment is standard. It's unmanageable to have like six different desktop systems. All HP, Dell, whatever brand, make sure they're updated. Make sure that you have an endpoint security and that somebody is monitoring it what happening on your vessel and taking reports and taking action on it. And then if you have done that correctly, go a step further and take your UTM, unified threat management. If that's all working and you really want to see whether a VDR is communicating to a television or to a printer, then you can install network detection or response. Coming to that, from the new regulation that is coming, that will be a mandatory item. That will be a great leap forward if you look at those regulations because then they even need to have multifactor authentication, for example, which is nobody is using that shipping at the moment.

Researcher: Indeed, clear. Which trend do you, do you see in the maritime industry that will be in the future regulations coming up, like you, you said before, network monitoring. Which other trends do you foresee?

Interviewee 3: There are not really trends on cybersecurity, but there are regulations that are enforcing cybersecurity and IT management. Those are the new regulations becoming effective January 1st, 2024 for new build vessels only. Although insurance companies will just say eventually you have to comply with that as well. So that's one. The other threat of course that they want to have more faster connections. So, the satellite connection becomes faster. You get the Star Link, One Web, all those kind of players in the market. We have a White paper from Star Link for example, one of the biggest issues, I already told it. Shipping owner still have Windows 7, then they connect their lightning fast 300 megabits per second Star Link dish to it and they have no antivirus or anything like it and they go browse the Internet. Well, you will be 100% victim of cyber attack. They first need to get their network straight and ready for the speed of those networks. Those are the biggest trends, actually one of the biggest trends. The satellite connections are getting faster because they want to do more data and the other one is that new regulations coming up for cyber security enforcing really on new build vessels.

If I if I get it correctly, then from your point of view is first you have to get the basics right, so have updated software, have everything up to date and then you can expand it and see what the regulation says, incorporate that.

You can use the NIST framework for it for example. That's one of the things that were the IMO uses, but that you can use. Don't use illegal software. We still see KMS activator being used on vessels and then our software goes like [error]. So, they blocked the KMS activator. But that's also one of the things that if it's illegal, you don't know what it's doing in the background.

Researcher: You don't know what they changed in the software.

Interviewee 3: One of the biggest detections that we see in our systems is Kingsoft. Kingsoft is spyware plug-in and it's being used in translation programs. What does it do? You want to have your documents translated. The captain puts it in the software, the software sends it up to the Internet, and the servers are in China. You will get a nicely translated document back, but your document will be in that cloud. That's something that I don't really don't realize. They're giving all their information for free just to get it translated. That's something that the maritime industry still doesn't understand. "But I get my translated document." "Yes, but you are giving them viable information which can potentially be used against you."

Researcher: Could be contracts, could be any type of document that they send. Let's say, if budget would not be a limiting factor, then what would you do to enhance the ship security?

Interviewee 3: Well basically what I already said is just a proper network setup because that's currently not done. If you have your security correctly arranged, monitored, password protected and locked and then I think you are already there. It's not that difficult. People always thinking that budgets should be really big. Depending, if you pick Palo Alto then you need a big budget. Other than that, if you just take the normal suppliers, you can get very far with pretty low cost. But the problem is that you're talking about $1000 a month for example, which on a vessel is pretty cheap for us, if you compare it. That vessel is 60 million, but for ship owners it's like: "A $1000 a month, no we will never do that." It's really some...

Researcher: If you look at the potential damage you can have, it's nothing.

Interviewee 3: Well, that's also the thing. If a vessel can't sail away and have to stay at additional day in port, you will have earned it back. That's the thing. An additional port stay at the port of Rotterdam is somewhere between the $50,000 to $100,000 a day. A day! If you only have to stay an additional day, you will have your cyber security for the next three years free of charge basically. If you can prevent that.

Researcher: So that's an important feature to show that what you do, is actually saving money for the owner.

Interviewee 3: That's one of the reasons why we have those reports saying: “OK, we are saving money for you.” We're not calculating any additional port days that you have to have to have to do for this. But just giving them a ballpark figure, saying: “this month you save $6000 because you had so many infections that they were blocked.”

Researcher: Yes, indeed. Previously you said that you could really compare shipping with hospitals. In which way can you compare them, can you elaborate more on that?

Interviewee 3: They often use the same technology to monitor systems, those that they use. Serial connections and those kind of systems they get in a hospital, are serial connections. IP to serial, to monitor the flow rate of medical pump for example or breathing apparatus. In maritime you also have that serial connection, IP over serial, but that will be for our radar or for voice data recorder and so on. So those are pretty similar on network structure. Only the device that you monitor is a bit different.

Researcher: And is it also that they use older systems?

Interviewee 3: Well they have it. Good thing with hospitals is that they actually are having correct plans and budgets and everything for it, which they don't do in shipping very often. You can see hospitals on Windows 7, but then those Windows 7 still get updates because they paid additional for it. In maritime they will not pay for those updates. That's where it goes wrong. That's one of one of the things actually that's the biggest. Hospitals they will stay on for example Windows XP, Windows 7 for the most maximum amount of time, but then later on then they will upgrade. They have a clear path for that.

Researcher: So, it's not only awareness that they have better in line, but there's also that they plan it from the beginning stage.

Interviewee 3: Yes, they plan it and they actually have IT budgets. We have so many customers that don't have an IT budget. That just say: “We need that solution and we will mingle it in this budget somewhere.”

Researcher: If you would look at the maritime industry again, how would you compare the maturity level of the maritime industry compared to other industries, let's say the finance industry?

Interviewee 3: Compared to the finance is just low. It's bottom low. It's below the floor even. Finance is really on the most maximum level because they are dealing with finance. They have every regulation that you can come up with, [which] they are complying to. With maritime, it's no, it's low. But if you be serious like compare it to normal on shore, smaller companies. Even then it will be low to mediocre, that's the best to say. Even the bigger companies, that we were we speak to, which had major cyberattacks, they're now re-evaluating their cyber systems and go like: “Well maybe we can save a bit on that.” “It costs you 7 billion a couple of years ago. Now you want to save on it again?” They always try to save and cut the costs on it. But it's just below medium. It's not even medium, not just below. It's between the low and medium basically.

Researcher: So there is a lot to gain.

Interviewee 3: There's really a lot to gain as well.

Appendix I.IV. Interview 4

Researcher: Perfect. So, the first questions are more about the organization and how it fits within the maritime industry. Can you explain what the organization does and how it is related to the maritime industry?

Interviewee 4: I'm working at [the organisation] which is a part of [the parent holding company]. [The organisation] stands for [the full name of the organisation]. So, what we are doing is explained in the name shipbuilding. And the name itself says [part of the organisation's name]. A couple of years ago the organization was called [the old organisation's name] and now it is part of the [parent holding company]. We are building ships for over the whole world and are a big organization with 11,000 employees, with 30,500 in the Netherlands.

Researcher: Yes, quite substantial. Can you explain what your role in your organization is?

Interviewee 4: I have been working as a senior cyber security engineer, since November the 1st 2021. So more than a year now.

Researcher: Okay, yes. And did you have…? Sorry.

Interviewee 4: First I was working for the [project name]. Which is the new, the replacement, of the [frigate type], [a European Navy] and nowadays I'm working for the [project name].

Researcher: Okay, yes. Familiar projects. So, what was your previous role at the organization?

Interviewee 4: Well, not on this organization, but before that I was working with [the organisation] and I worked for 39 years at [Dutch governmental organisation], with 38 years as a [role] in the [navy]. So, I was a navy officer and I have been working for 38 years.

Researcher: Okay, yes. So quite experienced with the ships and how they operate in practice. Did you always work on the cybersecurity side or did you have previous roles that were less related or how would you say that you got into the cybersecurity?

Interviewee 4: I have had a lot of [navy] and my last function was at joint IT commands at the [Dutch governmental organisation]. And there I was head of the [department]. There I saw, so… That was a call. There I saw there was a lot of lack of knowledge of cyber security. In that role I had made a lot of courses at the Naval school at [location]. And there they have several modules of cyber security. I've followed them all. And after that, when I was leaving the Navy, I've been working for a year as a CISO at the joint IT commands at [Dutch governmental organisation] in [Dutch city].

Researcher: Okay. So quite experienced in the cyber security industry as well. If you look at the maritime industry, how would you say that the landscape has changed in the last 5 years, 5 to 10 years?

Interviewee 4: When I look at [a European Navy], a major change has taken place with regard to cybersecurity, for example, for current ships, the defence security policy, DBB, is looked at with the very similar at the ISO 27000. But the DBB is also subject for changes. Because it is more inclined towards office automation. For example, to accredit a ship, DBB is still being looked at. But in practice if you want to accurate accreditation of a ship, you are busy to reengineer the ship. That's why I believe more in building with the principle of secure by design and that is good because many new maritime units will be purchased by the Navy in the coming years. We have a new tanker, we have new frigates, we have new submarines. So that is the chance to make it better and to implement the cyber security requirements.

Researcher: Okay. If you would look at [a European Navy], let's say five years ago the security by design was less present and now it's something that you would emphasize more on to have it secure by design and not just to put equipment and see what will happen.

Interviewee 4: With the ships which we are now sailing, they are 15-20 years old or older and so it is very difficult to implement the cyber security requirements in those ships. We also build in those days with the classes and the focus on cyber security.

Researcher: Yes. Indeed. If you look at cyber incidents, what would you consider an incident?

Interviewee 4: I always reason from, the CIA triad, confidentiality, integrity and availability. Which is: The confidentiality is the unauthorized disclosure; integrity is the unauthorized modification or impersonation and availability is for example a denial of service. A breach of a system security policy in order to affect its integrity or availability and or on unauthorized access or attempted access to the system. I see that as a cyber incident.

Researcher: Yes, so when the CIA triad it's being let's say broken, not broken. How would you say that? When it affects the CIA triad, then you would say it's an incident.

Interviewee 4: Yes.

Researcher: Okay, clear. If you look at ships, what would you say are the main challenges for cyber security on ships?

Interviewee 4: The main challenges are to protect the system 24/7. Detecting of abnormalities and detecting in time and response quick and adequate in case of. So, protecting, detecting and response in case of.

Researcher: Is it something you see at the other organizations that you work with that they value those principles as well?

Interviewee 4: No, not enough. When you read the [news]paper, you can read every day that there is a cyber incident in any organization.

Researcher: Is that something…? Sorry.

Interviewee 4: Nowadays we are still vulnerable.

Researcher: Yes. And let's say protection, detection and response is that something that would set your organization ahead of other organizations in the world of cyber security, compared to your competitors perhaps?

Interviewee 4: I am reasoning from the Navy. I'm not reasoning for [the organisation], because I'm not involved or responsible for IT at [the organisation]. What was your question again?

Researcher: Let's say you are looking at navies, if you look at [a European Navy], your value protection, detection and response, and if you look at other navies, let's say in Asia, do they have the same principles or do they look differently at cyber security?

Interviewee 4: I think it's the same, but the complexity of a naval ship, is that in an organization, you want to have a SOC, where you can monitor and response at time when you see abnormalities. As a naval ship, you're not always connected, so you have to do the SOC activities on the ship. The knowledge as well and that's probably because we don't have all the knowledge on the ship.

Researcher: No, it is a limited amount of staff that you already have trying to… That's why it's highly automated to limit staff and not to have too many. And then on top of that you need quite specialist who are able to do… Compared to other navies, they perhaps put in more staff which makes it less automated, less complex and…

Interviewee 4: One of the challenges of [a European Navy], in the future, in the near future, is to sail with less manning. Maybe you know the program: “Manning of Automatization”. Of that program is to think about IT-things and automatically-things, so you can sail with less crew. But it makes you affordable when you put more IT on board.

Researcher: Yes, indeed. There's always a balance to find between… Yes, indeed. If you look at the maritime industry in general, what would you say are the top 5, or top 3 of the main vulnerabilities?

Interviewee 4: When you talk about the actors, I see the state actors, the non-state actors like script kiddies, hackers and disgruntled employees/employers. That is top 3 of treats. And in addition, any member or staff, regardless of rank or function intentionally or not, or unintentionally pose a threat by ignoring or circumventing cyber security measures procedures. So that makes you vulnerable for all your systems.

Researcher: Yes, I remember that I one time heard a story, but that was 10 years ago when I started at the company, that somebody had plugged in an USB to look at pictures or to look at videos which was infected with a virus, so it spread out in…

Interviewee 4: It is a main threat.

