TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technology
Department of Software Science

Karl Lubja 178780IVCM

SYSTEMATIC GENERATION OF CYBER ATTACK SCENARIOS AGAINST A SHIP

Masters Thesis

Hayretdin Bahşi, PhD

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia Teaduskond
Tarkvarateaduse Instituut

Karl Lubja 178780IVCM

LAEVA KÜBERRÜNNAKU STSENAARIUMITE SÜSTEMAATILINE GENEREERIMINE

Magistritöö

Hayretdin Bahşi, PhD

Tallinn 2020

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Karl Lubja

Date: May 19, 2020

Annotatsioon

Laevandus on maailmamajanduse alustala, olles otseselt või kaudselt seotud 90% maailmamajandusega [1]. IT-lahenduste kastusele võttu tempo on sellegi poolest olnud aeglasem võrreldes teiste sektoritega. Isegi kui IT-lahenduste rakendamine laevas loob uusi võimalusi nii meeskonna kui omanikfirma jaoks, suurendab see ka potentsiaalseid võimalusi ründajatele. Samuti on ka küberkaitse merenduses võrdlemisi vähe uuritud arvestades merenduse tähtsust, samas on uustulijatele antud uurimisväljas üsna suur lävi. Antud lõputöö eesmärk on lihtsustada merenduse küberkaitse uustulijate lävendit kogudes kokku olemasoleva kirjanduse ning esitades potentsiaalsed süstemaatiliselt genereeritud küberrünnaku stsenaariumid, mille sihtmärgiks on laev ja selle operatsiooniline tehnoloogia. Loodud stsenaariumid põhinevad süstemaatilise kirjanduse ülevaatel ning intervjuudel merenduses töötavate ekspertidega. Kokku tuvastati 3 põhilist rünnakut ja eesmärki laevade vastu, mis omakorda jagunevad 17 erinevaks kõrgetasemeliseks stsenaariumiks. Eksperte intervjueeriti 13 korral 10 erineva inimesega. Olgugi, et kirjanduses eksisteerib sarnaseid töid, mis peamiselt koosnevad erinevate ajalooliste õnnetuste ja näidete kirjeldamisest, pole ükski neist kasutanud süstemaatilist metoodikat või metoodika kirjeldus on olnud pealiskaudne. Lisaks, pole keegi varasemalt kasutanud eksperte merendusest, et valideerida loodud stsenaariumite võimalikkust.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 51 leheküljel, 9 peatükki, 10 joonist, 3 tabelit.

Abstract

Humankind has been a seafaring species for thousands of years and has passed the test of time. Ships are the bedrock of the global economy as shipping facilitates around 90% of the global economy [1]. The field of maritime has lagged behind in adoption of IT-related services compared to other sectors. Yet as these advancements provide additional opportunities for the field, they are a fruitful soil for attackers alike. Moreover, cyber security in maritime remains relatively under researched compared to its importance and there is a significant glass ceiling for anybody interested in the field. This thesis aims to lessen the gap and entry difficulty by gathering existing literature into one paper and proposing possible systematically generated attack scenarios presented with the use of attack trees against a ship, specifically against a ship's operational technology. The scenarios are based on a multivocal systematic literature review done during this thesis and validated using expert interviews. In total, 3 major attack goals with a total of 17 high-level scenarios were identified and validated by 13 interviews of 10 people. Similar, mainly smaller, works exists where the author proposes some scenarios or gathers past cyber related incidents related to shipping but none of them have used a systematic methodology or the proposed scenarios are rather shallow and the validity of proposed scenarios has never been proposed to industry experts.

The thesis is in English and contains 51 pages of text, 9 chapters, 10 figures, 3 tables.

List of abbreviations and terms

Abbreviation	Definition
MTS	Maritime Transportation System
CPS	Cyber-Phyiscal System(s)
OT	Operational Technology
ECDIS	Electronic Chart Display and Information System
GT	Gross Tonnage, a unit used to measure sizes of ships
AIS	Automatic Identification System (ship's equivalent to a plane's transponder)
BIMCO	Baltic and International Maritime Council
PMS	Power Management System
VDR	Voyage Data Recorder
TPU	Tensor Processing Unit
ATS	Anti-Fire System
IAS	Integrated Automation System

Table of Contents

List of Figures

List of Tables

1. Introduction

Much of the global goods moved around the world are done so by using the Maritime Transportation System (MTS) thus playing a vital role in the global economy, MTS is responsible for around 90% of global trade according to the estimates of the United Nations [1]. MTS is an umbrella term that consists of ships, ports, operating companies and everything else that is necessary for transporting goods or passengers via waterways. Even a small incident can cause damages that reach extraordinary sums but also the social value of the maritime sector can be impacted as well. For example, the Maersk cyber attack in 2017 created damages up to $300 million [2] or a disabled rescue ship may mean that help does not arrive in time and in turn additional injuries and/or deaths may occur. In addition, in some places ships are the only connection with the rest of the world and any stoppages can impact the morale.

Nature of the maritime sector itself dictates that technological changes and advancements take longer to be adopted due to the long lifespan of ships and time necessary to build ships, especially large-scale ones. These advancements, namely IT related, come at their own costs – new attack vectors that enable malicious actors to disrupt the normal functioning of the MTS. Similarly to technological advancements, cyber security in the MTS is also lagging behind compared to other sectors where the life cycle is shorter, generally 25-30 years for ships [3]. While the Maersk attack was more IT related, this thesis mainly focuses on Operational Technology parts of a ship i.e. systems that are used to control the physical state of the ship. Lately, the International Maritime Organization and related European agencies have started to focus on the problem in recent years, it is still under researched and has a long way to go especially on vessels. In addition, the International Maritime Organization adopted a resolution in 2017 that cyber risks should be addressed in safety management systems by 2021 the latest [4]. As such there is interest from the maritime industry to focus on the subject and due to that Port of Tallinn will provide assistance during the thesis, mainly in the form of information.

1.1 Research Question

The research questions answered in this thesis are:

- What are possible attack scenarios against a ship?
- What is current state of knowledge in academic literature about cyber attacks against a ship?

Identifying possible attack scenarios is achieved with the use of a Multivocal Systematic Literature Review and through conducting interviews with industry experts. Multivocal Systematic Literature Review is also used to identify the current state of cyber attack related information against ships.

1.2 Scope

The objective of this thesis is to be as general as possible in terms of the types of manned ships this thesis applies to. This means that no specific ship type, whether it be a cargo, cruise, fishing or any other ship type, is specifically focused on. However, the ships in question should be fitted with IT-enabled systems such as ECDIS, AIS etc. Also, it should be taken into account that the information gathered, especially from expert interviews, comes from people related to commercial ships and the attacks designed are meant for larger types of ship, specifically cargo or passenger ships. The limitation primarily comes from the set of experts interviewed during this thesis as most interviewees are related to companies operating cargo or passenger ships. This does not mean that the techniques can not be applied to smaller or other types of ships but it is still important to consider. Moreover, commercial ships have better physical security not to mention that the crew consists of professionals. Although the final attack scenarios in some way or another rely on human error, the scenarios that the proposed goals are achieved intentionally not by mistake.

Another big part of the scope is that the thesis primarily focuses on operational technology meaning that the information gathered and attacks created are related to the operation of a ship and specifically the inner air-gapped part of a ship i.e. offshore systems that are on a ship. In addition, this thesis does not come up with a complete risk assessment as the created attacks and scenarios are not assigned probability values.

1.3 Novelty

Firstly, there are existing papers that gather historical data about different ship system vulnerabilities but none of them provide a systematic approach and the methodology seems to be vague. The usage of Multivocal Systematic Literature Review in this thesis should provide reproducible results. Secondly, to the knowledge of author, no papers exist that

use expert interviews to gather ideas and feedback for possible attacks. Thirdly, existing literature about attacks use historical incidents and vulnerabilities but no one has used experts to validate them against the real world. Fourthly, this thesis also deals with both operational and technological aspects of cyber attacks towards a ship.

1.4 Content

The thesis contains of 7 content chapters: Related Literature, Ship - a system of systems, Systematic Literature Review, Expert Interviews, Attacks, Discussion. Chapter Related Literature will cover existing work using similar methodology in academic literature related to cyber-physical systems like use of systematic literature review or different methodologies to represent scenarios. The next chapter, Ship - a system of systems, describes different components that constitute as a ship and give necessary background knowledge to the reader about operational technology. Systematic Literature Review chapter describes the process and defines the protocol of conducting the SLR and results. Sixth chapter of the thesis, Expert Interviews, contains descriptions and content of the two phases of interviews conducted in this thesis and provides additional background knowledge about operational and procedural side of MTS. Primary contribution of the thesis is presented in the chapter Attacks where data gathered from the SLR and interviews is combined to present the synthesized attack scenarios with descriptions to the reader. Finally, the Discussion chapter provides additional thoughts about the attacks, limitations of the thesis and some insight into possible future work.

2. Related Literature

The scope of this research is cyber attacks against a ship, specifically against operational technology and off-shore systems. One of the primary methodologies for gathering data is the usage of Systematic Literature Review, specifically Multivocal. Although a SLR had not been conducted in the field of maritime cyber attacks related to it, similar works do exist. In 2019 Awan and Ghamdi [5] collected and reviewed 59 historical incidents from literature related operational technology in the ship, specifically in the integrated bridge system. Data gathered by them originates from various white and grey sources but exact methodology regarding search query, inclusion and exclusion criteria is missing or vague. Another similar work from 2019 is a master thesis from Denmark that dealt with analyzing attack surfaces of a ship [6] using literature as one of the primary sources of information. Similarly to this thesis it was done at least in some part in cooperation with ship operating companies and experts. The author did go into detail with specific systems and was able to conduct an asset based risk-assessment. Tam and Jones also did a cyber risk assessment of an autonomous ship [7] using their created MaCRA framework [8].

Aside works about historical incidents and similar existing literature based works, there really is not anything similar to this thesis in the field of maritime cyber security, most deal with a specific component of a ship, mostly navigation network related like ECDIS [9, 10, 11, 12, 13, 14] or AIS [15, 16] to name a few.

3. Method

The primary idea of the thesis was to gather initial background knowledge and possible attacks using Multivocal Systematic Literature Review and expert interviews, then synthesize and create possible attack scenarios in the form of attack trees using data gathered and finally present the created scenarios to experts in order to gather their ideas and feedback on the feasibility and possibility of the attacks.