Researcher: Yes, and then you can plug all the USBs [entries], but still people always find a way to misuse equipment unintentionally, of course.

I¤: Yes, it can be intentionally as well. What you see now in the way we are living now in Europe, in the Netherlands, with all the problems of energy and cost, very much cost, there will be employees, we have debts.

Researcher: Yes, who are in debt.

Interviewee 4: Yes. So when they meet some bad guys and they say: “Here you have a USB stick, I can give you 1000 dollars when you put this USB stick in your system.” That is that is a threat as well.

Researcher: Yes, indeed. If you talk about people who do that, it is mainly state actors who have the funding, but do you also think that it is for example criminals, who want to get information on maybe locations of naval vessels?

Interviewee 4: Yes, of course. What you see is that the Russian hackers are very active. Chinese as well. And they are 24/7 trying to get into the system. The benefit of the IT systems on the naval ship is that they are not Internet connected, which can be Internet connected when you put systems like he GMDSS or other communication to the outside and then you are connected to the Internet and then you are vulnerable as well.

Researcher: Which systems do you think are the most vulnerable? You said the GMDSS, other communication systems. Are there other systems that you think are targeted by attackers?

Interviewee 4: Can you hear me?

Researcher: Yes.

Interviewee 4: Hello. Yes, I am waiting for… Now I can hear you again.

Researcher: We are talking about the systems which are under attack. You mentioned the GMDSS and other communication systems. Are there other systems that you think are sensitive for attacks?

Interviewee 5: From the maritime domain region, from capabilities and the capabilities, for example the power supply or the propulsion or their steering weapon and sensors. So in any way we would be interested in influencing these systems based on this day.

Researcher: Okay. It's clear for me. So now we have looked at the threats and if you look at how can you combat those threats? What would you say [your organisation] can use, or the Navy can use to fight those threats? What do you foresee in the near future or for now?

Interviewee 4: Yes. What we are doing for the [project] is setting requirements for building blocks. And then you're talking about, for instance, hardening for the OS, network segmentation, applying a specific host based and network force firewalls etc. So that are the technical measures.

Researcher: Yes. Are there also socio-technical measures? So, user policies or things like that, that form integral part of it? Or is it more that you look at it from a technical side?

Interviewee 4: The business is the responsibility for the defence itself. But we can build something and [your organisation] builds something, what the Navy wants though, since when you talking about which user is allowed to use the system, you can make it in the technology. For instance, a VLAN is based on what the business wants.

Researcher: And if you look at… Let’s say, that the budget would not be a limiting factor, how would you make or how would you enhance cyber security on the ship? What would be your main focus?

Interviewee 4: By applying the most advanced IT protection, such as the latest firewalls, a SOC. Making a SOC. That is when you're not limited.

Researcher: No, indeed. When you have unlimited funding and unlimited resources. And if you would compare the maritime industry compared to other industries, because you have some knowledge broader in just the maritime industry. Are there similarities the maritime industry and critical infrastructures?

Interviewee 4: I think it's just the same, but for a naval ship, we are talking about a ship that's to be used in a war. So, the attacks are different. But when you're now looking to the Ukraine and see what the hackers has tried to disrupt the energy centrals, it's similar, but that's the war as well.

Researcher: And when you look at the maturity level? How would you compare those?

Interviewee 4: For [a European Navy], where we are in a growth process in which a [the project] is the first to be seriously provided with really serious requirements. And that will be growing in the in the next future. I think that what would you know nowadays see is that… That is why your question about budget was interesting. For instance, for [a project], maybe you know, we haven't spent all that money for the requirements we want. So, there's a less and requirements involved in the ship and [the project] the Navy will spend more money for cyber security.

Researcher: Yes, for the [previous project] was more we have a ship or a cyber security issue that we see from the outside. Can we do it? And with the [the new project] it's more we want to have a cyber secure ship. What can you do for that?

Interviewee 4: Exactly.

Researcher: Yes. Clear. Alright. I think it's all clear and answered. I'd like to thank you for your time.

Appendix I.V. Interview 5

Researcher: The first questions are more about getting or to establish sort of demographics of you and the organisation where you work at. Can you explain what your organization does and how it's related to the maritime industry and perhaps tell as well what size the organization is?

Interviewee 5: The organisation I'm working for is [the organisation]. We are mainly delivering projects and products especially for the maritime domain, so for the naval domain and for the yachting domain. Typical products we deliver are with respect to the bridge, so for the navigation bridge and also a part for the automation on board of ships. So, all devices for a ship safety for instance and automation of that. There's also an energy management system or power management system that we also deliver. It's highly automated and an IT and an OT, operational technology, driven product and projects in which we also integrate technology from our suppliers. The company size is approximately currently around 500, but we are still growing in a pretty high pace. The questions and the demands on further automation on board of vessels is only increasing.

Researcher: You see a market increase in automation.

Interviewee 5: Yes. What we for instance see is that there is a pretty high awareness about the possibilities with the automation with the devices that are currently installed on board of a ship. Traditionally called the industry 4.0. Everything today comes with a network plug and it gives you a lot of information that you can use for new applications to optimise your own, the navigation or automation or power management. There's a lot more of automation necessary to process all that data.

Researcher: Okay. And that's where you step into to it, to process it and to make it visible for users.

Interviewee 5: Exactly. That's our end user value. To make all the data and all the intelligence to make it available to the end user to make decisions or to aim for autonomous sailing for instance. When it comes down to cybersecurity, we don't deliver a separate product cyber security. So, we don't make an intrusion detection system that in our [organisation's] brand. But what we do is to make our products incorporate cyber security. We integrate cyber security measures in our products. Can you maybe just pause the records?

Researcher: Yes sure.

Interviewee 5: Because there's someone coming into the room right now.

Researcher: Okay, I think it started again. Yes, it is started. So, we were talking about the organization and what it does. Can you explain what your role in the organization is and how it relates to cybersecurity?

Interviewee 5: Yeah, of course. I'm one of the [department within the organisation] and within that department we have the Cyber Systems Group. We address on the one hand cyber infrastructure, so the whole network infrastructure, the virtualization and how that can be applied in the products that we have. Another topic is the cybersecurity topic and we differentiate in implementing the cybersecurity in the cyber infrastructure, so within our own group, but also supporting our other groups, which is for instance the [bridge] to integrate cybersecurity measures within the applications. Then my role within the group is that I started as the cyber security architect, so I made the first sketches of what does the regulation mean? What does the different standards say and how can I translate that to cybersecurity functions that can be implemented in applications or can be provided as a common service to the applications or can be integrated in the infrastructure itself?

Researcher: You look at the current governance rules, you look at the client specifications and then you look at their own product and see how it can match together to comply with the rules and regulations and demands.

Interviewee 5: When I got in three years ago there were a lot of program requirements from customers which already addressed cyber security in a sense. And there are a lot of different standards and what we did is, I said, “Okay, I'm going to gather everything that is requested from our customers. But I'm also going to look at the standard and determine what are the different topics that they address. So that we can make our own cyber security functions which you can specify and for which we can give the guidelines to the teams, or we can implement themselves which cover the different program requirements or the different rules and regulations.” Because in a sense, if you look at the different standards and the regulations, they all look alike. They may be slightly different in the wordings, but if you look at what technology or which measures and what's the governance process around it, they are all the same. Then we said, “Okay, we're going to translate that to our own standard so that we are not depending on which standard our customer requires, but we can make adaptation to the standard if necessary.”

Researcher: More like smart adjustments.

Interviewee 5: Yes.

Researcher: You're working at the organization for three years now. Did you do the same work at different organizations?

Interviewee 5: Before I started working at [the organization]. I was working for a long time for [an applied research organization]. That is [a research organization for the government], and I was always in the in the area of information security / cyber security. I even wrote for [an governmental organisation], a document or a guideline for how they should incorporate cyber security within their acquisitions. There's this set of requirements which they use in current acquisition so that they now get from the other perspective. Now I receive my own document with my specifications, which is nice. And I was always in a consultant way involved in the cyber security implementations for the [research organisation], the [governmental organisation], the government and also for a big telecom operator in the Netherlands.

Researcher: Okay. Clear. So, you have many years of experience you could say in into the information security, cyber security. If you look at the cyber security in the maritime industry, how would you describe that it has developed or what has changed in the last five years?

Interviewee 5: I think that the awareness is increasing. Some incidents always help and never waste a good crime. I think at the board level there is an increase in awareness that there is a high dependency and increasing dependency on the correct working of their operational technology on board of a vessel, which is also dependent and interconnected to other systems, instead of a standalone system, which they trusted a long time because it was physically separated from the rest so nobody could attack it. The awareness about the threat is only increasing. However, on the other side, what I see, and it's not only maritime but it's more like an industrial control system perspective, is that they always, and that's valid, they always have a high demand on safety, and that's where there's a difference between the information security, if you look at for instance also the standard as an ISO 27001, which describes your security management system and a typical safety management systems in which there safety is much more a dominant factor than data protection for instance. What you also see is that in the OT environment and the ecosystem they are getting more mature and products become available which take into account especially the specifics of an OT environment. In the last five years I think at the end at an awareness level they are increasing. The technology is becoming available to address cybersecurity within the maritime domain. And that the systems that you see integrated on board of the vessel are also increasingly based on a common technology for which already, the technology is available. So, at the tipping point of, years ago we didn’t know we were vulnerable, now we know that we are vulnerable and we also see the impact, so we should implement something and we should have a risk management system. To at the point

that, now there are also the security measures and the products are available, so now there's no excuse to do nothing.

Researcher: Okay Yes. That is interesting. The mechanisms or the technology is at a high level, at a certain level that you cannot say, “Okay, we have an incident. So that's a part of life.” You have to do something proactively.

Interviewee 5: Yes. Exactly. Another observation that I have is that, a few 3-4 years ago, if you said cyber security within the maritime domain, then they still compared it to, okay, then we're going to hire a cybersecurity specialist. Then a lot of the time there was a cyber security specialist from an information technology. Nowadays you more and more see that there is a separate domain the cybersecurity for an operational technology, which is significantly different than an IT environment. But it also becomes its own expertise domain, which makes it a lot more easier to have the right discussion for instance, also for us with our customers. I know now that maybe about three years ago when I just started over here, I had some discussions with customers. But I had a discussion with an IT security. So, then they come up with a lot of security measures and I'll tell you one. It is about, that the system should lock after 50 minutes inactivity. That is perfectly fine for your desktop environment. However, the commander on the bridge looks at his radar, but he's not going to operate the radar system itself. So, from a system perspective, it's idle and if he loses his radar image after 50 minutes, he will be furious. And then they didn't understand it and so that was a lot of discussion and struggle in the beginning. And nowadays you see, that they understand the difference in the systems on board of the vessel, and the discussions also become more easy and then you can also have much more a risk based security measure selection.

Researcher: Okay, yes. The qualifications of people are also increasing. They're more qualified now. Before it was either they didn't know anything or they were too much IT-oriented.

Interviewee 5: Yes, exactly.

Researcher: Okay, clear. If you look at ships, what would you consider a cyber incident on a ship?

Interviewee 5: That's a very good question. I find it very hard to qualify something as a cyber incident because if you basically if… There are a lot of events I think, but that doesn't necessarily mean that something qualifies as an incident. To me if you say are there are a lot of events on board of a system? Yes, there is especially in the in the transition that we are undergoing and also for instance means that sometimes you need to adjust your process on board of a vessel or also the process of deployment and commissioning of your system for instance. There are a lot of events in

the sense of that they are still misusing the system in a way which was not intended to be used. So that for me that becomes a cyber incident. Because we have for instance a staging system for deployment of our new update, but they don't use it, they just walk around with the [organisation's] USB stick and because it's still enabled, then they can just upload their own update locally. For me that's an incident and it's also detected, and it will generate an event. Does that mean that it's also an incident? For me, it becomes an incident when there's a disruption of the system. But if you look at: "Are there still potential attack vectors on the system?" I think there is. Also, because we cannot change the whole system overnight. There is the certification etc., etc. But it's a combination of it that we do not only rely on our technical measures, but also on procedural measures. The example I gave about the bridge which we cannot lock, for instance automatically lock. We also rely on the procedures, procedures on board of the navigation bridge in which it states that at every moment there is someone available on the bridge, because that's part of regulation, we can rely on the unauthorized access to the system because there's someone on the bridge, so we make a lot of notions.

Researcher: Indeed. What would you say are the main challenges for cybersecurity on board a ship?

Interviewee 5: I think the biggest challenge is to have the correct balance between a safety and a security objective. It is still used or abused from a safety perspective to say, "Okay, but that will violate my safety regulations, so we don't do anything." That's one big challenge. So that's also a mindset still. Technically I think we can adopt a lot of measures, which are common practice. However, there's a challenge about the connectivity and mostly external connectivity. And because I can install perfectly well antivirus on each system, however, I need to update my signature files every hour, every two hours and then I can still make it available in a controlled manner, which is staging area, etc., etc. However, the ship doesn't always have high bandwidth connectivity to get the newest update for instance, so that is a challenge. It will become less of a challenge because there the overall global connectivity will of course be more easily. Sometimes there is just no connectivity, or one decides to have no connectivity and then it becomes difficult.

Researcher: Okay, so it's a balance between safety and the ships operation and the challenge of external connectivity. That's the main…

Interviewee 5: Yes, and the acceptance of the user, but I think that's not maritime specific, that's in general. The weakest link is always the user and they need to adapt. So that's the challenge. And if you see it as a challenge, the biggest challenge is to show them the added value of security instead of making them afraid with new threat actors or whatever.

Researcher: Yes, okay. Which cyber security strategies does your organization promote on both ships?

Interviewee 5: What do you mean by security strategies?

Researcher: What would the [organisation] way of solving a cyber… For example, to find the balance between safety and ships operation. How does [the organisation] deal with that?

Interviewee 5: What we basically do is we derive our cyber security strategy or architecture from a standard. We took the DNV, DNV has a cyber notation, in which they state and it also includes an entire risk assessment and risk management phase. But they differentiate between different levels of cyber security, which can be applicable for refits or for new builds. Because you can imagine a new build, you have more freedom to have new measures implemented instead of a refit, because that's always limited. But we tend to challenge our customers, with a risk assessment to say what are the main risks that you try to cover because if they just say, “I want the cyber secure system”, then I cannot answer the question because when is it secure for you? Because in the end if you want no risk, it becomes a very expensive system. If you don't spend anything it becomes a less secure system. We try to get involved in the first part with the risk assessment and the risk management part so that we can derive and of course we have our own standard which we say, “okay, there are some measures defined also in the standard which you always get.” For instance, if you say, “Within the DNV they state the grouping of systems and zones”. So we say, “Within our infrastructure, from now on every time we are going to have a logical separation between for instance bridge systems and automation systems and we have a different VLAN for our common services.” We already separate the components within the infrastructure. We have a baseline and segmentation is one of them, but there are multiple security measures which we say, “Okay, we are uncomfortable to sell any system without these measures.” And based on that, this baseline, we start the risk assessment and determine, if you still think there's an unacceptable risk, then we have a selection of measures that you can supplement your baseline with.

Researcher: The strategy is actually to find out what the customer wants to protect, what he wants to achieve with having cyber security on board the ship and then based on that prescribe a set of rules and if there is more that the customer wants to achieve then implement that and state what would be the changes to the to the baseline.

Interviewee 5: Yes. We have the baseline which we find minimal set that we need to do. On top of that, it becomes a risk driven and risk assessment and together with our customer to determine additional measures.

Researcher: Okay. Clear. How would you compare this strategy to other organizations?

Interviewee 5: This strategy isn't rocket science, because every standard prescribes this approach, right? However, if I look at other organizations, they tend to be more like prescribing a set of requirements they just enumerate. For which I don't see where the requirements come from, and which risk they try to address. I see other companies prescribing the measure, but also the solution and that's something that I don't like, because if I don't know why I'm doing certain measures, I will most likely not adhere to the security consequences. If there's a difference, because what I said, the approach we take is just a standardised [approach], which I also see in a lot of other companies, but if there is a change, it's most likely that I see other companies forgetting the step of the risk assessment and just say, “Okay, I have a DNV or I have the IEC standard and I just want Level 3 without any explanation or reasoning behind it.

Researcher: Yes, without any option to change it.

Interviewee 5: No.

Researcher: Yes, okay. We talked about the major threats in the maritime industry before, but if you look at the systems, which systems which you think are the most vulnerable?

L5: Yes, that's, that's pretty hard in the sense that, in the end, if we look at the current and the future systems, they are all interconnected. In the sense of the chain is as strong as the weakest link. Then still if there's a weak link within this whole chain, the chain will break in the end. But having said that, what are the most vulnerable systems? I tend to say the legacy systems and because all the legacy systems were not built with security in mind. They were mainly built with a safety objective in mind and on the left assumption that they will never be interconnected with other systems. They lack any patching, they lack any form of authentication or whatever, so that they have pretty open systems. However, if they are standalone then they still stand alone. But I see that they are getting connected anyway, so that would be the most vulnerable system. Looking at entry points, then there's of course all external links which become becomes a potential entry point to the system. However, if I see how we how we implement them and how we separate them from the rest of the system, I'm not really concerned about that. They are all also pretty predictable in what traffic they will send. On the other side, what I mentioned in the beginning, we do the navigation bridge, automation, power systems. On board of the maritime vessels there's also an office environment. With just their office laptops and the connectivity with the internet and just to watch the movie or the quarterfinal of the World Championship, for instance. I think that they are secure. There's a lot

of awareness about security over there, but it doesn't mean that is the easiest way to get in the system. Because it's very unpredictable and they want to access everything, of course.

Researcher: If the path is known then it's easy, but because they want to access all information available then it's more difficult to see what's what are anomalies.

Interviewee 5: The system itself, the OT, that operational technology system, has a pretty predefined behaviour. But as soon as there are users involved with their own applications or mailing and websites or media. Then it becomes unpredictable, so it becomes very hard to determine normal behaviour.

R. Yes, okay. Clear. Which actors would you say cost most threats for the industry?

L5: That is hard as I'm then going to differentiate between the yachting industry and the naval of this world. Of course, for the naval it becomes a lot of state actors because they are afraid of espionage or disrupting their maritime ship during operation. They are less concerned about the rest of the actors. If you look at yachting, then there's a lot of awareness about espionage. Then it becomes more of the organized crime.

R. You mentioned before also, that, because I consider them actors too, own personnel that misuse the system. Would you say that is a bigger risk or would you say equally as state actors and organized crime?

L5: I think that if you look at the risk, in the sense of the traditional equation of the possibility and the impact. An internal employee for instance, they don't tend to abuse the system to disrupt the system. They use the system to make their life easier. The possible likelihood that they disrupt the system will be fairly low. However, because it is maybe daily operations or whatever that they tend to be more frequently in generating cyber events, but with a low impact. But for a targeted attack, as a state actor would typically be doing, maybe the likelihood is slightly lower because we tried to protect the system from those type of actors. But the intent is much more hostile. So, they would typically disrupt the entire system if they want to.

Researcher: Yes. The goal is to shut it down completely, but to have a maximum impact and the likelihood that they can achieve that is quite low. And with the own personnel and their own member of the organization then becomes the opposite. It's a very low impact, but because they used a lot, it could even out or less. In the standard risk assessment way. Let's say there's no limitation in budget, which actions would you take to enhance security on a ship?

Interviewee 5: That is a very good question. I would invest first of all in a lot more of the situational awareness, so logging and monitoring and making also a translation to actionable information. So, if I have a cyber event and there's an incident and it should be classified as a cyber-attack with a possible disruption, I want to translate it to the ship's capability so that I know that, for instance, if a bridge station is hacked, that I know, which capability will I lose if I lose at all capability because it's all highly redundant and whatever. But nowadays it's a lot of raising alarms but not making it the translations to a ship's capability. That would be the first thing that I would invest in. Secondly, I would also make it more easy for the end user. For instance, well what we did is, we centralized our whole user management and our account management. So instead of that they have to remember passwords for each system they have just one username, one password for all the systems. But still, it's a username password and they tend to hate that. I would like to make that a lot more easier for them. That where the two first things that I would invest in. Thirdly. but then it comes down to also the connectivity and how to be more predictive and also to have more patching and update frequently available on the infrastructure.

Researcher: A higher connectivity would improve security.

Interviewee 5: Yes, because it becomes possible to have more frequent updates and more frequent patching.

Researcher: If you would compare the cyber security on ships with other industries, would you say it's comparable to critical infrastructures? Or would you draw different parallels for the industry?

Interviewee 5: No, I think definitely that they should be seen equal, and they also have the equal or the similar challenges. And I tend to say that they both have an increased awareness and that they… A critical infrastructure or the in industrial control systems and the maritime environment, they are all at the same level in picking up the pace and implementing.

R. So they're quite comparable, you would say.

Interviewee 5: Yes.

Researcher: Okay. That was the last question. I would like to thank you very much for participating.

Interviewee 5: You are welcome. If you have any questions or whatever, you know, to find me.

Appendix I.VI. Interview 6

Researcher: Thank you again very much for having this interview with me. The first questions I have are more about how the organization is and how it looks like to establish a sort of demographics you could say. Can you explain what your organization does and how it relates to the maritime industry?

Interviewee 6: My organization is called [the organisation]. [The organisation] is a small entity within the [Parent Holding]. [The Parent Holding] is mainly a shipbuilder, ship design, shipbuilding and a little bit of services. [The organisation] is all about the development and deployment of remote monitoring solutions together with some remote access to the ship and a little bit of checking updates towards the ships before they are being deployed on systems on board. Those are the three main activities.

Researcher: So, development and deployment, checking and I missed the second one.

Interviewee 6: Yes. So, indeed the development of report monitoring solutions and bringing it into the market. The second one is what did I say? It's development, it's deployment, or monitoring, monitoring solutions. It is remote access, remote access to the ship, remote access to systems of on board of the ship. And the last one is facilitating updates and upgrades of systems on boards by having them checked based on the digital twin of the ship.

Researcher: Okay, clear. What size is your organization?

Interviewee 6: It is about 30 people.

Researcher: And can you explain what your role in the organisation is and how it relates to cybersecurity?

Interviewee 6: I'm the manager director of this company and at the same time, I've been in the lead of developing the tools we are using for monitoring and digital trends.

Researcher: So, you have a role as a general manager as well as development...

Interviewee 6: We started with a project. The project became a program with several projects. I was program manager and I have a mechanical engineering background. But I have been involved into digitisation and automatization in the last 20 years and. And I use a little bit of the experience to lead a team of professionals with expertise to develop the tools and the services we are offering to clients today. So it started as a program and then only a year ago we started to make it into a entity. To have more focus on the business.

Researcher: Okay. So, you have had different roles within organization. Yes, before and now you're focusing more on this part.

Interviewee 6: Yes.

R. So you have a broad background knowledge of how ships operate and how it works.

Interviewee 6: Yes. Before I worked at [the parent holding], I was working at operators at [dutch dredging company]. I think, you know [the Dutch dredging company]. I was working on the fleet, I was working on the technical departments.

Researcher: Okay, clear. So now the following questions will more be about, how do you view cyber security in the maritime industry? So, if you look at the maritime industry and let's say the last five years. How would you describe the industry and how has it changed, when it comes to cyber security?

Interviewee 6: When it comes to cyber security, if you look five years ago, then I think cybersecurity awareness was not that high. I think conventional ships have been designed to operate as an island, so without having a connection to the rest of the world. And at the same time in the last five years, each and every system provider has been automating and digitalising their products and by having that the opportunity comes to use that skills that capability of the system to get connected to other systems on board, but also to get connected to the shore. And the shore can be the supplier itself or the operator or any other entity. I think it has grown and by doing so, I think the awareness is lacking a little bit on the implementation of remote monitoring, remote access and I think in the last 2-3 years there are some steps made by IMO and IACS Class Society which helps increasing the awareness and increasing the efforts taken in making vessel cyber secure.

Researcher: Okay, yes. Clear.

Interviewee 6: But that is only at the start. It's only at the beginning, I think.

Researcher: So, if you would compare it to five years ago, it was non-existent and now it's starting to grow.

Interviewee 6: But we are still in the phase of awareness and having the first steps towards taking measures on cybersecurity.

Researcher: What would you consider a cyber incident on a ship?

Interviewee 6: To me, when there is a cyber incident, it means that there would be access or access to data, access to ship systems without having wanted it to occur. So, If it's without any deliberate access accidentally or maybe a little bit more hostile, if there is an intruder. But I think already if it's by incident, it could already be a little bit a cyber security issue to my opinion.

Researcher: And what would you say that other main challenges for cyber security on ships?