Multivocal Systematic Literature Review offers a concise and condense method for passing relevant information about possible attacks and past real world incidents. In addition, SLR as a method is reproducible. In order to conduct a SLR, the author defined concrete methodology that can be found in Chapter 5. The methodology consisted of defining the purpose, search process, inclusion/exclusion criteria, data extracted. As a part of the SLR, the gathered data was additionally classified with MITRE's ATT&CK®for Industrial Control systems[1] which is intended to be used for description of adversary actions in an ICS network [17].

The interviews were conducted in 2 phases: unstructured for background knowledge, especially operational side of shipping, and structured for gathering ideas and feedback about the created attacks. First phase was extremely important due to the author's complete lack of prior knowledge about shipping in general. Moreover, the unstructured interviews helped with analyzing and making sense of the literature read during SLR in addition to aiding the author understand aspects from the operational and OT side of a ship. After the attacks were created in Chapter 7, a second round of interviews were conducted with similar approach to the first round. It was important to gain feedback from operational and OT point of views but the second round applied more focus on the operational side as to learn defensive techniques and procedures in the case of an attack in addition to feedback what they think is possible. The interviews also provided to be a valuable source of information about data flow in a ship's OT network as this information is something that is largely missing from existing literature. More information can be found in Chapter 6.

The motivation to use attack trees for presenting attacks comes from their ease of use and possibility of presenting a range of scenarios in a compact form. Furthermore, the

[1] https://collaborate.mitre.org/attackics/index.php/Main_Page

usage of attack trees has become extremely widespread and the methodology is constantly developed making it possible to use the created attacks as an input for other work. Attack graphs were a possible alternative but Lallie, Debattista and Jal [18] found that attack graphs were less standardized.

4. Ship - a system of systems

A ship in itself can be considered as an organism - a set of systems that cooperate in the pursuit of a common goal. This chapter will explore the different systems that together constitute as a ship and will present dependencies between different systems - informational and network.

A ship is not truly a ship if it does not possess the capability of autonomous operation (not to confuse with self-operating vehicles). Ships must be able to operate for prolonged periods of time without any outside help. With the help of rapid technological improvement, vessels have begun to operate much more efficiently in terms of manpower and overall economics by automating tasks necessary for successful ship operation, for example navigation enhancements in the form of ECDIS have greatly simplified the task of navigation. This chapter will introduce and explain different systems and technologies that are required for operating a modern ship. In addition, the definition a ship presented is largely based on commercial ships and takes into account recommended best practices.

As far as this thesis is concerned, only offshore i.e. systems that are on a ship are considered. Also, all of the information gathered here is sourced from the Multivocal Systematic Literature Review and expert interviews.

4.1 Navigation network

The key problem when operating a ship is to exactly know where the ship is located at present. During the interviews that the author conducted in the making of this thesis, interviewees from Port of Tallinn, used the term navigation network that encompasses everything related to navigation of the ship. This section will highlight and discuss different systems and aspects of the navigation network that enable normal operation in terms of navigation.

4.1.1 ECDIS

The biggest tool in the crew of a modern ship's arsenal of tackling the navigational problem is **E**lectronic **C**hart **D**isplay and **I**nformation **S**ystem. ECDIS is a computerized

replacement that consists of electronic charts and different sensors for paper and manual based navigational means. In 2009, the International Maritime Organization introduced a regulation for all newly built passenger ships greater or equal than 500 GT and cargo ships greater or equal than 3000 GT to be fitted with ECDIS, the exact adoption date depended on the type and size of ship [19]. Ships also must include redundancies for different systems and ECDIS is no exception - ships usually are fitted with a backup ECDIS(s).

ECDIS takes data as input from several different systems in the navigation network, merges the data and displays the data to the bridge in a meaningful way. A typical ECDIS setup will use data from AIS [20], GPS [20], radar [20], gyroscope [14], echo sounder [14], weather station 6.5, NAVTEX 6.5. A typical standalone setup of ECDIS can be seen in Figure 1.

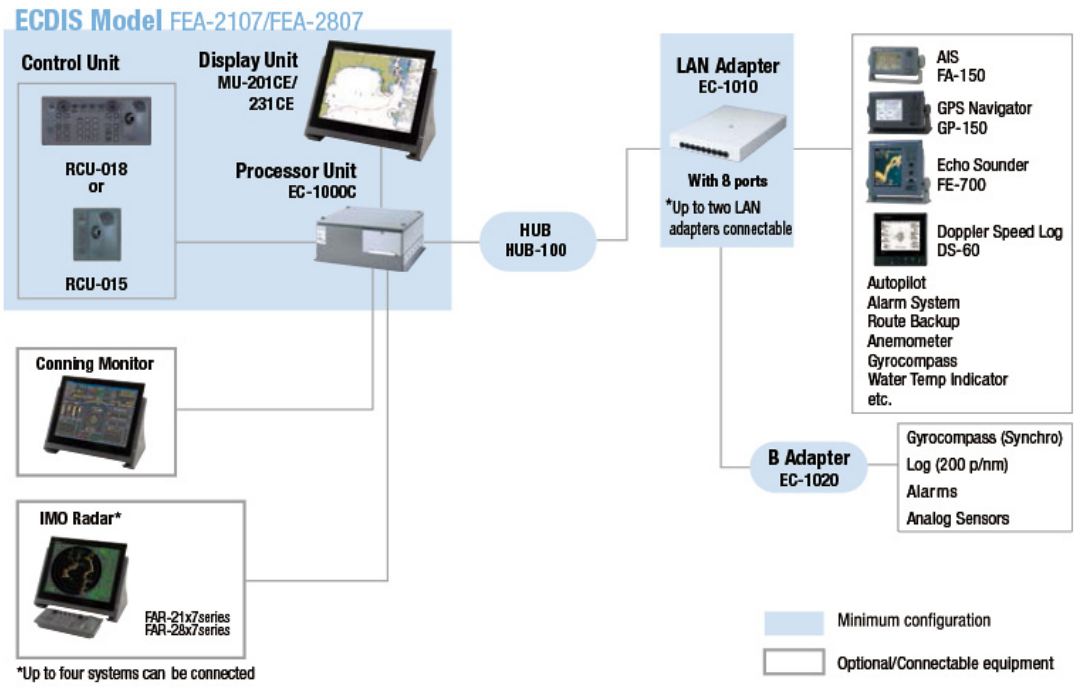

Figure 1. *Standalone ECDIS setup [21].*

ECDIS is also dependent of electronic charts (as the abbreviation suggests) which in Estonia are made by the Estonian Maritime Authority. The charts are bought by a third party provider and then the same third party provider offers a service to ship operating companies to keep the charts updated. While some ECDIS vendors provide means of updating the charts, the prevailing method is using USB memory sticks [12]. Per the interviews and SLR, the third party provider only provides the charts and the ship operator itself handles updating the charts. Typically there should be a dedicated USB memory stick that is just used for updating ECDIS charts and is only accessible to the crew i.e. no

random USB stick is used. Periodicity of chart updates is hard to pinpoint but they tend to be fairly regular, for example charts are updated every week in the case of the Ferry Tiiu as learned in the visit to Tiiu, please see Section 6.2.

4.1.2 AIS

AIS, short for Automatic Identification System, is similar to a plane's transponder. It is responsible for exchanging information about a ship's name, flag, ship type, payload type, current position, course, speed and destination. The data is transmitted between ships using radio equipment with the approximate range of 25 miles (ca 40km). Additionally it is possible to transmit aids-to-navigation such as shipwrecks, shorelines or buoys that may impact the safety of a ship. Bulk of the information transmitted is static and configured in AIS of a ship (easy to input malicious data by the crew or actor) but course, speed and position are retrieved from GPS of the ship. Static information of AIS includes but is not limited to ship name, ship flag, payload type. There are also two types of AIS systems: integrated and standalone. Integrated AIS systems are built-in to the ECDIS of the ship and receive the same GPS data as ECDIS but standalone AIS setups come with its own GPS sensor.

4.1.3 Weather data

The navigational network receives weather information from two sources: ship's onboard weather station and NAVTEX. NAVTEX is used to receive navigational and weather forecast data on a ship via radio equipment. The data transmitted can range from storm warnings to warnings of military exercises in the surrounding area.

4.1.4 GPS

GPS on a ship works more or less the same way as a GPS in a smartphone but there are additional measures that improve the accuracy of the GPS data. Along the shore there can be DGPS stations that are used for GPS satellite location data calibration. The stations are maintained by maritime authorities of the station location. Very accurate coordinate and time data is available from the DGPS stations which is used by ships to mitigate certain inaccuracies that may come from the GPS satellites.

4.2 Rest of the ship

Alongside the navigation network, everything else on a ship is rather separate and there is no higher encompassing group. This section will detail the rest of a ship.

4.2.1 Power Management System

The PMS is responsible for two things: electricity generation and management in a ship; and providing required power for the thrusters. In some ships, like Port of Tallinn's Tiiu, the two things are one as the thrusters on Tiiu are powered by electricity. All in all, the system monitors electricity consumption and generation and makes adjustments to the generators accordingly.

4.2.2 Steering and propulsion

Thrusters of a ship steer and move the ship in the required direction. Input for the thrusters is received from the wheel of the ship that resides in the bridge. Depending on the ship type, there may be several bridges where operation of the thrusters is possible due to redundancy and safety purposes.

The usage of the term thrusters can be a bit conflicting depending on the context. Port of Tallinn employees used the term as the main means of propulsion and steering but during interviews some interviewees were confused by its usage as thrusters can also be used to describe devices on a ship that are used for lateral movement at low speeds. In this thesis under the term thrusters it is meant specifically the main propulsion device of a ship.

4.2.3 IAS

IAS is something that did not come up during the SLR and was brought to the attention of the author by Kristo Klippbeg in the interview conducted in Section 6.5. According to Mr. Klippberg it is responsible for gathering sensor input from systems not related to navigation, for example PMS. It is also responsible for gathering navigation network related alarms from ECDIS and sending them to the VDR in order to reduce the load on the navigation network.

4.2.4 Autopilot

There are three types of autopilots: regular that just maintains speed and course, tracking that is able to follow a preplanned route and speed that is able to follow a preplanned route and change speed during preset points of the route. The autopilot gives commands to the wheel which in turn gives commands to the thrusters. Tracking and speed autopilots receive the route and information related to it from ECDIS and use sensor data from GPS and compass if it is required from the type of autopilot.

4.2.5 VDR

VDR is the central logging point of the ship, in normal situations the data that resides in the VDR is unused but in case of accidents or other incidents it is a valuable source of information for any investigation. In the VDR, commands in the ship, crew communication and other inputs are logged.