Interviewee 6: I think the conventional networks on board are not designed to deal with these kinds of threats. So, the communication is normally open, access to the systems is quite open. Which, was okay, because everybody on board was there with a permission. But that's changing. I think that's one of the biggest challenges. We have a little bit of legacy or maybe quite a lot of legacy of system developments which are becoming good and being smart and being interactive, but the companies which have designed and build them were not used to also take into account the cyber security risks.

Researcher: No indeed. And if you would look at the top five or top three main risk, which main threats do you see?

Interviewee 6: One of the main threats I see is that somebody on board is accidentally, making use of a network access or a system access and causing a threat for the system. That's I think one. The second is that there could be already some interference between systems because the new way of communication has not yet been evaluated when it is fully integrated. So, systems can communicate more, but it can also make some interference between systems. And of course, the last one is if there would be excess remotely or via the entertainment network on board. Then you could also, get access to systems which either you deliberately tried to get access to or by accident you get access to. And not understanding what you are doing and maybe causing quite some issues, some treats.

Researcher: So, the main threats are more internal threats you could say.

Interviewee 6: What I wanted to accomplish is… It's also on board. When I talk to people, they think about getting fetched from outside of the vessel, but the threats are already on board of the vessel. So, getting access to a network via an Internet Protocol is also possible when you are on board. So, when I go on the ferry and I used the entertainment network very often, the entertainment network is directly connected to the Propulsion Control network. Because they have a shared connection to a router. And then very often it's not that difficult to get access. Even it could be by accident if you get access. So, it does not only start by checking the modem which gives access to Internet from the vessel to the outside world or from the outset world into the vessel. I think it's also about the threats

which could be available because this unprotected network on board. By passenger or by maybe one of the team members, crew members, or maybe by a chief engineer entering the vessel to do a job. It is all good. But not taking care of in managing who's accessing the network. Do they have the capabilities and the permissions to do whatever they want to do?

Researcher: Yes. Indeed. And as an organization, how would you combat those threats that you named before so people use network without any permission or without authorized access, knowingly or unknowingly. the interference between systems that they can interfere with each other and let's say the remote access. So external part is going into the network.

Interviewee 6: What's your question? to prioritize this or?

Researcher: No, how would you counteract those threads?

Interviewee 6: First of all, whenever there is granted access to a ship in real life conditions, then I would call the captain if I'm allowed to go on board and then he will ask me to identify myself because before I accessed the vessel and I think in the cyber connection it's the same: Identifying whoever you are, getting permission to access the network and once you access the network, having restricted access to only those systems or those parts of the network where you have to do a job. And when you are finished with your job, normally you would report to the captain in real life, what did you do? What did you change? And I think this should also be done in the cyber security world, in the cyber security access. So logging whatever is being changed, updated and reporting these changes and updates. And when you are finished, I think in the real-life world you will ask the captain to go off the ship. I think in this case it will be the same and if you are not active on the network, I think by default, your permission will be discontinued after some time of not using the connection and so these kinds of processes, needs to be in place. What we do in my company is that we do this by using software and making it into a service and then accessing the vessel as the first state gates. And then accessing systems on board of the vessel as a second layer and of course on top of these tool, there's a need of protocols because you cannot do all the software you need to also people and hands. To have some agreements how to use these tools and I think these are the layers of protection, which I think are minimum to be applied.

Researcher: So, it is mainly based on user management. Granting access like you would have in real life situation that you are authorized to make some decisions or to make some changes. The same would be in the cyber world or in the network world.

Interviewee 6: Exactly and you could say next to that the networks, the systems designs as have been implemented on board should comply to some requirements and which maybe are not used today as a requirement. Starts with having a good quality, robust network by itself, having the basic elements applied to make sure that interferences are handled and not possible. And, starting from the quality of network, building up the functionalities which needs to be running on the network and having a clear definition of responsibilities, accountabilities. Even on system design.

Researcher: Yes. So, from the beginning of design, have it done in a correct way. So take cyber security by design.

Interviewee 6: Yes, cyber security by design next to cyber security managed. And I think that's also how the class society started to develop their rules and regulations.

Researcher: Let's say there is an unlimited budget. Which measures would you take to make a ship completely cyber secure?

Interviewee 6: The first measures, I would start with is looking at the kind of type of approvals on cyber security for all systems on board. All components and systems. Then looking into a level of cyber security notation to make sure that the systems combined in the full design integrated design comply to the minimal requirements to make it safe and finalizing with a kind of a management notation. To make sure that owner, users, suppliers or the other stakeholder would be involved, can comply with the process of getting access granted and making use of all these designs and systems in the right way.

Researcher: And if you would compare your solution of getting everything and all the steps correct. Do you see differences or similarities between other organizations in the maritime industry?

Interviewee 6: Yeah, I think there is a big difference in level of adoption and level of understanding. When you when I look at supplies of systems. Then the majority don't have a type of approval on cyber security yet. I think that very little vessels are having a notation, cyber security notation. And there are very little operators, owners, officers who have a cyber managed organisation in place. But there are some specialized companies which are ahead, there are some integrators in the market who are taking the lead. And I think that these are the front runners and I think that what I try to focus on is to work along with these front runners. So, the differences are big. I think it is not because they don't want to. It is because of awareness as if it is about the question how I see that class societies try to push but don't dare to disrupt too much because then there are too little to comply. And at the same time the insurance companies are looking into it. They try to push it a little

bit and operators of the larger sized vessels or larger sized fleets are looking into it. They are starting to take actions. And I think the smaller operators they're waiting.

Researcher: They just comply with the minimum set.

Interviewee 6: Yes, but maybe the risk there is a little bit less because they are very often not yet connected to Internet either. So, they also lagging a little bit on the adoption of these new technologies sometimes.

Researcher: And the budget is of course different compared to... A satellite connections for them is more expensive compared to for larger operator.

Interviewee 6: Yes.

Researcher: If you would compare ships to critical infrastructure such as power supplies or hospitals, do you see similarities in possible cyber incidents?

Interviewee 6: Yes, of course. The similarities are that big that I learned that it makes sense to make use of their knowledge, their expertise, and implement it in the maritime applications. That is also what we do. For the solutions we have; we have typical solutions for cyber security. We made sure that they have type approvals for cyber security, but to be honest, the requirements for getting a maritime type approval are not that high. What we did is that we involved companies from outside the maritime industry, because they are already at a higher level, so adopting their principles, their methodologies, their solutions makes it much easier, faster to get on a good level of being becoming professional.

Researcher: Okay, yes. You can compare, you can actually learn a lot from other industries.

Interviewee 6: Yes, often enough on the technologies can be directly implemented.

Researcher: But that's a bit the maturity level that you could say.

Interviewee 6: The maturity level yes. That is the right word.

Researcher: That it is much more mature compared to the maritime industry. And you can really see that it is still in the beginning phase.

Interviewee 6: The security is at risk, but at the same time, it is also an opportunity. The opportunity side is that it is really a client demand to have security on their data and on their access. And it makes sense. So offering a solution to that need, is a opportunity.

Researcher: Yes, indeed. And also, to be able to have connections and to actually test something before you put it on board.

Interviewee 6: And I think in some other industries, this awareness is there for a longer time and therefore the solutions are better because it is not only a threat and risk, but it also needs to be a solution which is easy to use because it is an opportunity. The users are selecting the cyber security measures which are easy to apply, which are not limiting too much in the daily operation, in our daily needs. It is connected. And giving access to data, access to vessels, is very often also a practical need. So having a solution for that helps also organizing access in general. Without having the cyber security as a main objective, granting access is just a need. I want to have Caterpillar to be accessing their engine on my vessel. And I want it today because I want to have a problem solved today. That is a need and it does not have to do something with cyber security, but please do it cybersafe. So, then it is an added value.

Researcher: So, there is a need to have all those connections available, and the question is how can you do that in a secure way?

Interviewee 6: An that is what you need to make secure connections with granting access. You are granting access anyway, so you can also use the access commercially. The solution for granting access can also be a solution for cyber security, but also for access other people as to commercial solution. I hope you can understand.

Researcher: You have the connection, you make it secure. So why not use it as an added value.

Interviewee 6: Exactly.

Researcher: Okay, clear. I think I have covered all the topics. I would like to thank you very much for participating in this interview.

Interviewee 6: No problem.

Researcher: I will stop the recording.

Appendix I.VII. Interview 7

Researcher: The first questions I have are more about your organisation and how it fits into the maritime industry. Can you explain what your organisation does and how it's related to the maritime industry?

Interviewee 7: Sure. [The organisation] is what we call a classification society. [The organisation] is in charge of classifying ships. It can be in terms of hulls, stability, safety, quite anything that is related to a ship, a vessel. More specifically, for five years we already test and also to certify cyber security for ships. First by writing a rule notes and then by applying them. What's interesting with [the organisation's] position on maritime cyber security is that we both interact with shipyards, shipowners, suppliers. We have a very centric position, and we can see all the challenges the various actors have. And then the form of the collaboration is, I would say, infinite. We can certify equipment, but we can also deliver feedback on design of a product that doesn't exist yet. It's quite infinite.

Researcher: Yes, quite broad. It is broad what you do, but it is more completely all over the maritime industry, with a large span of [influence]. How big is your organisation.

Interviewee 7: I don't want to tell something that's wrong. I think we are 5000.

Researcher: Okay. It's just to get the size [of the organisation]. If it is a small company of 10 [people] or if it's bigger.

Interviewee 7: It's quite big and global and the activities are performed all around the world, even for cyber security. Personally, I'm working at the office in [city of department]. We're a team of five and there is a local expert outside pretty much all the other areas of the globe.

Researcher: What is your role in the organisation?

Interviewee 7: I'm [name of interviewee], I'm a cyber security analyst, which means that I can approve design for ships equipment. And I'm also the proud father of the latest technical solution for [the organisation], which is the network discovery tool, which is a tool we aim to use in a few years to make sure that the plans that we approve are what's effectively on board. Because as we may talk about today, the main challenge is the visibility and sometimes the gap between what we think there is on the ship and what is truly on the ship.

Researcher: Did you always have this type of role in the organisation, or did you have different roles at different organisations as well?

Interviewee 7: My background?

Researcher: Yes.

Interviewee 7: I obtained my engineering diploma or master's degree in Engineering and specializing in cyber security. And after a short period of operational security in a SOC, I dived into [the organisation] and it's now three years that I'm at [the organisation]. Three years and a half, sorry. Time flies.

Researcher: So you have also knowledge about other industries, you could say?

Interviewee 7: Yes, I have, I would say generic knowledge about cyber security, but since, I think my knowledge has got very much précised on ships and also the maritime industry, but it's in broader ways, [such as] ports, etc.

Researcher: The next questions are more about the views that you have on cyber security in the maritime industry. How would you describe cyber security in the [maritime] industry and would you say it evolved in the last five years?

Interviewee 7: With pleasure. I think this is a very broad question. I have this feeling, because of the central position of [the organisation]. Cyber security in the maritime industry can be translated to multiple challenges and each of the stakeholder has their own. I will try to have maybe a bottom-up approach, starting with the suppliers and then translate to the shipyard and then to the shipowners. Because these are today the three stakeholders that we see interacting on the cyber security of a vessel. If you take the problem for the beginning. Suppliers are producing equipment systems that are made to fit on a ship and at those first states the challenges for cyber security is how to make a product that is secure by design. At this point you have many challenges: Network, […] services, communication. And this is, I would say, the most practical security. These challenges translate to the shipyard. The shipyards have to make sure that at the integration time, and the integrators also, have to make sure that the integration time, the initial configuration in which the ship is delivered, is still in conformity or in compliance with regulations. For instance, making sure that the installation process was paying respect to the suppliers demands. But also, that interconnecting multiple equipment, because a ship today is more and more connected, especially with the needs for data that is related to decarbonization and more sustainable shipping. This makes a challenge to interconnect equipment that need to operate or share data. Of course, from the cyber security point of view, this adds complexity and the challenge for the integrator and the shipyard is to make sure that connecting the systems to another [system] does not affect the global ship level of cyber

security. And once the ship is delivered to the ship owner. First of all, of the ship needs to be in an initial condition that is first of all quite good. Then the ship owner has to first take knowledge of that configuration, which is an important step that is today not always taken. And then [the ship owner] has to update the documentation all along the life cycle of a ship. Let's say ships, and I'm not taking any specificities here, can be bulks [carriers], cruise ships; because then the challenges are even more specific depending on the type of ship. Ships life is 30-40 years, of course you have to keep the equipment updated and some at some point make some change to make the level of cyber security match the era that the ship lives in, of course, and the threats are not the same. Maybe a year ago there was not the same threat levels. The threats are evolving fast and so must evolve the ship designs. This is in the end with the ship owners. If we have this approach from bottom up, we can say that most of the requirements apply to the upper layers of those stakeholders and the issue is that there are no compulsory requirements that would involve suppliers and shipyards into providing the ship owners with the initial inputs that match the requirements. Today, the pressure is on the ship owner's side and a key aspect of the upcoming regulations is to lower a bit the pressure and to make it more mandatory for shipyards and suppliers as we see with the with the users. The users are aiming to involve more the suppliers and the shipyards into building the initial documentation needed and the initial configuration suitable for a ship.

Researcher: In order to make the life of the shipowner easier or to have it more controllable.

Interviewee 7: Correct. To make the initial inputs that the ship receives at the commission period of a ship more accurate, easy to maintain. This is also a change because when the ship owner receives PDFs while the question of maintainability of such documentation is a question. I think it appears a quite dumb question, but this is an issue that we had at [the organisation] when reviewing and certifying documentation with ship owners are sometimes unmaintained. I think this is the real-life example of the struggles of the stakeholders.

Researcher: If you look at cyber security you see it as from bottom-up and then it starts with the suppliers having everything in place, meeting all the requirements that are given, followed by the ship builders or the yards applying it correctly and making sure that everything is according to the documentation. And then at the last step where the most work is, is the ship owners, who have to maintain it for the years to come or for the years that they use the ship. Thank you. That was a big summary.

Interviewee 7: That was a big question.

Researcher: I summarized it maybe too much, but I will keep the main thought behind it in mind. And if you look at the different systems on board the ship, which system would you say that are the most vulnerable to cyber incidents?

Interviewee 7: I think again, it will be a quite long answer. Sorry for that. A chance that we have at [the organisation] is that we see all type of ship. Except inland maritime, but this is another story. Of course, depending on the ship that you are assessing, if it's an LNG or bulk carrier, a cruise passenger ship, the key component systems are sometimes different. There are similarities between them, with the most known example of the navigation systems covering the critical components such as GNSS, GPS and then the insecure by design AIS, infamous. I think those signals that are driven into what we see more and more is an integrated navigation system which cover and make sure that every navigation component is in the same network such as Autopilot, giro-pilot, every sensor that I aim to assist the cruise into taking a decision to drive a ship. Then you have the other part with the machinery, the propulsion, the AIS, which is more and more interconnected in order to perform data telemetry, meaning more and more connected, meaning more and more exposed in terms of cyber-attacks. And I think I will stop here. So, then you can have some specificities for each type of ships of course. For instance, LNG carriers all the LNG system, which is mended to make proper energy transactions are key components such as the loading computer on bulk carriers, we know that this is the main surface of attacks for fraud operations in port area because these components are quite vulnerable for now. And then on when you have a cruise ship, you have a very critical systems, not for the shipping service, but for the passengers and depending on the level of experience a cruise company you want to provide the guests. Some of them are very luxurious and you can see, for instance IPTV as a critical system which is in fact questionable because of course IPTV is not… You are not going on a cruise to watch TV. But for some companies this is a truly important system and for the passenger's experience must not suffer any trouble due to cyber activities and IPTV might be targeted as such.

Researcher: So, it is a brought the range of threats. There is a lot to do in cyber security. Going a little bit back, if you look at the incident, what would you consider a cyber incident?

Interviewee 7: I would say to the [organisation's] risk methodology that defined a bunch of scenarios and this is freely available on the Internet. So I think you might want to refer to it later. We defined a bunch of scenarios, of attack levels, because when we assess the risk, But we define criteria on some keys area of each system. One thing that we consider is the attack level. So first we have what we say: Unintended behaviour. That behaviour is meaning crew members triggering conditions on an equipment that is not supposed to be triggered. Let's say you want to operate the propulsion and

you do a misconfiguration, and then it breaks the engine. This is what we called the unintended attacks. Then there is what we call bypass attacks, meaning for instance on a passenger ship, people wanting to have free Wi-Fi. They have a bunch of knowledge, and they want to bypass the current regulation. This is not malicious of course, but this is what we call bypass attacks and then we start entering into the malicious operation. We first standards that attack level. So I would say you could for instance scan the IT network of a ship with a basic knowledge, common tools, I don't know [E.g.,] Nmap etc. And for us this would be already a cyber incident because most of the time, I would say the ship architecture is not built, so that behaviour would be caught. And then you have more serious threats coming up, with the cybercrime ecosystems, a ship can be seen as a standard information system, even though we have to admit that we never saw such scenarios applied in reality. Most of the incidents hitting the maritime industries are related to port stations or onshore business infrastructure of a company. Because the ship's got a unique connectivity points and those on port are… Well, that's a kind of a requirement, because it's so critical, but those end points are very hardened and most of the time well protected. And last but not least, of course there is the state sponsored activities. This is quite a touchy subject to discuss, but I see that we saw a nice examples of what it will be with the ongoing conflict between Russia and Ukraine. I think we had a lot of research at [the organisation] done on for instance could an event like the that said event, I'm not sure if you are aware of it, but could an event like that apply to the maritime industry target on purpose the maritime industry, some companies and what would be the consequences of such an event. So I think we see a bit more clear in some threats that are high level and I think this is not an unlikely scenario anymore to say that this is technically a possibility. Again, a very long answer.

Researcher: No, it is okay. It is quite clear. Take it from the view of [organisation]. So it's quite good.

Interviewee 7: I think I can give some precise examples maybe because of course there is a common set of attacks that we always consider when assessing the risk. There is the well-known, I would say spoofing and jamming of the various equipment onboard. GPS, GNSS, AIS also. So more and more the GPS communications are more secure with source authentication. For instance, Galileo step out of the game by introducing this, I think it's called OS-NMA which authenticates the sources. So performing spoofing and jamming on GPS signals is getting more and more complicated. But the true system that will never disappoint people is the AIS because the AIS is not built to enforce security features, so I think it's still quite easy to spoof a ships or stuff like that. And of course, this is maybe a topic that will be under later depending on the will of the organisations. And I think this is quite the common attacks that you can perform to disrupt a ship’s network. Of course, there is more advanced scenarios where you have a connection between the OT system, either the navigation or

the OT, and then a lot of research are done on how to jump from the IT space to the OT space. The disappointment comes from the fact that if you succeed into achieving such a jump, then having malicious attacks that could jeopardized the ship safety, it's quite easy. So for that I think as a student you might have read “The Great Disconnect” which is a report which we are not in, but we always look in it because it's good quality. The Great Disconnect is a CyberOwl report. Maybe you have heard about it. It states that an actor performs disruptive actions of a ship in a time duration which is comprised between 2 and 12 hours without knowing anything about the maritime industry. So, it's quite concerning.

Researcher: Yes. So, it doesn't take for example, a state actor or a malicious user if they really want it, they can easily spend 2 to 12 hours.

Interviewee 7: Of course, unlimited time and money we consider when assessing such.

Researcher: It is quite viable indeed. How does your organisation deal with these cyber incidents or let's say cyber security threats?

Interviewee 7: I would say, that we are not involved in the operational security. So, all we do is… Where to start again… First of all, we are having an impact on regulations. So, at [the organisation], back five years ago, we were to own rule note the NR 659 which define a various level of requirements. There is, I would say, basic standards to match the current requirements. So as such we have class notation for ships which match the IMO guideline. And then while we can speak about the IMO guideline, this is the first step. Of course, this is not sufficient because there are no technical requirements, but this is the first step and the goal of [organisation], is to provide a way for a ship owner to be compliant with that rules and certify. This was the first step and then we have I would say in new rule note [Rule Number from 2020] more advanced requirement for ship owners that want to tackle the cyber security issue at the design level and make some efforts into technical implementations, which is called the Cyber Secure Class Notation. And in that requirement, we do include very demanding requirements on for instance the way you operate a remote access to the ship. Even at a system level. What does this remote access serve as a purpose? Is it telemetry, operation, management of the system? And depending on this mode of communication we define requirements that can go of some basic techniques such as VPNs to I would say very advanced technique with Bastion and Bastion host and DMZ implementation and to prevent malicious activities from those remote access and then of course a lot of network rules etc. And as you may know those requirements are evolving with the introductions in 2024 of the UR E26 and E27. Shall I describe them completely or?

Researcher: Yes, in broad lines.

Interviewee 7: If you want it. So, the IACS, which is the International Association of Class Societies, has released the UR E26 E27, of course [organisation] is a part of those requirements writing and I can say that that [name of former employee], which is our former boss, was the chairman of the IACS on the Cybersecurity Panel. So as a classification to say, we have a word on the regulation that are pushed through the maritime world and those who are in E26 and E27 are unified requirement that aims to enforce the collaboration between these stakeholders. First by defining what is cyber resilience for a ship and with a bunch of requirements that are dedicated to involving the shipyard and then by defining an equipment level, what would be the technical requirements, that an equipment should follow if you want to be installed on a ship. Those requirements are mainly extracted from the IEC 62443, which are common guidelines in industrial control systems requirements. This might not be a surprise; this is the first step because there is only 40 points, that are taken on from the IEC and the IEC is a very big document with a lot more of possible requirements. But the idea behind those unified requirements was to say, "The IMO-guidelines define how to analyse the risk and manage the risk, but without having any impact on technical requirements." So no reviewer. This is the big change. There are requirements that have to be followed. They are not very demanding in all the others industry on shore, this is more demanding. But this is the first step of course and everyone has to step up his game. And the idea is not to say, "Okay, you cannot do that, you cannot go on a ship." The idea is to be, I would say, more on the collaborative aspect and raising thus the level of the whole industry by forgetting no one and making it accessible for everyone. So that's the world of the URs. In a few words.

Researcher: Perfect. Thanks. If you look at… Well, you covered it a little bit. If you look at threats of the maritime industry, what would you consider, let's say the top 3 to top 5 threats to ships?

Interviewee 7: I would say the, there won't be even lower in the ranking, but of course the electromagnetic activities that are related electro… I think that is the English word, sorry that are related to spoofing or jamming right signals. I think what is first is the GPS and GNSS because sometimes those signals are used to take automatic decision, if you have an autopilot plugged, so it could be quite effective. Then of course this is an assessment between likelihood and the impact, because if you have a high impact but that never occurs while it's not worth considering. I still think that is has not yet happened, but I think we should be very careful and fear such an event is a supply chain attack on the system because, this would enable not a ship attack but the fleet attack or even more so for instance with a back door piece of code or on a system that is implemented on board, that would enable each time the system is deployed to have a remote access to the ship and then

perform operations. And the supply chain, I think is a subject that is cross industry, not only the maritime one. But the challenge with the maritime industry is that the equipment is never updated […] for good reasons, because sometimes it's totally isolated. But with the digitalization, we have to have that in mind when we are building a ship, because what's isolated at the first step of the ship will become connected and then if you have such components that are backdoor by supply chain, then this could be very impactful. I think I will stop there then. Of course, on the IT part, but that's more true on the cruise vessel. the personal data of the passengers, everything which is stored potentially on board is a critical component and that could be targeted with much more standard tools by attackers.

Researcher: Indeed. That part is less, you're less able to control what the passenger takes onboard.

Interviewee 7: Yes.

Researcher: Yes, indeed. Okay, so let me see if you would consider there's no budget, so you have unlimited budget, which action would you take to enhance the cyber security on a ship?

Interviewee 7: This question is, I would say, I do also have to not mix between the reality and what I would see as a person implemented on the ship. Because for instance, let's talk about dreams. I think a full monitored out network with tap device, meaning a separated instance for monitoring with an onboard SOC is not something that is going to happen, of course. Even with an unlimited budget, people will find better ways to spend that money. But on very practical actions, I think… This is very hard, because we aim to provide that low, of course, cyber security for maritime industry. So, what would matter the most and that would be cost efficient and that no one is doing, would be a regular check of compliance and architecture knowledge-based updates. This is very basic. That response must disappoint. But this is a step that still needs to be taken. Most of the time it's not about even money, but skills, and that is something that I think is still a challenge today. Of course, this is to be taken with the way that every shipping company has its own standard, so some are very advanced. I don't want to say, “Everything is bad, and we are nowhere.” No. There are very advanced companies that are way above the standards, but most of the time such basic requirements might apply and might be useful to consider for a shipping company, that has newly unlocked the budget.

Researcher: So there are quite some steps you could take without investing a lot, but by having the proper knowledge.