4.3 Network topology

In 2018, BIMCO released their cyber security guidelines what can be considered best practices for maritime companies [22]. There they propose that OT network should be segregated from other networks such as office or guest networks, please see Figure 2. However, during this thesis it was not possible validate that this implementation is widely spread due to the research methods but as far as this thesis is concerned the proposed network segregation is used as a baseline in terms of network security for commercial ships. Dan Herring said in his interview, Section 6.3, that situation in terms of network segregation it is pretty woeful all around. However, this aspect depends on the type of ship - cruise ships for example put more emphasis on cyber security and network segregation as they have guests and other personnel on board whereas fishing boats or cargo ships only have the crew onboard and less emphasis is positioned on cyber security. Moreover, the types of ship largely define the resources available in building, operating and maintaining the ship. Large ship companies, whether cruise, cargo or transportation, have massive amounts of resources to ensure proper cyber security on their ships but smaller actors have to prioritize little resources they have.

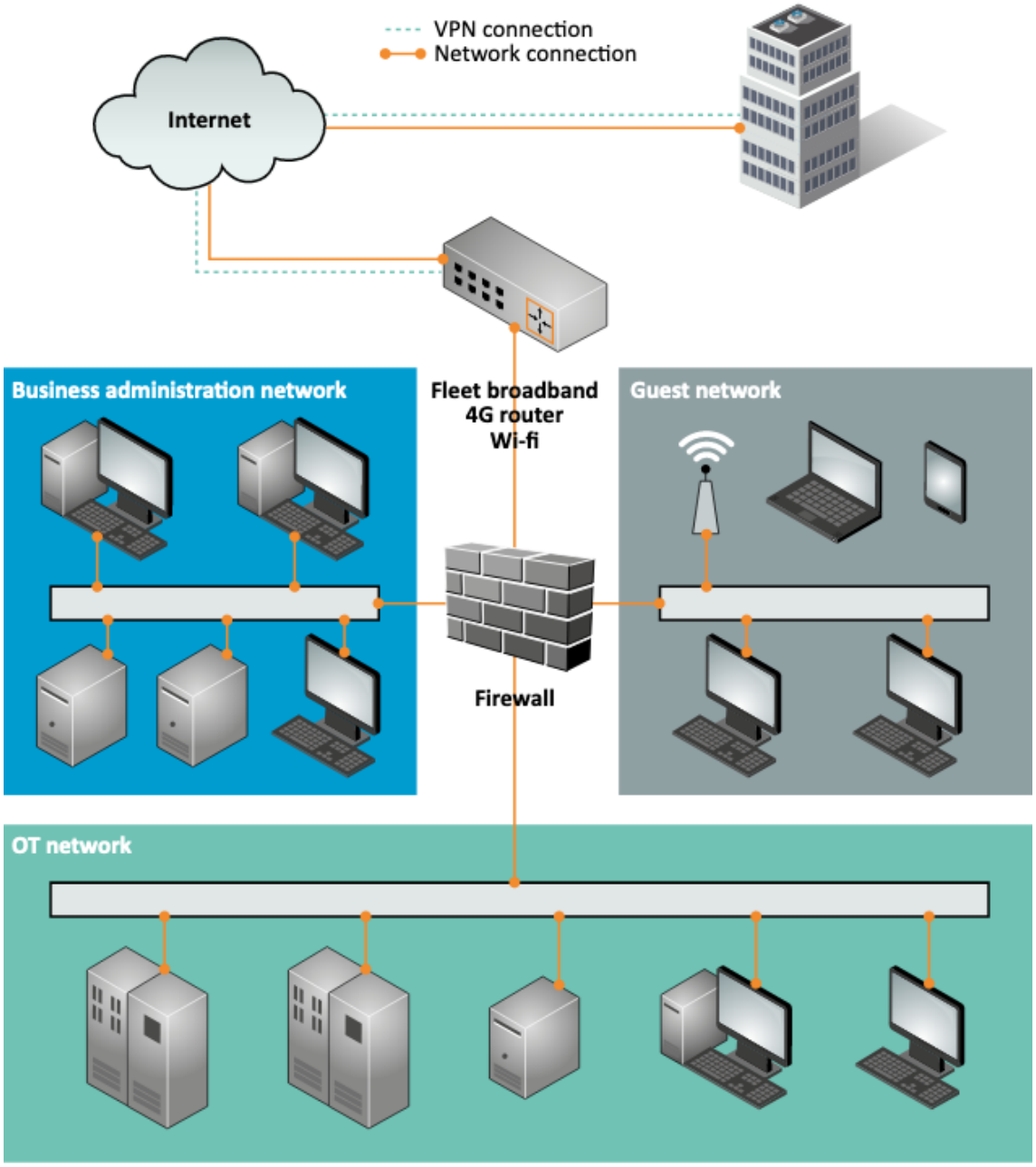

Figure 2. *Best practice ship network [22].*

All in all, the important thing to note is that if access is gained to the ship's internal network, OT network in Figure 2, it should be possible for the attacker to reach any device in the network when there is no further segregation in the ship's OT network. While the best case scenario in terms network security should not enable the attacker to command and control a malicious device connected to the OT network remotely from the internet, there are still options available. For example, during the visit to Ferry Tiiu, please see 6.2.2, the unprotected guest WiFi was accessible from the bridge which means if an attacker connected a malicious WiFi capable device to the bridge, it would be possible for the

attacker to control the device remotely by connecting to the unprotected guest WiFi.

After the interviews with Guldar Kivro and Kristo Klippberg with some additional input from Reimo Suurmets, the author was able to build a network graph of communications of the OT network, please see Figure 3. However, there is no realistic method to validate whether it is industry standard. As the interview contents, see sections 6.4 and 6.5, suggested the network traffic paths are one-way. Commands sent to the cyber-physical systems are sent using one network and the feedback (sensor data) is collected with a completely separate network, mainly IAS. According to the interviews, the networks are logically separated using VLANs and with some mentions of physical separation (separate switches). Moreover, there should be a firewall on the ship itself that handles traffic between the guest, office and inner networks. However, during the interviews the author was unable to completely verify the components of the network segregation. As this is based on Port of Tallinn's example, general conclusions can not be done and further research is required. Another important note is that according to Reimo Suurmets the OT network is configured and installed in the factory and the shipping operator may install additional networks on the ship, such as a CCTV network, but generally the network is as it comes from the factory.

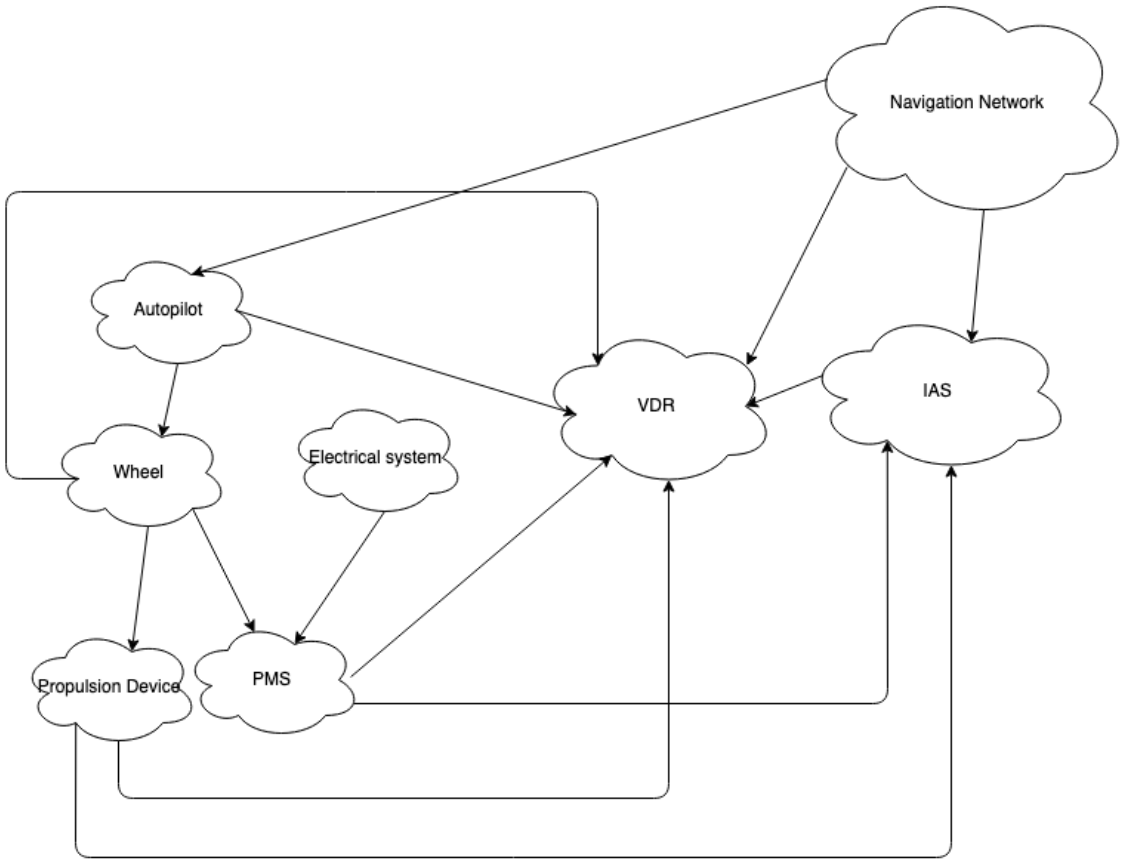

Figure 3. *Information Flow of the OT network based on Interviews in 6.4, 6.5*

5. Systematic Literature Review

In order for the Systematic Literature Review (SLR) to extract reproducible results it is important to conduct the SLR using a strict predefined protocol [23]. One of the main purposes of the SLR is to gather as state-of-the art information as possible, a goal which cannot be achieved without including grey literature [24] as various incident reports/articles might not be discussed or present in scientific literature. Thus this SLR will be a Multivocal Literature Review (MLR) and will be based on the guidelines proposed by Garousi, Felderer and Mäntylä [24]. Although they focus on software engineering (SE), cyber-security and SE belong to the same general domain of computer science making it applicable in this thesis.

5.1 Purpose

Specifically in this context, the main purpose of the multivocal literature review is to provide comprehensive knowledge about known vulnerabilities, inner-workings or other aspects of a ship that might be possible to exploit and can be used as an attack vector. Various proven or theoretical attacks against ships and its subsystems will be considered. Secondary purpose of the SLR will be to give the author supplementary information for designing the interview questions.