Interviewee 7: Yes, and internal knowledge. At [organisation] we are very happy to help. But of course, I think there is a challenge coming to ship owners, if they are relying on external help. Which is good for us, but of course we are also very keen when we meet shipowners that have internal knowledge and ways that we can start speak with on every aspect and understand why we are, for instance, seeking such documentation, why we are thinking that their level of documentation is insufficient. Because sometimes we have to explain why.

Researcher: It is good to have to have a conversation on a similar level.

Interviewee 7: Yes. But the role of [the organisation) to step up the game.

Researcher: To be a little bit higher and to pull it up, maybe that's better. And if you would compare the maritime industry to other industries, how would you say, for example, that the maturity level of the cyber security in the maritime industry is compared to perhaps the healthcare with hospitals or critical infrastructures with power supplies?

Interviewee 7: That is a very tough question, because all of the systems we know have caveats. I'm living in France, so for instance the healthcare architecture is also subject here. And I think in the US we saw recently that the critical infrastructure wires were also not in his best shape and need investment. Also, as I mentioned, I have no background in others industry, which make this question quite uncomfortable for me. But I would say, that we do not have to merge the level of maturation industry have without considering the level of threats, because it's true that onshore, the activities can target maritime companies as any others, and that the onshore system has much the same requirements that others. So, I would say that this part of companies is as mature as the others and then translating to a ship those requirements is more a challenge than we can think. It's not something that we say, “Okay, I've done it onshore, I have quite secure.” Of course, the level zero risk does not exist, but you say, “Okay, onshore I have some solutions” Well, they are not transposable to a ship because there is a challenge, there is the bandwidth issue that makes that the monitoring real time is not possible. As simple as that. You do not have on the field experience, you hardly have a cyber expert on board, because otherwise a lot of people would have a good job of doing cruise or traveling with a ship only to have the cyber security responsibility of the ship, which is I think is a nice job. But this is not understandably in cost terms, because the stress levels are too low for now. What was the question?

Researcher: So how would you compare the maritime industry to…?

Interviewee 7: Yes. Before answering, I will add something that I already mentioned; Is that the level industry is very heterogeneous. We truly saw every single situation from the very impressive architecture with the very well managed one and then the totally bugged one which is blurry, and no one knows where is everything. So, this is very heterogeneous and if we take the industry as a whole, the lack of requirements is playing on ships make this industrial a little bit less mature than the common ground. I'm not speaking about banks or our key component, but I would say there are regular IT companies, the cyber security of the maritime industry is quite lower. But I think this is due to the context of a ship and that where you feel isolated because of the satellite connection, but in fact you are not. And then it is not urgent when you connect the ship to the ground at the port station when it's at the yard. So, I think this is a false feeling that you cannot leave the ship.

Researcher: The false feeling of safety. Let me check my questions if I have any other things. No, I think you covered it all. I would like to thank you very much for participating and for helping me. And I will stop the recording.

Appendix I.VIII. Interview 8

Researcher: And I think it started now. Yes, it started now. The first questions are a little bit about the organization and to establish the demographics of where you stand. Can you explain what your organization does and how it relates to the maritime industry?

Interviewee 8: [The organisation] is a provider of energy storage solutions. So, we provide often to system integrators battery systems for hybrid electric vessels. And that's our main focus to provide energy storage solutions. Currently it is batteries, in the future it will be fuel cells and a quite imminent future. We are currently the market leader. Picking up [a large part] of the global market of energy storage solutions. We look at that over in the headquarters in [the north of Europe], but the engineering department are located mainly in [North America]. With sales offices also around the world and tech sales and so on globally. Our fuel cell department is also located in [the north of Europe].

Researcher: Okay, clear. And about what size is the organization?

Interviewee 8: 250ish. 250 employees. Approximately a bit over 100 in [the north of Europe]. A bit under 100 in [North America] and the rest is spread out worldwide.

Researcher: And can you explain what your role in the organization is and how it relates to cyber security?

Interviewee 8: Yes, I am the global responsibility for regulatory affairs. I'm keeping track on the classification societies and what they bring up of new requirements and also flag states. And also, all the requirements such as fit for 55 and so on, but that's not very related to cyber security anyway, but I am trying to connect all the different stakeholders internally to try to pull together to get those above and beyond the requirements, of course. And also, then cyber is part of that. And we have a compliance team working with our engineers, working on bits and pieces on the product level to ensure compliance with the requirements and we also have a digital department section which works with analysing data and getting information from the systems on board. Currently it is only one way. And using that data in a good manner. So that is not a product level cyber issue, but it is still an [organisation] issue. But we also have a… So that is pushing it a bit to more towards the IT department for [the organisation], assuring that the data we get from our customers we did that safely as possible and also the gateway to the ship. Even for the future when we will try to get durable both way communication. This is quite an important, to keep track on cybersecurity. Even more when you have a both way communications.

Researcher: Now the cyber security of that part is more related to one way traffic but in the future will be made for two-way traffic and then the additional complications that arise will have to be tackled. Okay, yes. Clear. So how long have you been in this position at the organization?

Interviewee 8: I joined [the organisation] in February this year, but prior to that I was ten years with the [national maritime authority], responsible for green technologies such as batteries and fuel cells and ammonia and hydrogen and all the fancy new fuels. So, I came from a regulatory background, but prior to that… I'm a merchant, so chief engineer, educated chief engineer and used to sail on ships. So, my part has taken me where I am today. But I'm not educated within cybersecurity, so it is just based on background and training.

Researcher: But you have a big background in the maritime industry. So long. And if you look at cyber security in the maritime industry, how would you say that the landscape has changed in the last five years or maybe 10 years?

Interviewee 8: It is 10 years since the last time I was working, or 11 years since the last time I worked on a ship and I hope things have developed a bit since that. Because then it was it was quite rudimental, very limited the focus on cybersecurity and what was connected and what wasn't connected. So, I know it is better, but I haven't tested the systems, I haven't used them on… It is also a part of the culture on board. You can build any systems, but if the crew aren't aware and if the crew are ignorant of the threat, then it is difficult to make a system that can withstand somebody opening things up, plugging in. "I found a memory stick, should we check what is on it?" Making its fool proof is difficult. So, it also needed to have a change of culture on board the vessel to make them aware of the threat from the cyber security. I think the vessels that are probably more targeted than the other ones have that focus, such as large passenger ships and so on. But when the systems get more connected, then even all ships could be a threat to someone or something. Hopefully they have quite good focus on this when they develop autonomous ships. I once thought of the discussions of the vessel Yara Birkeland and it was a great focus from the system integrators and DNV and NMA to keep track on that. So, I think the first ones will always have focus on that, but you need to still have focus on the vessel #10. When you get more and more automated functions, several of the ferries Norway have automated the fjord crossings and automated docking and so on, when that systems are pushed out to the market, so that everybody has something like that, making the ship quite vulnerable also for attacks.

Researcher: Yes, indeed. Do you see an involvement in, or do you hope more for…?

Interviewee 8: Yes, we get a lot of more questions, but we get a lot of more questions from the companies you expect that ask these questions, so big companies with large assets, where they might have already been exposed to something. But there are still a lot of boat-owners and vessels that don't ask these questions, so there is still a lot of room for improvement. Typically, that's the smaller ship-owners, the smaller vessels and so on, where you don't have those questions raised. But those vessels also need to have focus on these and those ship owners and their systems they are using more the system integrators and everybody on board those vessels are not at the same level as the ones they were delivering to the larger vessels or to more special vessels and so on, and there is focus on it. And it is new for all of us used… They have probably done the right thing to get training and education within this, but it is not something that a typical automation engineer has a lot of focus on or at least have a lot of knowledge about. It is something that this whole industry needs to pick up on a bit. When the global requirements come in 2024, it's still quite… It is not very strict requirements, but it will at least start something.

Researcher: Yes. It will start the process of thinking and…

Interviewee 8: And I guess that is quite wise of the classification societies to not go from zero to 100%, but when they start introducing at least get in place some basic requirements, so the industry starts to think about this and then the requirement can evolve.

Researcher: Okay. Clear. If you look at a cyber incident, what would you consider an incident on both of a ship?

Interviewee 8: Basically something, that shouldn't be there or present. I don't like, somebody getting access physically through getting an open network port or something where they can get access to something that they shouldn't have or as malware software gets into a place in the system where they shouldn't be. So, when somethings are present, that shouldn't be there. It can be, in many cases, that they are not able to do any harm, but that's if they get their access the first time and are not able to do any harm. That is still a failure for the cyber security, because they got in. So, you can't say that you had a cyber incident only when something was damaged, or they caused them an incident.

Researcher: It is not only what you notice immediately, but also what's happening in the background.

Interviewee 8: Yes.

Researcher: Clear. And what would you say are the main challenges nowadays on board of the ship for cyber security? You mentioned awareness before.

Interviewee 8: Yes, crew awareness is something, but also who is responsible for the whole system integrity because a vessel is not something that's built by one single company and like for instance, a car, they were the manufacturer and also doing every single system on board, so it is much more diverse onboard a ship than most other entities, because if you have a company, an onshore company, and then that company is responsible for establishing the correct infrastructure […] the protection. But when you order a ship, you have a ship owner which doesn't own the ship [yet] and when it's in the yard, just forward the requirements. And the shipyard will often only do mainly steel work, basically or more or less build the vessel itself. And then you have a huge load of different systems and manufacturers, and they all connect in something, and you have the systems integrated, which take part of the propulsion system and then electrical grid and so on. But then you start to connect to the online [world], the ship's computer system and you connect the navigation equipment, but that's not part of the system integrator skills in many cases. So, who has the total ownership to ensure that this system have the correct robustness and doesn't have any open access points. And putting that responsibility to all somebody it is when the ship is in operation, that responsibility falls to the ship owner. It is difficult for the ship owner to have control of all, and I guess they will be a bit in a dilemma to point towards who they put in charge of ensuring that the system is okay. But prior to getting the vessel to the shipowner. Who will take charge of and showing the quality of the system and confirm to the shipowner that this system is, or whoever is certifying this system, who will take lead and ensure that all the system manufacturers connected to the grid are compliant with whatever they need to be compliant but making it a system.

Researcher: You mentioned before… So you have propulsion integrators, you have people who take care of the power grid of a ship. Are you saying that it's lacking, that there's someone to be responsible for the cyber systems as they would call it, or the IT infrastructure?

Interviewee 8: Yes. Because I guess the system integrator would take up a huge share of that, but then we would have navigation equipment that would be needed if that's connected, if you got on board entertainment or on-board server or infrastructure for onboard computers and so on. And you also get that connected into the same system. Because in many cases there are not that many connections off the ship, so they all need to be connected to each other somewhere and having that total responsibility for the IT or cybersecurity infrastructure on board a ship that it's not easy to point towards who should take that responsibility. Does [your organisation] want to do that or who wants to take that responsibility? Because it is a complex system and it is okay to be responsible for

your own deliveries to that system. But when you get all of these things connected and at different levels and so on. Who is? Everybody can say they are compliant, but when you can combine so many different systems are they all together compliant when you put it in a system?

Researcher: Yes, indeed. That is always the big question.

Interviewee 8: And for the electrical system if we go back 20 years, when they started to be more automated, the systems onboard ships. The system integrator came and took that role to have the control of the systems, getting the systems working together, getting alarms and getting all of these things working together. But now we have a new challenge, which is pretty much similar; getting all things functioning together. But it is still at a different level in the system. But it could still be a system integrator that takes that role. But it would widen the scope of the system integrator when they need to ensure that all the IT infrastructure is sound for towards cyber. But somebody needs to do it.

Researcher: If you look at your own organization, which cybersecurity strategies does your organization promote?

Interviewee 8: Unofficially [the organisation] was [exposed] a few years ago by externals. And after that there has been quite a lot of focus on this safety access, being aware of the emails having a huge focus on getting out spam emails. Not using memory sticks and so on. And we also recently hired two guys. Most of our IT systems have been supplied by external parties until now. So, all the IT infrastructure has been more or less handled by a third party up until now, but now we have hired two guys, one will focus more or less only on cyber, but both of them are from the financial world. So, working on cybersecurity and banks and so on. I think we will see change. Until now, it has just been a focus area, but maybe lacking the total strategy for the whole [organisation]. Not a set strategy, it has just been that you need to be aware, you need to be careful as we have been exposed to things prior. But with those two guys on board, I guess we will see… We are already seeing changes in how thing works. But I guess also the whole strategy and so on will be developed quite soon. And the guys working on the software for communications and so on, they are… We're still quite a small company, so the guys working on software… They have communication between onshore and vessels they can build together with the cybersecurity guys on our own IT and systems, as well as for the BMS where you have software and so on. That's the benefit of not being 1500 guys or 2000 guys. Even though it is not their scope, the new cyber or the new IT guys, we can pull them in on product level as well.