5.2 Protocol

5.2.1 Search process

The search process will be conducted automatically via keyword-based search engines for conference proceedings, articles in journals and grey literature. Grey literature might be of lower quality but the amount of academic literature in the field is low and certain incident reports will provide valuable data in terms of practical and feasible attacks. The main search engine to be used is Scopus because Scopus is a index of publications. In addition, “regular” search engines, such as Google, will be used to find reports or articles, grey literature, about specific security incidents that might provide valuable insight.

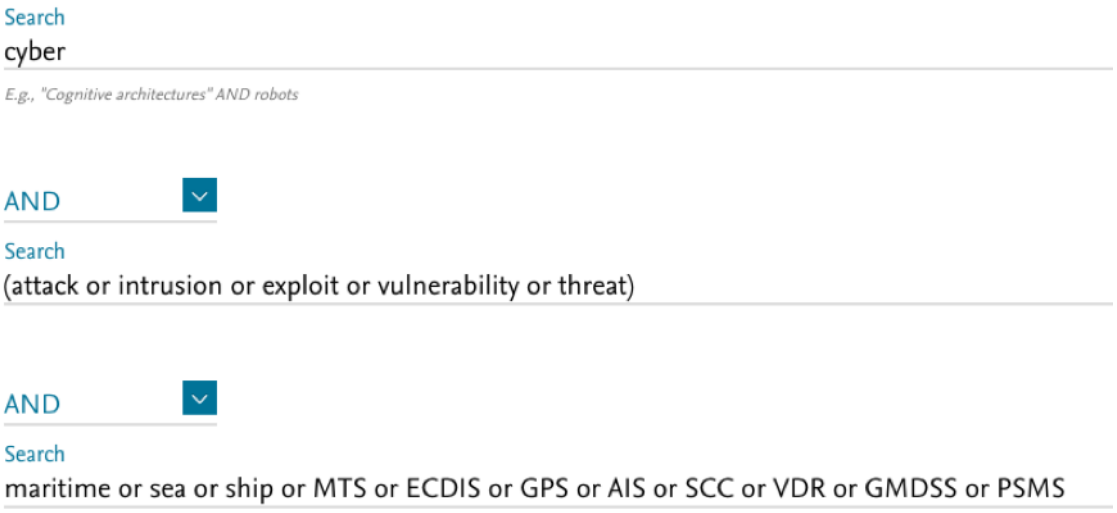

Figure 4. *Search query in https://scopus.com*

5.2.2 Search strings for Scopus

Keywords are divided into three groups (seen below in **Figure 4**):

1. To limit papers that deal with anything cyber - "cyber".
2. To limit results into papers that discuss anything attack related - "attack", "intrusion", "exploit", "vulnerability", "threat".
3. To limit results into papers that deal with the maritime sector or a ship's subsystems – "maritime", "sea", "ship", "MTS", "ECDIS", "GPS", "AIS", "SCC", "VDR", "GMDSS", "PSMS".

5.2.3 Inclusion criteria

If a paper meets any of these qualities, they will be included:

- Papers about vulnerabilities, exploits, attacks, human behaviour and practical examples.

The SLR will not include or exclude papers based on the publishing dates mainly due to the lack of literature.

5.2.4 Exclusion criteria

If a paper meets any of these qualities, the paper will be excluded:

- Papers not related to the maritime transport system.
- Papers not related to offshore systems.
- Papers not related to attacks, vulnerabilities or threats, for example frameworks, legislation etc.
- Papers not accessible using Taltech resources.

5.2.5 Data extraction

The data extracted from each paper will be:

- Type of literature (white/grey/black)
- Producer (academic/corporation /governmental organization)
- Year of publishing
- Area ((**N**) Navigation/(**C**) Communication/(**P**) Propulsion/(**S**) Steering/(**O**) Operational/(**HA**) Human Aspect)
- Information classification ((**V**) Vulnerability/(**E**) Exploit/(**S**) Scenario)
- MITRE ATT&CK tactic for Industrial Control Systems (where applicable)
- Preconditions
- Goal
- Summary

Area data point is decided by to what part of the ship the data extracted applies to, for example AIS spoofing could apply to navigation or AIS denial of service could apply to both navigation and communication. Operational and human aspects are quite similar in most cases but there are minute differences, for example crew overreliance on interface/sensor data would be classified as human aspect and procedural aspects to ECDIS chart updates or maintenance schedules constitute as operational. Steering and propulsion are rather straightforward as they directly relate to data points about physical movement of the ship.

Difference between vulnerability and exploit is that vulnerability is a flaw or aspect of a ship that could be used by the attacker and exploit is the method or way to use a vulnerability, for example usage of VSAT default configuration to send malicious data to a ship would be a exploit and that the ship's VSAT equipment uses default configuration would be a vulnerability. Scenario is basically a combination of multiple vulnerabilities and exploits with additional description what could be the result of the combination, for example using AIS spoofing to create a false positive collision course warning in a ship that might result in the crew taking evasive maneuvers.

Preconditions, goal and summary are rather self-explanatory. In order to use the extracted scenario, vulnerability or exploit, the attacker must fill certain requirements prior to the specific attack, for example the attacker might need some equipment like AIS transmitter or the attacker should have a foothold in the ship. Goal depicts what is achievable by the attack or what is the objective of the attack, for example force autopilot off the pre-planned route. Summary is a short description of different aspects of the attack that includes methodology and steps that should be taken.

Mitre ATT&CK for Industrial Control Systems is useful for additional classification as it may cover aspects that may not be so perceivable from other data points extracted except summary. All of the data points cover different facets of the data extracted and this kind of classification just adds another facet. However, the limiting factor is that it is meant for ICSs and while ships are fitted with them, using the classification may not paint the whole picture.

5.3 Search results

Based on the previously defined protocol and criteria, two searches were conducted separately – one from academic sources and one from grey literature based sources.

5.3.1 Academic sources

Scopus search, conducted on the 18th of January 2020, returned a total of 463 results. Next, irrelevant papers were removed that did not meet the aforementioned criteria by reading the abstracts of papers, which left us 97 results. Finally, the final set of papers was determined by fully reading the content and a total of 28 papers met the criteria out of the total 463 papers from the initial search result.

5.3.2 Grey and black literature

The search for non academic sources via Google Search was a bit more general as grey and black sources might not use the same terminology as research papers. However, the criteria for accepting a source would match with academic sources and is strictly related to incidents/attack towards off-shore systems. Due to the limited scope a simple search query of "cyber attack ship" was used to find appropriate sources.

The data was extracted in a similar format but was filtered by reading the contents of the first 5 pages of the search results. This limitation was decided by conducting experimental

searches and examining duplicates.

5.4 Final results of Systematic Literature Review

The final extracted data and results of the SLR can be found in Appendix A. of SLR result in Appendices is far from ideal but the extracted data in table form is the best and most convenient way of displaying the data. This way the all of the relevant classifications and information is together and easily extractable by any reader. Summary might be the only data point that could be separated from the table but in that case other columns and data points lose context. Results of the SLR will be referenced in the text using the syntax (SLR #), for example the 23rd row of the extracted data would be (SLR 23).

In total 46 data rows were extracted from the literature of which 27 were assigned vulnerability class, 17 were assigned scenario and the remaining 2 were exploits. As to area of the data points, 6 were human aspect related, 22 were navigation related, respectively 2 and 1 were assigned propulsion and steering values and finally 11 were operational related. Some of the data points were assigned multiple area values as they dealt with several different aspects. Almost half of the sources were related to navigation which perfectly makes sense as navigation is the key problem in shipping. However, it might indicate that one facet of shipping or ship's OT is rather heavily researched whereas other aspects are pushed aside. A more likely explanation is that certain systems that are related to navigation are unique to shipping, for example ECDIS and AIS. Everything related to human behaviour, CPS security, network technology or mechanical is more general or covered by other fields of research.

6. Expert Interviews

During this thesis, one of the sources of information are so-called expert interviews. Although a Multivocal Systematic Literature Review was conducted in this thesis, they still may not convey a complete picture of the real world, this is where expert interviews excel as they can provide information about IT, OT and functional aspects. Together academic sources and data from people, who everyday either work on a ship or deal in matters related to the ship, complement each other very nicely giving us an almost complete picture. As this thesis is done in cooperation with Port of Tallinn, most of the experts are provided by them. Mainly due to the time constraints it is not possible to include more experts from different companies and fields of shipping. The aforementioned homogeneity of interviewees is one of the weak points of this thesis. Still the interviews provide great insight into day-to-day operation of a ship and gives an idea on how the real world works.

In total there were 13 interviews of 10 different people that took place from November 2019, when the first interview took place, until May 2020. Of the total of 13 interviews, 3 were technical, 4 were operational and 6 were a mix of technical and operational. This chapter will describe the contents of the interviews and information learned from them, additional information about the interviewees is available from Table 1. Of the total 12 interviews, 5 were unstructured preliminary interviews where the author gathered background information about the inner-workings of a ship, remaining 8 interviews were structured and followed specific questions about the attacks created during this thesis in Chapter 7.

6.1 Taivo Kivimägi, 03.11.2019

On the 3rd of November, 2019 Taivo Kivimägi in a unstructured interview introduced the author the general idea of shipping and what is necessary to successfully operate the ship. As this meeting took place before actual work on the thesis had begun, it was more introductory to the subject. One of the key takeaways of the talk was that navigation (where the ship presently is) is the single most important issue when operating a ship. Mr Kivimägi also highlighted that DGPS stations are used to calibrate the GPS signal received from satellites. DGPS stations are placed along the shore and this means that it can only be used when the ship is in range of the DGPS station.

Interviewee	Profession	Date
Taivo Kivimägi	Advisor at the Estonian Maritime Authority	03.11.2019 03.05.2020
Indrek Korela	Chief of Information Security at Port of Tallinn	11.03.2020 13.05.2020
Dan Heering	Early Stage Researcher & Project Manager at Taltech	26.03.2020 08.05.2020
Guldar Kivro	Head of Shipping at TS Laevad	30.03.2020
Kristo Klippberg	Technical Consultant and service provider for ships	31.03.2020
Reimo Salumets	IT infrastructure architect at Port of Tallinn	29.04.2020
Artur Kaev	Cargo ship captain	04.05.2020
Meelis Mägi	Marine Safety Manager at TS Laevad	06.05.2020
Jarmo Kõster	Harbor Pilot & Head of Shipping Centre at Taltech	08.05.2020
Tõnis Tikka	Second Officer on MSV Botnica	08.05.2020

Table 1. *Table of interviewees.*

6.2 Visit to Ferry Tiiu with Indrek Korela, 11.03.2020

Port of Tallinn arranged a visit to the ferry Tiiu which operates the Rohuküla-Heltermaa line. During the visit the author was able to converse with Indrek Korela, Chief of Security of Port of Tallinn, captain of Tiiu, and a couple of mechanics.

Similarly to the first meeting/interview, this visit was unstructured and more to understand the side of the crew and company but the visit to Tiiu was much more in-depth. Tiiu can be classified as a modern ship and is relatively new - finished in 2016 [25]. This section will detail the data gathered from the visit.

6.2.1 Ship networks

Firstly, there are three networks on the ship: guest wireless network, office wireless network and ship/OT network. The guest network is unprotected and is connected to the internet, the office network is password protected. The three networks on the ship are separated by a firewall and VLANs/subnets, outside connections including internet is provided by 4G via 2 different service providers for redundancy. All of the connections in and out of the ship go through the central firewall before accessing the internet and the connection between the ship and central firewall is tunneled using VPN/IPSec. The ship OT network is separate from other networks and air-gapped most of the time but

connection is enabled to subsystem providers during maintenance. Connection from the air-gapped network to the maintainer is provided by the same 4G routers on the ship. The ship's internal system communications use TCP/IP all the way down to cyber-physical systems that control mechanical parts of the ship. In addition, in order to enable remote maintenance requires physically plugging in a specific ethernet cable in a specific switch. There is also an additional firewall on the ship that manages network on the ship and prevents traffic between office, guest and OT network.

6.2.2 Bridge

Based on visual inspection there were unused USB ports available but all of them were extremely visible and no doubt a malicious device would be spotted. Some of the visible USB ports were not in use at the time of visit and were intended for use with USB memory sticks or peripherals which means that they are capable of data transfer. Moreover, the mice used to control the ship's ECDIS were wireless (Bluetooth). A potential attacker could compromise the ECDIS's underlying computer via the USB ports or via a potential Bluetooth exploit. According to the captain, ECDIS updates are done weekly. All of unused surfaces were covered by cabinets that could opened with an universal key and according to the captain there should be USB ports. Moreover, the wireless networks were also available from the bridge which in turn can be used together with an internet capable malicious device to compromise ship's internal network and receive/send data using the public WiFi. Usually there is only one person on the bridge during normal operation of the ship.

6.2.3 Physical Security

Physical security on the ship is provided by locked doors and the crew. The crew is always on the ship, including nights. However, during the visit we were taken to the bridge using unlocked doors (probably locked during the night) and it was quite easy to reach the bridge from the passenger area. Moreover, it would be quite simple to acquire the necessary routes from cafeteria workers. There is always a chance of somebody noticing an unauthorized person but that is negligible from the point of view of the attacker. However, as mentioned in subsection 6.2.2 it is somewhat difficult to find a suitable place for a hidden device.

6.2.4 Miscellaneous

The captain of the ship shared an experience from a previous workplace where a failure in the anti-rolling system caused all of the pistons of the system to engage at once and

forces created by the pistons caused the ship to tilt 15 degrees to one side. During the interview the cause was not discussed but it is very useful for the author as an actor can use the Anti-Rolling system for its benefit. However, Tiiu did not contain such system as it is useful in ships that traverse seas and oceans. According to the captain, Tiiu's navigation runs on batteries and all sensors are duplicated to reduce chance of failure. In addition, there are two types of autopilots for ships: automatically correcting autopilot or autopilot that just maintains course and speed.

CSO of Port of Tallinn, Indrek Korela, offered an interesting insight that since the company is relatively new to operating ships and had been offering IT dependent services prior, their cyber resilience is higher compared to a company that only deals with operating ships, especially smaller companies.

The ship has third party personnel who offer services to passengers and use the ship's office network for card terminals, point of sales and other required services for business operations.

6.3 Dan Herring, 26.03.2020

The unstructured interview largely consisted of discussing functional dependencies and experience of Mr. Herring. He provided with useful resources to obtain answers to my questions. Moreover, as someone with experience as a seaman and lately practicing cyber security, Mr. Herring has insights and information to anyone interested. In his experience, the state of cyber security in the field of maritime is dreadful. Especially in terms of network security and segregation allowing attackers that have gained a foothold in the network to access all connected parts of a ship. Obviously this is a general statement but is a good indicator of the current state of affairs.

6.4 Guldar Kivro, 30.03.2020

The interview was a semi-structured interview. On a related note, Mr. Kivro worked on the procurement process of Port of Tallinn's ferries and actually captained one of them from the factory to Estonia thus he can provide extensive insight into the inner-workings of ships.

The meeting discussed primarily topics related to the inner-workings of the ship:

- How data flows in a ship's internal network?

- How is a ship's internal network built? What security measures does the network use?
- Incidents from literature and could similar incidents happen at Port of Tallinn
- Sensor data manipulation. What are fail-safes in terms of malicious actors or other failures?

6.4.1 Data flow in a ship's network

As noted in Chapter 4.3, the literature about a ship's network topology is either scarce or does not go into great depths aside from recommendations to segregate different networks. Mr. Kivro provided information that a ship's internal network is further segregated - Autopilot, Power Management System, Anti-Rolling System, Navigation, CCTV and IAS etc. While they share physical devices, they are logically separated using VLANs and subnets. Moreover, it is difficult to list all the systems as there are many different types of ships and each of them require systems and services that are specific to that type. In terms of data flow, the traffic is always one-way depending on the system, for example PMS and Anti-Rolling Systems are managed from the bridge but do not return any data. Reading data, whether it is from the PMS, Anti-Rolling System or any other cyber-physical system, is handled by the IAS. ECDIS also only reads data from its various sources. However, from this interview it was unclear whether IAS gathered all input data and distributed it around to systems that require it or does IAS have a narrow scope. In addition, there is some confusion or lack of knowledge as to what system obtains information from what system even if you have years of knowledge and extensive hands-on experience [1]. To solve this issue Mr. Kivro kindly made an introduction to Kristo Klippberg who was able to explicitly define ship's internal data flow, please see interview from Chapter 6.5.

In terms of network security, if a malicious actor would be able to access an unused port on a switch for example, there is no network access control in place to stop the "unknown" device from communicating and exchanging data. To the best of their knowledge, lack of access control in a ship's inner network is widespread.

6.4.2 Duplication of sensors and systems

Duplication is key to a ship's operation, especially to its reliability as when a ship is at sea there are no viable options if a critical sensor or system fails. The amount of duplication

[1] Lack of knowledge is not caused by incompetency and is not directed at people interviewed but is a general problem that affects shipping as a whole due to complexity of ships and the sheer number of components present. The complexity causes the decentralization of knowledge and it is unrealistic to expect one person or several to comprehend all of it.

depends on the type and purpose of the ship, as do many aspects of ships. For example, Port of Tallinn has Botnica, a deep diving vessel, and ferries: the duplication on the ships are of different measure. As Botnica has to support diving personnel, it has to keep running no matter what and thus every system/sensor has at least 2 backups. She also has 3 different control centres so that in case of a fire or other serious accident another centre can take over and operate the ship. In stark contrast, the ferries operated by Port of Tallinn duplicate (maximum of 2 of each system) safety-critical systems as the danger to human lives is not so imminent. ECDISs are also commonly duplicated, in the case of ferries they have a total of 4 ECDIS systems onboard, and are autonomous in their processes. Each of ECDISs gathers their own data and processes it meaning they are complete separate. Although, ECDISs are identical in configuration which does not make any attack directed at the ship's ECDIS significantly more difficult. However, the duplication of sensors and systems is in itself a fail-safe - data is compared from each sensor and then compared, in case of a significant difference alarms are raised (the ferries are configured to sound more than 2200 specific alarms).

6.5 Kristo Klippberg, 31.03.2020

Meeting with Kristo Klippberg was very information dense and he provided a lot of information of how different systems work and interact with each other.

The main questions discussed were:

- How is unidirectional data flow ensured?
- What system interacts with what systems? (ECDIS, IAS, VDR, sensors, Autopilot, PMS, Thrusters, Anti-Rolling System, CCTV, AIS, GMDSS)
- How does the ECDIS duplication system work?
- How does sensor data reading work? Is all of the sensor data gathered by IAS and then distributed to the rest of ship's network?

6.5.1 Unidirectional data flow

Typically the data flows one-way - commands are sent to the cyber-physical systems via one network and feedback of the CPS or sensor data is read from a completely separate network. In any case if data is sent "up" from the first network, the network is configured in a way that in such cases the request is dropped. So that the unidirectional flow is ensured by software means, VLANs and subnets, an this configuration of course is prone to human error. However, there is at least one exception - the thrusters of a ship can directly deny a

command from the autopilot.

6.5.2 Sensor interaction

In order for a system to retrieve data from a sensor, the system must make a request to the TPU, serial-to-lan converter, of the sensor and then the TPU will return sensor data. In addition, as sensors tend to be duplicated, background processes of the consumer of sensor data compare readings from same type of sensors and raise an alarm in case the sensor readings difference exceeds a certain threshold. The threshold depends on the type of sensor and data output from the sensors. For example, it is possible to configure ECDIS to use multiple GPS sensors simultaneously and display data from both sensors on the ECDIS screen.

Most of the data read on the ship is handled by two systems: ECDIS and IAS. ECDIS is part of the navigation network and IAS basically handles everything else from the PMS to the ATS. IAS is also responsible for gathering alarms from the navigation network and forwarding them to the VDR for logging purposes. All in all, sensor data is directly accessed by whatever system requires the data but broadly there is only 2 larger systems that read sensor data.

6.5.3 Navigation network

Navigation network is a broader term that encapsulates ECDIS, sensors and radio equipment. Common navigation network setups consist of at least 2 ECDISs where always one is master and the others are slaves. Any change done in the master is always synced with slaves. The changes can be separated into two: configuration changes and other runtime changes. For example, in ECDIS the user can choose which GPS, compass or other sensor it will use from the duplicated sensors. When a switch is made to a different sensor then all of the slave ECDISs will receive the change and also switch to the new sensor. This means that the master ECDIS always chooses the sensors to use. Another example is defining a route, when the route is defined or altered, the new route will be synced to the slaves. Configuration changes are a bit different. Configuration file is persisted in the ECDIS and contains information about network configuration i.e. where what sensor is in the network, where are other ECDIS machines in the network. In case of a configuration change, the modified configuration is distributed to all ECDISs but in order for the new configuration to take effect the ECDISs must be rebooted. Also, it is important to highlight that run-time changes are synced in real-time.

Apart of duplicating ECDISs, there is built-in redundancy for network failures. All of the ECDISs are connected to each other and are in the same network, each ECDIS has its own switch and in case of cable or device failure, an ECDIS can use another ECDIS's network connection. The switch over is immediate and will raise an alarm in the bridge.