Researcher: Yes, they can think about it, they can give advice. You could say that [your organisation] has. made step of awareness and now it's implementing the easy gains and you foresee that in the future will be getting more advanced and the same will happen for the products of [your organisation] itself. If you would look at your organization and would compare to other organizations, how would you compare it? Regarding cyber security. Are you on the same level or do you think it's more advanced or less advanced.

Interviewee 8: I think we are not way beyond anybody else, but I think comparing at least ourselves to other battery suppliers, I think we have a lot more focus on data and also than people that knows programming, cyber software and all of these things. And we have had the incident when we were exposed to it, so it raised awareness quite much. Even though it didn't damage anything. They crashed a few computers and so on. So it wasn't an attack for getting information, it was more, I guess a random incident that were more towards breaking our system or breaking computers and crashing computers and so on. More than a dedicated attack to get information. But still, it raised awareness. So I think we are better than some, but not best. And we are focusing quite a lot on it now. So, I think we are well positioned for upcoming requirements. I guess in 2024, when we come to those requirements, I think the most stringent requirements will come from big ship owners, more than the requirements of the classification requirements, the most difficult questions will come from the industry itself by then. That will challenge us, but it will also push us in the right direction.

Researcher: And if you would look at the top major threats or five threats of the maritime industry, what would you say that… Which systems are the most vulnerable to attack?

Interviewee 8: I would guess either navigation equipment or [electrical] systems getting a shutdown on the vessel could be critical as well and the easiest. But breaking and bringing a shutdown could be done through other systems as well. So, if you get a falls or if something else does something. If somebody gets into our systems and most of these things are the shutdowns and so on, those are mainly hardwired and not something that you could change through connecting it to a computer. Those are embedded into the chips itself. Getting a battery system to shut down during a cyber-attack, could be, should be at least, difficult. They probably would manage some way, but it shouldn't be easy to trigger that. File systems give false value to trigger or shut down. But there are probably access points, that could confuse the system, making it this whole system being crashed or something. So if you change the values and so on, then it will cause confusion at least. But I guess for a typical… I guess I would be most afraid for the navigation equipment.

Researcher: And where would you think that the most threats are coming from? What would you consider the main sources of those cyber threats?

Interviewee 8: It all depends on of the vessel, of course, and the operation. For the oil and gas industry I would be afraid of people from a bit east of both Netherlands and Norway. Because if you are during a DP operation, if somebody screws up your DP, next to oil and gas installations, it could damage it quite a lot. At least you would get a shutdown of that production site. For passenger vessels I would guess they would weigh more typical people out looking for ransom. So, a different set of people.

But for container liners and so on, that would make an impact to global trade. So, it is probably a more political level as well as for the oil and gas. It all depends on the vessel.

Researcher: The game could be for the, let's say either the different states or criminal organizations. Let's say there is no limiting factor in the budget. What would you do to enhance cyber security on a ship?

Interviewee 8: I guess it's not a budget factor, but I would put somebody in charge pointing to one entity and give them the responsibility to ensure that the cyber is handled. And that shouldn't be a… It would come at a cost for somebody, but it wouldn't be an astronomical amount of money. More or less that somebody is in charge, and somebody do have control of the systems on board.

Researcher: So, what you consider is more an alignment of all the different requirements we have one idea on what the status of the ship is, cyber security vice, and that you can easily adapt to it if needed.

Interviewee 8: And also testing. If you had one entity responsible for this whole system, you can also do testing and you have somebody to point towards if something fails. If nobody is to have the total responsibility and you start doing testing and something fails and it fails in a kind of a grey area where it could be several stakeholder's fault, then the pointing game will start. And that was also an issue when we started getting more automation and so on board the ship. "Something failed, we don't know why, it is probably you". "No, my system is okay, it is probably you." So, when you don't have anybody having the total responsibility, you always get the finger pointing.

Researcher: Yes, because everybody think that their own system is working correctly. And it may work correctly as a single unit, but as a combined unit you can have… Yes, indeed. If you would

compare a ship to other industries, how would you compare the cybersecurity incidents on a ship and a land-based installation.

Interviewee 8: For a land based company, it would be more maybe getting access to information and so on. Or the disrupt operation of that company. But for a vessel, a vessel is a moving object, and you can keep the vessel as a hostage, and you can also cause the vessel to cause damage to a third-party object. And that's more similar maybe to a car or other moving object. But then you have something that there is no question who has the total responsibility of the system. It is not like you have a sub supplier to Tesla which screws up the system. The whole product is the level from one entity and then it is easy to point towards the responsibility, but a vessel is much more complex than most other systems. For an onshore company, you wouldn't have the same kind of connected infrastructure. You would maybe have your office grid where all your computers are connected, and you would have a secondary grid where all the ventilation and those things are. But if you shut down those things it wouldn't cause any damage. If you screw up the heating and cooling system in an office building it doesn't cause any damage. Power companies could be exposed to similar threats. You could put down a whole grid if you get access, but there's no question who's responsible for the system. But when it come to a vessel, you have more or less a single access point where everybody is connected to. You could have two, but the redundancy in the connection lines is that huge. For an office building you could have huge amount of incoming lines and you could spread out your network and you wouldn't necessarily have all on the same... And it's more manageable, compared to when you put all the systems in the world in one box and you connect them together. And you have crew that have their laptops with them, you have the passengers, and you handle of that, as if you only would have one or two satellite dishes. In some way there will be some interconnection between these systems

Researcher: Indeed. Oaky, I think that's it. Thank you very much for participating. And I if I get you correct, your main idea is, that the responsibility is a major factor. If you put the responsibility at the correct person, they can make it work with cybersecurity, they can make a ship completely secure.

Interviewee 8: You have to put the responsibility on somebody or some company or some entity.

Researcher: And at the moment it's too vague for everybody, there are many grey areas where they will point to each other. It is clear. Thank you very much.

Interviewee 8: That will be your future job, I guess.

Researcher: I hope so. Who knows?

Interviewee 8: But I think it's important, and I think there is room for somebody to take that responsibility and the system integrator could be somebody that would take such responsibility. They already are connected to most of the ship systems, so it would be a good starting point to do.

Researcher: Okay. Thank you very much. I will stop the recording.

Appendix II. Codebook

Appendix II.I Comparison To Other Industries

Comparison to Critical Infrastructures

Description: Comparison of the maritime industry to critical infrastructure.

Inclusion Criteria: the statement compares the maritime industry to critical infrastructures.

Comparison to Different Industries

Description: Comparison of the maritime industry to different industries.

Inclusion Criteria: the statement compares the maritime industry to different industries.

Comparison to Governmental Projects

Description: Comparison of the maritime industry to governmental projects.

Inclusion Criteria: the statement compares the maritime industry to governmental projects.

Differences Shore and Vessel

Description: Differences between on shore and on a ship.

Inclusion Criteria: the statement contains differences between cyber security on shore and cyber security on board a ship.

Financial Industry

Description: Comparison of the maritime industry to the financial industry.

Inclusion Criteria: the statement compares the maritime industry to the financial industry.

Healthcare

Description: Comparison of the maritime industry to healthcare.

Inclusion Criteria: the statement compares the maritime industry to healthcare.

Learning From Other Industries

Description: What can the maritime industry learn from other industries?

Inclusion Criteria: the statement contains lessons that the maritime industry can learn from other industries.

Similarities Shore and Vessel

Description: Similarities between on shore and on a ship.

Inclusion Criteria: the statement contains similarities between cyber security on shore and cyber security on board a ship.

Single Connection Point

Description: There is only a single connection point from the ship to the outside world.

Inclusion Criteria: the statement mentions that ships only have a single connection to the outside world.

SMC

Description: Comparison of the maritime industry with small to medium sized companies (SMC).

Inclusion Criteria: the statemen compares the maritime industry with small to medium sized companies.

Appendix II.II. Governance Measures

Audits

Description: auditing of cyber security measures.

Inclusion Criteria: the statement contains audits as cyber security measures.

Classification Rules

Description: Rules from classification societies.

Inclusion Criteria: the statement contains governance measures from classification societies.

Compliant

Description: Compliancy to rules and regulations.

Inclusion Criteria: the statement mentions compliancy with rules and regulations.

Holistic Approach

Description: approaching cyber security on multiple layers and as an interaction of different measures.

Inclusion Criteria: the statement mentions that cyber security should be dealt with on multiple levels and layers to be effective.

IACS Rules

Description: Rules from IACS.

Inclusion Criteria: The statement mentions rules from IACS.

IEC62443

Description: IEC62443 standards.

Inclusion Criteria: The statement contains the IEC62443 standards.

IMO Rules

Description: IMO rules.

Inclusion Criteria: The statement contains rules from the IMO.

IT Policy

Description: IT policy as governance rules.

Inclusion Criteria: the statement mentions IT policy as governance measures.

NIST Framework

Description: The NIST framework.

Inclusion Criteria: the statement mentions the NIST framework.

Regulation

Description: regulations to achieve cyber security.

Inclusion Criteria: the statement mentions regulations in general as a cyber security measure.

Requirements

Description: requirements to achieve cyber security.

Inclusion Criteria: the statement mentions requirements in general as a cyber security measure.

Risk Assessment

Description: risk assessment to achieve cyber security.

Inclusion Criteria: the statement mentions risk assessment to achieve cyber security.

Risk Management

Description: risk management to achieve cyber security.

Inclusion Criteria: the statement mentions risk management to achieve cyber security.

Appendix II.III. Harm

CIA

Description: Confidentiality, Integrity and Availability

Inclusion Criteria: the stamen mentions breach of the CIA triad as harm.

Data Leak

Description: leak of data to undesired parties.

Inclusion Criteria: the statement mentions data leaks.

External Threat

Description: threat from an external party.

Inclusion Criteria: the statement contains a threat from an external party.

Grounding or Collision of a Vessel

Description: grounding of a vessel or collision of a vessel with an object.

Inclusion Criteria: the statement contains grounding of a vessel or collision of a vessel with an object.

Indirect Effect

Description: an indirect effect of a cyber security incident.

Inclusion Criteria: the statement contains an indirect effect as harm.

Intentional Informational Harm

Description: harm to informational systems that is intentionally inflicted.

Inclusion Criteria: the statement contains intentional informational harm.

Intentional System Harm

Description: harm to physical systems that is intentionally inflicted.

Inclusion Criteria: the statement contains intentional system harm.

Power

Description: harm to power generation or distribution systems.

Inclusion Criteria: the statement contains harm to power generation or distribution systems of a ship.

Propulsion

Description: harm to propulsion systems.

Inclusion Criteria: the statement contains harm to the propulsion system of the ship.

Responsibility

Description: taking responsibility.

Inclusion Criteria: the statement mentions responsibility as harm.

Unavailable Systems

Description: unavailability of systems in general.

Inclusion Criteria: the statement mentions the harm of unavailability of systems in general.

Unintentional Informational Harm

Description: harm to informational systems that is unintentionally inflicted.

Inclusion Criteria: the statement contains unintentional informational harm.

Unintentional System Harm

Description: harm to physical systems that is unintentionally inflicted.

Inclusion Criteria: the statement contains unintentional physical harm.

Appendix II.IV. Maritime Cyber Security Characteristics

Air-Gap

Description: the physical separation between IT systems and OT systems.

Inclusion Criteria: the statement contains the air-gap between IT and OT systems.

Analogy with Ship Automation

Description: analogy of cyber security on ships with ship automation.

Inclusion Criteria: the statement contains an analogy of automation systems on ships with cyber security on board ships.

Different Infrastructure

Description: the maritime industry has a different infrastructure compared to other industries.

Inclusion Criteria: the statement mentions that the maritime industry has a different infrastructure compared to other industries.

Diverse

Description: diversity of characteristics.

Inclusion Criteria: the statement mentions that the maritime industry is diverse.

Evolution Example

Description: evolution of the maritime industry.

Inclusion Criteria: the statement describes the evolution in the maritime industry.

Fast Evolving

Description: quick developments.

Inclusion Criteria: the statement describes the maritime industry as fast evolving.

Front Runners

Description: group or organisation which

Inclusion Criteria: the statement describes front runners.

Industrial Network

Description: industrial networks within the maritime industry.

Inclusion Criteria: the statement mentions industrial networks.

Integration

Description: integration of different systems.

Inclusion Criteria: the statement contains a reference to integration of different systems.

Interaction of Multiple Stakeholders

Description: multiple stakeholders collaborating.

Inclusion Criteria: the statement mentions multiple stake holders.

Less Manning

Description: reduction of crew.

Inclusion Criteria: the statement mentions the reduction of crew.

Level 1 Maturity

Description: the lowest maturity level.

Inclusion Criteria: the statement mentions the lowest level of maturity.

Low Maturity

Description: a low maturity level.

Inclusion Criteria: the statement mentions a low maturity level.

Passive Attitude

Description: passive attitude regarding cyber security.

Inclusion Criteria: the statement contains a passive attitude regarding cyber security.

User Acceptance

Description: acceptance of cyber security by users.

Inclusion Criteria: the statement contains user acceptance.

Appendix II.V. Socio-Technical Measures

Access Policy

Description: access policy as measure.

Inclusion Criteria: the statement mentions access policy of users as a measure.

Cyber Security Framework

Description: an organisational framework for cyber security measures.

Inclusion Criteria: the statement contains a cyber security framework

Holistic Approach

Description: approaching cyber security on multiple layers and as an interaction of different measures.

Inclusion Criteria: the statement mentions that cyber security should be dealt with on multiple levels and layers to be effective.

Incident Reporting

Description: reporting of cyber security incidents.

Inclusion Criteria: the statement contains reporting of cyber security incidents as a measure.

IT Policy

Description: IT policy to reduce cyber security incidents.

Inclusion Criteria: the statement contains IT policies as a measure.

MSSP

Description: Managed Security Service Provider.

Inclusion Criteria: the statement contains managed security service providers as a measure.

Password Protection

Description: passwords for protection of vulnerable systems.

Inclusion Criteria: the statement contains password protection as a measure.

Response

Description: response to cyber incidents.

Inclusion Criteria: statement contains response to cyber incidents.

Risk Assessment

Description: assessing cyber security risks.

Inclusion Criteria: the statement contains cyber risk assessments.

Risk Management

Description: managing cyber security risks.

Inclusion Criteria: the statement contains risk management.

Security By Design

Description: incorporating equipment that is secure by design.

Inclusion Criteria: the statement contains secure by design.

Security Managed

Description: manage cyber security by combining different security measures.

Inclusion Criteria: the statement contains security managed as measurement.

SOC

Description: security operations centre.

Inclusion Criteria: the statement mentions the use of a SOC as cyber security measure.

Software Installation Policy

Description: policy for the installation of new software on workstations.

Inclusion Criteria: the statement contains software installation policies as cyber security measure.

Update Policy

Description: policy for updating software.

Inclusion Criteria: the statement contains a update policy as cyber security measure.

Updated Operating System

Description: operating systems with the latest updates.

Inclusion Criteria: the statement contains updated operating systems as cyber security measure.

User Friendly

Description: having cyber security measures which are easy to use.

Inclusion Criteria: the statement contains user friendliness as cyber security measure.

User Management

Description: managing user access to different systems.

Inclusion Criteria: the statement contains user management as cyber security measure.

Appendix II.VI. Technical Measures

Bastion Host

Description: a hardened / isolated host.

Inclusion Criteria: the statement contains a bastion host as cyber security measure.

Content Validation

Description: validation whether content is unaltered.

Inclusion Criteria: the statement contains content validation as cyber security measure.

Continuous Development

Description: continuously improving.

Inclusion Criteria: the statement contains continuous development as a cyber security measure.

Discovery

Description: discovery of cyber incidents (malware or network intrusion).

Inclusion Criteria: the statement contains discovery of cyber incidents as cyber security measure.

DMZ

Description: demilitarised zones in networks.

Inclusion Criteria: the statement contains DMZs as measure.

End Point Security

Description: end point security software.

Inclusion Criteria: the statement contains end point security as a cyber security measure.

Equipment Approval

Description: approval of equipment by a notified body.

Inclusion Criteria: the statement contains equipment approval as cyber security measure.

Hardening

Description: making equipment suitable for certain environments.

Inclusion Criteria: the statement contains hardening as cyber security measure

Holistic Approach

Description: approaching cyber security on multiple layers and as an interaction of different measures.

Inclusion Criteria: the statement mentions that cyber security should be dealt with on multiple levels and layers to be effective.

Locked Screen

Description: locking the screen after so credentials have to be entered for access.

Inclusion Criteria: the statement contains locked screen as a measure.

MAC address authentication

Description: authentication of the MAC address of equipment accessing the network.

Inclusion Criteria: the statement contains MAC address authentication as measure.

Maintainability

Description: maintainability of systems.

Inclusion Criteria: the statement mentions maintainability as cyber security measure.

Malware Detection

Description: detection of malware.

Inclusion Criteria: the statement contains malware detection as cyber security measure

Network Monitoring

Description: monitoring of the network for cyber incidents.

Inclusion Criteria: the statement contains network monitoring as cyber security measure

Network Segmentation

Description: division of the network for different use.

Inclusion Criteria: the statement contains network segmentation as cyber security measure.

Proper Network Configuration

Description: proper configuration of the network.

Inclusion Criteria: the statement contains proper network configuration as a measure.

Situational Awareness

Description: awareness of the cyber security situation in the network.

Inclusion Criteria: the statement contains situational awareness as a cyber security measure.

Source Authentication

Description: authentication of the source.

Inclusion Criteria: the statement contains source authentication as a measure.

Testing

Description: testing of systems.

Inclusion Criteria: the statement contains testing as cyber security measure.

Threat Detection

Description: detection of cyber threats.

Inclusion Criteria: the statement mentions the detection of cyber threats as a cyber security measure.

Traffic Segmentation

Description: differentiation of traffic.

Inclusion Criteria: the statement contains traffic segmentation as cyber security measure.

VPN

Description: VPN connections.

Inclusion Criteria: the statement mentions VPN connections as a cyber security measure.

Appendix II.VII. Threat Actors

By-Pass Attack

Description: A user who deliberately bypasses security to achieve their goal.

Inclusion Criteria: The statement mentions a threat actor who uses by-pass attacks.

Internal Threat

Description: An insider in the organisation who poses a threat.

Inclusion Criteria: the statement mentions an insider threat.

Non-State Actors

Description: external actors who are not affiliated with a state.

Inclusion Criteria: the statement mentions non-state actors.

Organised Crime

Description: organised criminals who are a threat.

Inclusion Criteria: the statement mentions actors from organised crime.

State Actors

Description: actors which perform their actions for a state.

Inclusion Criteria: the statement mentions state actors.

Appendix II.VIII. Threat

Blocked URL

Description: blocking of certain URLs.

Inclusion Criteria: the statement contains blocked URLS.

Breach

Description: cyber security breach.

Inclusion Criteria: the statement mentions cyber security beaches.

DDoS

Description: DDoS attack.

Inclusion Criteria: the statement contains DDoS attacks as a threat.

External Threat

Description: threat originating from an external party.

Inclusion Criteria: the statement contains external threats.

Firewall Scan

Description: scanning of the firewall for open ports.

Inclusion Criteria: the statement contains firewall scanning.

Infected USB

Description: USBs containing malware.

Inclusion Criteria: the statement mentions infected USBs with malware.

Interference

Description: interference of signals or messages.

Inclusion Criteria: the statement mentions interference of signals.

Internal Threat

Description: threat originating from within the organisation.

Inclusion Criteria: the statement contains an internal threat.

Jamming

Description: blocking certain signals.

Inclusion Criteria: the statement contains jamming.

Lateral Movement

Description: lateral movement while executing an attack.

Inclusion Criteria: the statement mentions lateral movement.

Low Threat Level

Description: the threat level is low.

Inclusion Criteria: the statement mentions a low threat level.

Malware

Description: malware in cyber incidents.

Inclusion Criteria: the statement mentions malware.

Man In the Middle Attack

Description: MITM attack

Inclusion Criteria: the statement contains a MITM attack.

Network Scanning

Description: scanning the network for possible vulnerabilities.

Inclusion Criteria: the statement contains network scanning.

Spoofing

Description: spoofing of signals.

Inclusion Criteria: the statement contains spoofing.

Spyware

Description: software used to access secure data.

Inclusion Criteria: the statement mentions spyware.

Unauthorised Access

Description: unauthorised access to systems.

Inclusion Criteria: the statement contains unauthorised access to systems.

Virus

Description: a computer virus.

Inclusion Criteria: the statement mentions a computer virus.

Appendix II.IX. Trends

Autonomous Shipping

Description: sailing without any crew on board a vessel.

Inclusion Criteria: the statement contains autonomous shipping.

Data Trending

Description: collection and trending of data related to OT systems.

Inclusion Criteria: the statement contains data trending.

Digital Twin

Description: a virtual copy used for simulation purposes.

Inclusion Criteria: the statement contains digital twin.

Less Manning

Description: reduction of crew on board a vessel.

Inclusion Criteria: the statement contains less manning on board of vessels.

Remote Sailing

Description: sailing a ship from a remote location.

Inclusion Criteria: the statement contains remote sailing as a trend.

Appendix II.X. Vulnerabilities

AIS

Description: Automatic Identification System

Inclusion Criteria: the statement contains the AIS as vulnerability.

Awareness

Description: Awareness of cyber security risks.

Inclusion Criteria: the statement mentions awareness as cyber security risk.

Bi-Directional Communication

Description: communication in both ways.

Inclusion Criteria: the statement contains bi-directional communication.

Budget

Description: the budget to take cyber security measures.

Inclusion Criteria: the statement mentions budget as a vulnerability.

Design Limitations

Description: limitations during the design.

Inclusion Criteria: the statement mentions design limitations as cyber security risk

ECDIS

Description: the ECDIS.

Inclusion Criteria: the statement mentions the ECDIS as vulnerability.

Engine Room Systems

Description: systems mainly located in the engine room.

Inclusion Criteria: the statement mentions engine rooms systems as a vulnerability.

GNSS

Description: satellite positional systems.

Inclusion Criteria: the statement mentions GNSS such as GPS as a vulnerability

High Speed Satellite Connections

Description: high speed connection from the ship to the internet using satellite.

Inclusion Criteria: the statement mentions high speed satellite connections as a vulnerability.

Legacy Systems

Description: older operating systems and systems.

Inclusion Criteria: the statemen contains legacy systems a vulnerability

NAVCOM

Description: navigation and communication systems.

Inclusion Criteria: the statement mentions the NAVCOM systems as a vulnerability.

Office Network

Description: network on the ship running office like applications such as email and word processors.

Inclusion Criteria: the statement mentions the office network as vulnerability.

Outdated Operating System

Description: operating system which is not up-to-date.

Inclusion Criteria: the statement contains outdated / not updated operating systems

Passive Use of Cyber Tools

Description: passively using cyber security tools.

Inclusion Criteria: the statement mentions the use of cyber security tools in a passive manner.

Point of Entry

Description: point of entry for a cyber attack.

Inclusion Criteria: the statement contains a point of entry which can be used as vulnerability.

Radar

Description: the radar system.

Inclusion Criteria: the statement mentions the radar system as a vulnerability.

Rapid Development in Automated Systems

Description: development of the IT systems influencing OT systems and automation on board.

Inclusion Criteria: the statement contains the rapid development in automation systems.

Remote Access

Description: accessing devices from a remote location.

Inclusion Criteria: the statement contains remote access.

Saving Costs

Description: reduction of budgets in order to save costs.

Inclusion Criteria: the statement contains saving costs as vulnerability.

SCADA / AMCS

Description: SCADA systems.

Inclusion Criteria: the statement contains the SCADA or AMCS as vulnerability.

Serial Communication Over IP

Description: communication of a serial protocol over an Ethernet/IP network.

Inclusion Criteria: the statement contains serial communication over an ethernet connection.

Skills

Description: cyber security skills of personnel of the organisation.

Inclusion Criteria: the statement mentions the (lack of) cyber security skills as a vulnerability.

Software Update

Description: update of software.

Inclusion Criteria: the statement mentions software updates as a vulnerability.

Supply Chain Attack

Description: Cyber-attack on an organisation in the supply chain.

Inclusion Criteria: the statement contains a supply chain attack.

Unknown Connections

Description: connections to the network which are unknown.

Inclusion Criteria: the statement mentions unknown connections as a vulnerability.

Welfare Network

Description: an IT network specifically used for internet access for streaming and social media.

Inclusion Criteria: the statement mentions a welfare network as vulnerability.