6.5.4 VDR

Every alarm generated in the ship is logged into VDR, every sensor input is logged as well, for example the thruster positions, revolutions of the engine, power of the engine etc. In addition, every 10 seconds a screenshot is done of the ECDIS screen, all radio communication of the crew is stored. Moreover, there are microphones in the bridge and all of that is persisted in the VDR. Every change to configuration, every change in the ECDIS - everything is logged and stored in the case of incidents.

6.5.5 CCTV

Mr. Klippberg also said that CCTV systems have the capability of calibrating themselves by gyroscope sensor data. In addition, some ships possess the ability to enable tracking mode so that cameras follow an object.

6.5.6 Personal Incident Experience

Mr. Klippberg shared an experience when he was working on a ship in the Vene-Balti ship factory. During his time there, a second ship in the factory was being retrofitted with some sort of GPS jamming/spoofing equipment. As soon as the modified ship had left the factory, it seemingly enabled the newly installed equipment and caused the nearby ships to show themselves to be in the vicinity of Vanasadam of Tallinn including the ship that Mr. Klippberg was working on.

6.6 Structured interviews

The idea behind structured interviews is to present the created attacks in Section 7.1 to people working in the maritime field and gather their ideas. So far the interviews were for gathering background information in order to create the attacks that are presented during structured interviews.

While attack trees make sense for illustrating and condensing data points, they are difficult to understand for people unfamiliar with them. Furthermore, the knowledge and skill

in English of the interviewees is unknown so due to the aforementioned reasons, the attacks were translated into Estonian with explanations. The exact material shown to the interviewees can be seen in Appendix B. In addition, the material was sent to the interviewees beforehand in order to give them time to familiarize and gather ideas about the attacks. However, some interviewees were unable to familiarize with material before the interview due to time schedule issues or the material was not received by the interviewee as some of the interviews were arranged by third parties and did not forward the material. Specific questions and topics posed to the interviewees can be seen in Table 2.

After conducting the interviews, it was apparent that interviewees, who prior to the interview had read through the attack descriptions, provided more applicable and additional information. This can be attributed inexperience of the author in terms of conducting interviews. Moreover, some questions posed to the interviewees were too broad and the author was unable to extract useful information.

6.6.1 Results of structured interviews

The second round of interviews lasted from 29th of April 2020 until 13th of May 2020 and consisted of 8 different interviews. The interviewees were Taivo Kivimägi, Reimo Suurmets, Meelis Mägi, Artur Kaev, Jarmo Kõster, Tõnis Tikka, Dan Heering and Indrek Korela. As the interviews consisted of the same content and questions, there is no real benefit to list and describe each interview separately.

Gaining a foothold in the ship

Interviewees agreed with the proposed attack scenarios for gaining initial foothold in a ship while largely anything is possible they tended to say that hiring a disgruntled employee of a ship or influencing a port employee, especially viable in third world countries, would be the most likely scenario. Per procedures anybody outside the crew of a ship visiting it, should be accompanied by at least one crew member but human factor plays a big role in this case, for example a port employee known to the crew might be trusted. Mr. Kaev highlighted that some ports follow strict physical security rules and protocols while others neglect it entirely, Mr. Heering expressed a similar sentiment. Reimo Suurmets put forth an idea about a spear-phishing attack where the attacker would find out maintenance schedule of the target ship and at the appropriate time pretend to be the maintainer. An alert crew would check documents but it is not out of the realm of possibility that the attacker could just walk aboard the ship without anybody asking questions and insert a malicious device, this was also something that the interviewees deemed likely. Obviously there is the risk of the actual maintenance worker arriving at the same time but that can be

Topic	Question
Gaining foothold	What is the likeliness of the attacker sneaking onto the ship and install malicious device? Do you have proposals for gaining a foothold in the ship? Are there any differences in operation and procedures on a ship at sea vs at port? Would a malicious device be noticeable and identifiable during maintenance or routine inspections? Is it likely that a malicious device would be spotted?
Crash ship	What are your thoughts about the scenario where attacker sends commands to the thrusters at a preset time? What is something that the attacker could do to increase the likeliness of the attack succeeding? Do you have any ideas about a scenario that also might lead to crashing the ship?
Capsize the ship	What aspects should the attacker take into account in the case of the proposed scenario? What kind of factors stop the attack from succeeding?
Immobilize ship	What mechanical component is the most vulnerable and should be targeted? What mechanical components could be repaired on the ship? What would be the course of action upon detection that some mechanical component is about break/malfunction? What is the course of action in the case of failure of the IT-based navigational aids? What are the main situations when the crew decides to call a tug or that the ship is uncontrollable?
Operational view	What are the main tools used for operational view at the crew's disposal? What systems on a ship should malfunction in order for the crew to stop normal operation? How does weather affect operation of the ship?
General	What kind of accidents do you have in mind when you think of ships? Do you have any ideas that have not been mentioned? How would the crew detect manipulation of sensor data? How is the vessel OT network separated from the office network? How is additional network segregation achieved in the OT network? Do you agree that your name will be published in this thesis?

Table 2. *Questions and topics discussed during structured interviews.*

solved using social engineering techniques, for example calling the maintenance company and cancelling the appointment. Mr. Kaev also brought to the author's attention that every time a cargo ship arrives at port, the port authority provides them with a disc or USB that contains cargo information and is supposed to be loaded into the cargo management system of a ship. Procedures dictate that the removable media should be scanned with antivirus software before inserting into the cargo management system but human error (laziness or time pressure) may cause ignorance of such procedures, not to mention that the antivirus is ineffective against unknown malware.

As to a crew member or a maintenance worker noticing a malicious and foreign device attached to a system, the interviewees largely agreed that it would be unlikely that somebody would notice. Mr. Mägi said that on Port of Tallinn's ships they stress the need to spot something out of the ordinary but in reality that applies to locations that are in view of the crew. The idea proposed to the interviewees was that the malicious device would be hidden and would only be visible in the case of maintenance in that exact location, for example the malicious device could be hidden in a electrical cabinet. The ideas seemed to converge that at some point it would be spotted but the actual timescale is hard to pinpoint. Tõnis Tikka said that due to the computerization of his ship, MSV Botnica, the crew in reality has no idea what devices are in their computer hardware rooms meaning that the crew is not able to spot anything that does not belong there. IT department of the company maintains and manages such areas thus the malicious device can remain undiscovered for extended periods of time, especially when the ship is doing its duties out at sea. Moreover, Mr. Kaev highlighted the issue with cargo ships and proposed another attack vector - upon arrival to port cargo ships are given a removable media containing information about the cargo that will be loaded onto the ship and that removable media will be inserted into the ship's cargo management. Moreover, he also said that is impossible to verify that the cargo information given by the authorities matches the cargo actually loaded onto the ship. This is something that supports one result of the SLR 43 where the authors proposed the idea of smuggling malicious hardware onto the ship as cargo. Also, according to Artur Kaev more often than not it is necessary to print out documents from a port authority removable media - a possible attack vector in case best practice procedures are ignored.

Crash ship

The most accepted and likely scenario according to the interviewees was the control over the propulsion device of the ship and sending malicious commands at a preset time or location. The likeliness of the scenario succeeding largely depends on the location, for example according to the interviewees the best locations would near docks, ports or when navigating rivers. Areas with small spaces that translate into miniscule margin of error

and narrow time window for reaction, additional examples could include Rukki Canal in Estonia or waterways between small rocky islands on the approach to Helsinki. Crew response time could be hindered by ignoring wheel commands from the bridge and closing the water-/fireproof doors, proposed by Taivo Kivimägi, to increase the time it takes to reach the propulsion device physical system that can be used in emergency situations.

Rest of the scenarios that were based on modifying sensor data, using malicious charts and manipulating autopilot were deemed less likely but likely nonetheless. It was also apparent that the interviewees placed huge amounts of trust into ECDIS charts and largely doubted the idea of the possibility of inserting malicious charts into the ship's ECDIS. Furthermore, the scenarios of modifying GPS data to force the captain or autopilot to take an unsafe route, would basically require that a person that does not pay attention to anything be at the helm of the ship.

Capsize ship

Objective of capsizing a ship largely was categorized as fiction and very unlikely. Although, it has and can happen it would be extremely unlikely that an attacker, especially an attacker focusing on cyber means, could induce a situation where a ship would capsize. Ballast pumps would be a ineffective option of creating a leaning effect in the ship as they are slow and typically used when docked. However, Anti-Rolling System is meant to be used during operation at sea and is much quicker in order to create the leaning effect. Jarmo Kõster put forth an idea to use the anti-fire system to pump water into the higher levels of ship decks to affect the buoyancy and general balance of the ship. He also highlighted that ships generally do not burn down but rather capsize and sink due to the weight of water used to extinguish the fire. However, the anti-fire system scenario suffers from the same flaws as ballast pumps since the anti-fire system can only pump a certain amount of water. Moreover, it would rely on nobody noticing that large quantities of water is flowing in higher level of decks. Based on Jarmo Kõster, Tõnis Tikka and Dan Heering the most likely scenario to succeed, although still extremely unlikely and requires incompetence from the crew, would be to somehow relocate large amounts of weight around the ship, specifically cargo. For example, cargo ships and some passenger ships transport trucks and trailers, this cargo might not be fastened properly. If the attacker could start moving the trucks and trailers by assuming control of the propulsion device and anti-rolling system, the attacker could create further instability by moving the cargo around ultimately capsizing the ship. The factor of human error cannot be stressed enough, creating the conditions of capsizing the ship would not be instant and extremely noticeable to the crew - Tõnis Tikka said that already a tilt of 3 degrees is very noticeable and there is a long way to go from several degrees to whatever tilt is required for capsizing the ship. In the event of calm

weather, it is very doubtful that this scenario could manifest. However, during terrible and stormy weather the attack would be more likely but in that case the attacker would play a small role in capsizing the ship as most is caused by the weather itself. Just to illustrate, Artur Kaev shared a personal experience where the ship was 5 degrees away from the limit of positive stability[2] after being caught in a storm.

Interviewees disagreed about what ship types would be the most susceptible to such an attack. Taivo Kivimägi thought that empty container and tanker ships would be most unstable and dismissed the idea of capsizing a cruise ship due to the low amount of movable weight by the attacker. Tõnis Tikka thought that cruise ships were more likely to capsize mainly due to their height, something that seemed logical to the author before conducting the interviews. Artur Kaev dismissed the idea of capsizing a container ship and proposed the idea of cargo ships, specifically cargo ships that carry trucks and trailers. Jarmo Kõster agreed with that proposal, especially if the heavier trucks and trailers are placed on higher levels. Nobody is right or wrong but the differences in ideas perfectly illustrates the uncertainty aspect of this attack and should be investigated further, possibly including ship engineers and designers into the discussion.

Immobilise the ship

Based on the interviews, it turned out that the best way to immobilize a ship would be to focus on a ship's communications rather than breaking mechanical components. Artur Kaev mentioned that prior to arriving to port, the ship must send documents to the port authority. Failure to do so, would result in fines and/or increased time spent in port due to document processing effectively immobilizing the ship. In some cases it might be possible to send the documents from the company's land based offices but most cases only the ship crew can send the appropriate documents. In essence if the attacker could disable communication to the outside world, mainly internet access using satellites, the crew would not be able to send the documents to the port resulting in economic loss to the company. Moreover, disabling all of the ECDISs on a ship would effectively immobilize the ship at least when arriving to port the ship would not be able to leave before the root cause has been found out and the problem solved. This only applies to cases where there are no paperback charts on the ship.

The initial idea of stressing the main engine by increasing the revolutions of the engines to reach a critical limit causing it to break was thought to be possible but after discussing with the interviewees it was deemed to be rather unlikely to succeed. The engine should be at a critical limit for a while and the forces (sound, vibration etc) created by the engine would

[2]Technical specification of the ship where if the ship exceeds this number, the ship will capsize. https://en.m.wikipedia.org/wiki/Limit_of_positive_stability

be too noticeable. It could be possible to stop oil or air flow in the engine causing it to stall or break. However, the author is unsure whether it is possible and how widespread such engine control systems are. Moreover, the interviewees said that determining what the attacker could affect should be asked from mechanics highlighting the need to expand the pool of interviewees in case of future research. Meelis Mägi helpfully pointed out that in case of an attack against mechanical components some countermeasures by the crew might not be possible. For example, when the attacker is manipulating mechanical components during stormy seas the crew cannot just turn off the engine to avoid mechanical damage as that could create a larger safety issue.

Block operational view

Big part of the safety system are the configurable alarms in the ship. Ferry Tiiu has around 2200 and Jarmo Kõster shared that one of the cruise ships that used to come to Tallinn had a total of 56 000 different alarms. As the alarms are sensor and parameter based, it would be very instrumental for the attacker to modify sensor data or suppress the alarms. Of course this depends whether the alarms are configured, based on the interviews and literature there are examples of both situations. In no particular order, the 4 most important sensors for operating a ship are compass, radar, GPS and echo sounder. The aforementioned sensors should be the priority of an attacker.

Human Aspect

Bulk of this thesis does not discuss the human aspect of attacking a ship but after the second round of interviews it is important to highlight this aspect. As many things related to computers and IT, the weakest links tend to be humans or human related. Simple errors can manifest themselves in magnitudes larger consequences. Artur Kaev shared a personal experience where the crew contacted a port agent a day prior to arriving to port in order to agree the time and location of rendezvous point with the harbor pilot[3]. The crew member responsible writing down the coordinates made an error of 1 degree that resulted in the ship being in the wrong location by 60 nautical miles. Moreover, the captain or any other crew member should have noticed that the incorrect location was basically in the middle of the sea. These simple communication errors and lack of double checking or momentary hesitations are the biggest threat to ships and shipping in general.

All of the proposed attacks rely on some degree of human error and during the interviews the author tried to find the best timing and location of an attack where the crew might not be so alert and the response time be delayed. The interviewees agreed that the alertness of

[3]Harbor pilot is an employee of the port who knows the port area waters extremely well and helps the crew of a ship safely navigate the waters into the port.

the crew is lowest between 02:00 and 04:00, especially during the 4 o'clock shift change. While weather is outside of the attackers control, with enough resources it could be possible to execute the attack during a specific weather event. This where the interviewees opinions deviated a bit but the larger sentiment was that stormy weather would be the best option from the point of view of the attacker, especially when trying to crash the ship. Modifications done to sensor data or manipulation of wheel controls might not be so easily spotted by the crew. Moreover, the attacker could affect the trust in sensor and interface data by creating false alarms or showing incorrect sensor data prior to the attack. This technique could be used several times so that in case of the actual attack, the crew might dismiss alarms or sensor data as being bogus and false positive before realizing that the data is genuine. However, this approach can be a bit pointless as it assumes that the attacker has control of the specific sensor or alarm and in that case it might make sense to completely suppress the alarms or just modify sensor data to reduce the chance of spotting something out of the ordinary.

Mentality of the crew is also an aspect that should be considered. Jarmo Kõster shared a glimpse into the crew that when the crew discovers that something has gone amiss, pretty much the last thing the crew expects is an attack. The premise applies even more to cyber attacks. For this reason, response of the crew might further be delayed while the crew tries to solve the problem that may or may not solve the issue.

Experience as with many things play a big role as well. The physical feeling of a ship is extremely important, seasoned members of the crew, especially the captain and chief officer, set certain marks when operating a ship and can feel abnormal things. Best explained using the term sixth sense. The ability of this "sixth sense" decreases when moving down the hierarchy of the ship, second or third officers rely more on the interface and sensor data. The same principle applies to mechanics - chief mechanic can detect some problems only by sound.

Miscellaneous

The type of ship plays a large role determining what kind of attacks are possible against a ship. Repeatedly during our interview, Artur Kaev stressed that cargo ships are significantly behind in terms of technology installed to the ship compared to passenger ships. Jarmo Kõster agreed with that statement and outlined the difference in cargo as the main reason. The responsibility and risk in transporting humans is far greater than containers. This principle also applies to duplication and attention to safety where passenger ships have more redundancy built-in.

When interviewing and asking feedback about the attacks from Indrek Korela he correctly pointed out that for a successful attack the actor should have means, opportunity and motivation. Specifically he did not find the motivation component of the attacks due to the resource intensiveness of conducting a successful attack. The amount of different variables, for example the vessel network configuration or other insider knowledge, and procedures an actor would have to identify before even designing and launching the attack means that the reward compared to resources required are greatly out of balance in favor of the resources invested into the attack. Moreover, extracting real monetary gain is nonviable or rather pointless by targeting ships specifically. For those reasons he found it difficult to identity motivation component in the proposed attacks. Even if an entity would possess all of the three components, there would targets with much better risk-to-reward ratios that would better suit an entity to whom monetary gain is secondary or even irrelevant. The ideas and reasons put forth by Mr. Korela are extremely logical and reasoned in the opinion of the author completely agreeing with him. According to Mr. Korela, the attacks are possible but the likelihood of the attacks is rather unlikely due to the missing motivation component.

7. Attacks

The main contribution of this thesis is the possible attacks and scenarios that could be executed in order to take control of the ship and ultimately cause monetary or other types of damage, both the attacks and scenarios could be used as an input for a risk assessment. The attacks created below only take into account systems that are more-or-less critical to operating a bare minimum of a modern ship and auxiliary systems, for example entertainment systems in a cruise ship have not been included for the sake of simplicity and generality. Similarly, duplication of certain systems has been excluded, for example ECDIS or sensors as properly planned and build ships should include built-in redundancy but the situation in reality is sometimes bleak (SLR 46).

The attack trees were built using SecurITree®[1] by Amenaza Technologies who kindly provided a free licence for this thesis.

7.1 Goals

During the thesis the author determined the ultimate goal would be damaging the ship as the impact of this goal includes monetary and safety loss impacts. The author has identified 3 major goals: crashing the ship, capsizing the ship and immobilizing the ship. All of them can cause monetary and safety loss, potentially even loss of human lives. While all of the result in physical consequences, they are achieved mainly via cyber means but physical means must also be used in the majority of cases, especially at the lower levels of the attacks. In the created attacks by physical means it is meant that in order to gain a foothold in the ship's system, the attacker may be required to physically access and be in the vicinity of the targeted system. Each of the proposed goals is separated to a different attack tree for ease of use and a total of 17 scenarios were identified across the 3 goals - 11 for crashing a ship, 1 for capsizing a ship and 5 for immobilizing a ship. However, due to the separation of the attacks trees and unifying parts of them like loss of operational view and gain initial foothold the actual number of potential scenarios is much larger as the number of scenarios calculation is based on the software used for this thesis.

[1] SecuriTree®by Amenaza Technologies. For more information, please visit https://www.amenaza.com/SS-what_is.php

7.2 Common parts of the attack tree

All of the three goals share a lot of nodes or sub-trees that are identical, such as blocking operational view where the attacker modifies operational technology in a way that would deprive the crew of necessary information or how to get initial access to the ship's internal network from where to mount the rest of the attack. This section will detail the common parts of the attack tree.

As a note, some nodes in the following attack trees are shortened to avoid repetition. While it is not an ideal solution, it makes different attacks more digestible to the reader and frankly makes it easier to edit the trees as a change must be made in one tree instead of several. In addition, some attacks are more probable than others and the author does not differentiate between them based on probability but the created attacks could be used as an input to do exactly that in another paper.

7.2.1 Gaining a foothold in the ship

Broadly there are 3 ways for the attacker to gain a foothold in the ship:

- Physically sneak onto the ship and place malicious device where necessary
- Compromise an intermediate device, maintenance computer or removable media, that is used for maintenance or routine operation, like ECDIS update, on a ship
- Exploit an external vulnerable interface that is connected to the ship's internal network

The most consistent, in the author's opinion, approach would be to gain physical access to the ship, be it some control room but the for the best results gaining access to the bridge would be bring best/worst abilities depending on the point of view. The consistency comes from that with physical access it is possible to access all major systems but cyber means might not allow access everywhere, obviously this greatly depends on the network configuration. Although this approach is difficult, it is still doable. One of the ways to achieve this goal would be to adapt the Trojan horse attack where the attacker would find an insider to work to the attacker's benefit, node "Trojan Horse Attack" in Figure 5. Given enough resources and time to the malicious attacker, it would be probable that the attacker would be able to find a crew member, harbor pilot or employee that was willing to smuggle and attach a malicious device to the intended system(s) (SLR 29). Another probable method would be for the attacker itself to sneak onboard the ship and crew area, node "Physically sneak onto the ship" in Figure 5. In case of passenger ships it would

be easier but an unfamiliar face could easily be spotted, especially in the crew area. In such a situation, a spot of social engineering could increase the likeliness of the initial objective of gaining a foothold succeeding, for example pretend to be a Cyber Security student in Taltech and use the excuse of gathering information for a Master thesis. Another option would be to use spear-phishing to find out maintenance dates and pretend to be a maintenance worker, node "Pretend to be a maintenance worker" in Figure 5. However, the attacker would have to exactly know where to place the malicious device in terms of available port and the physical schematics of the ship but that kind of information could be retrieved via social engineering techniques, for example from Facebook or other social media SLR 41, or finding an employee willing to help. After the malicious device has been connected to the ship's network, command and control of the device might be possible. One possibility is that the malicious device could be a Raspberry Pi with WiFi that could use guest WiFi for communication or a 4G enabled Raspberry Pi which would lower the chance of being detected although connectivity issues might arise.

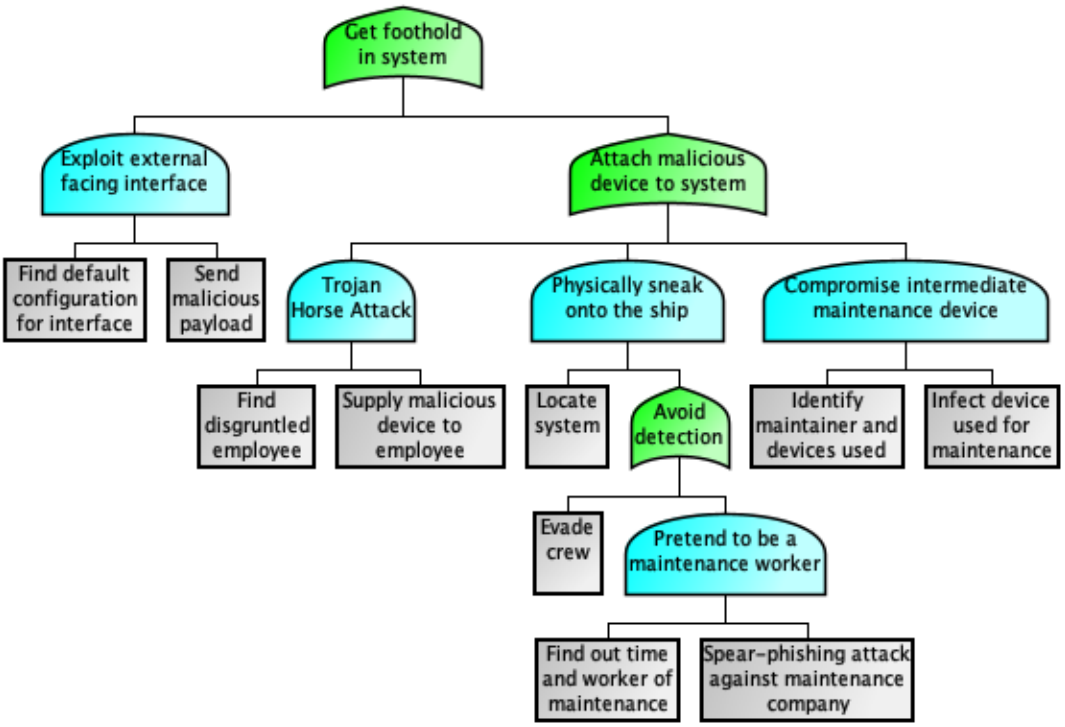

Figure 5. *General attack tree for gaining a foothold in a system.*

Certain maintenance activities on a ship can be done remotely but on-premise maintenance is still required, for some components at least. If the attacker infected a maintenance worker's laptop and the maintenance required connecting the equipment being serviced and the worker's laptop, it would be possible for the attacker to spread malware to the serviced system (SLR 23), node "Compromise intermediate maintenance device" in Figure 5. There is a real-life example of this when a service worker connected a device that

contained malware and the malware spread to the system delaying the ship's release from dry-docks [26]. Certainly it would also be possible to conduct privilege escalation and/or infect other systems on a ship from where the attacker can mount an attack against the whole ship. A more day-to-day variant of the same thing would be routine ECDIS chart updates done via removable media, node "Attach malicious device into ECDIS" in Figure 6, or cargo related updates received from port authorities via removable media. If an attacker could infect the removable media used for such cases, the attacker could in turn infect the ECDIS computer and from there do a great deal of damage, Nissim, Yahalom and Elovici describe possible techniques in [27]. Obviously, there should be certain procedures set for these kinds of cases but human factor or time pressure might result in ignoring these procedures and introducing unknown devices to the machine (SLR 37).

In terms of exploiting external facing interfaces, node "Exploit external facing interface" in Figure 5, there are possibilities but this area is rather foggy. There are ECDIS setups that use the internet to update its charts and it may be possible to infect the ECDIS computer by attaching malware to the charts, deemed unlikely by experts in Section 6.6 and displayed in Figure 6, or as the ECDIS computer typically uses older versions of Windows and in cases of it being connected to the internet or the attacker already having a presence in the OT network, certain remote vulnerabilities in Windows could be exploited by the attacker (SLR 24, 36, 34, 17). There are also real-life examples of attackers extracting model of VSAT equipment used in a ship based on AIS data and in many cases the default configuration of VSAT equipment is freely available on the internet which the attacker could use to to access the ship's internal network, ultimately giving the attacker the ability to modify data, such as GPS coordinates, and even upload malware [28].

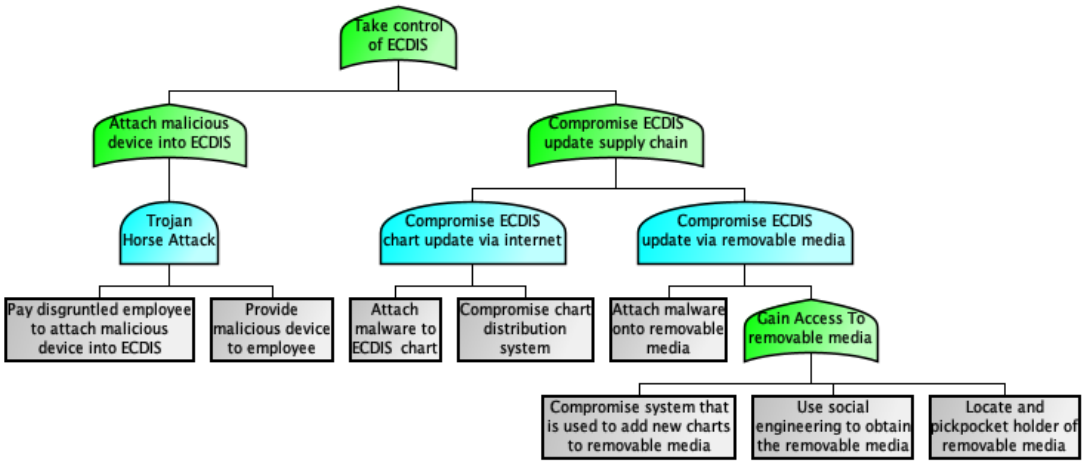

Figure 6. *Attack tree for gaining control of ECDIS.*

7.2.2 Loss of Operational View

Operational view is paramount for the normal and safe operation of a ship. The state of operational view depends on many things and there are some that an attacker could affect whereas some are out of control of the attacker but with good timing or luck it could help the attacker achieve its goals. First and foremost, the attacker could affect the key problem in shipping - the navigation problem (Interview 6.1). This includes disabling ECDIS via various means or modifying the sensor data, different auxiliary sensors could be affected. Key sensors to affect would be GPS, echo sounder, radar and compass for the navigation network. In terms of rest of the ship it really depends on the attack goal and systems affected, for example attacking the propulsion device would require to affect propulsion device sensors or in the case of trying to break the engine the attacker should modify engine feedback related sensors.

Roughly there are two ways to modify sensor data: directly at the consumer of data i.e. before the data is processed (SLR 25, 26), for example modify GPS data before ECDIS indigestion, or at the TPU from where sensor data is distributed to the OT network, node "Modify Sensor Data" in Figure 7. Additionally the attacker could affect the confidence in sensor data and feedback shown to the crew, node "Create diversions" in Figure 7. For example, several days or hours before executing an attack where the attacker sends malicious commands to the wheel and/or propulsion device, the attacker could sporadically display invalid position or direction of the propulsion device so that when the actual attack happens the crew would initially think that the sensor is malfunctioning. In addition, bulk of the alarms configured are raised only if some sensor data is outside of certain thresholds and the attacker could use similar techniques to achieve the same result - affect the confidence in the data thereby creating a diversion. Moreover, when such helpful data is no longer trustworthy it could cause the workload of the crew to increase immediately as the crew would have to validate data shown in the interfaces. This of course depends on the crew noticing that something is wrong and overreliance on interface data has been documented in [29, 30].

Disabling ECDIS, primary tool in navigation, could also be made unusable, node "Disable ECDIS in Figure 7. For example, if the GPS sensors in a ship failed, the ECDIS screen would not be able to update the ship's location on screen and the crew would have to rely on manual methods in order to determine the ship's location in real-time (SLR 15). Another method would be to conduct a Denial of Service on ECDIS, if ECDIS is under the control of the attacker and the attacker would introduce huge computations that would cause the actor introduced program to consume all of the available computational power therefore it would leave none to the servicing of ECDIS effectively disabling it (SLR 35).

In addition, it could be possible for the attacker to encrypt critical files of the ECDIS software making it impossible to run ECDIS (SLR 44). Developing on the same principle, the attacker could corrupt or delete ECDIS' underlying OS installation and non OS related files. Kristo Klippberg in his interview, see Section 6.5, revealed that certain systems[2] use configuration files that contain data about the network - where what system or sensor is. An attacker with sufficient control could encrypt or modify those files in a way that data is lost and the crew is unable to restore the correct configuration, node "Hide sensors" in Figure 7. This effectively would create a denial of service as the crew would be unable to use sensor data.

Weather events are something that are outside of the attacker's control but stormy weather could seriously inspect visual means of operational view. In case of bad timing, the response to an attack could be delayed or even worsen the results. An attacker could decide the timing of an attack via freely available websites such MarineTraffic[3] and plan accordingly depending on the destination. However, this thesis is primarily concerned of cyber means thus such kind of phenomena is really not in the scope but should still be considered.

7.2.3 Clean up

Typically major actions in the ship, communications, alarms or system changes, leave behind a digital trail in terms of logs. The main point of logging in a ship is the VDR and in order to hide tracks of malicious activity, VDR should receive priority from the attacker. Mainly there are two ways to achieve this: stop a certain system that the attacker has under control sending log data to VDR or corrupt the VDR entirely. There are also historical examples of a USB memory stick attached to the VDR that contained malware and corrupted all of the data in the VDR [31] (SLR 30).

[2]For example ECDIS or IAS. It is unknown to the author whether other components of the ship, like wheel, autopilot, also have configuration files which contain information about their subcomponents.

[3]https://www.marinetraffic.com/

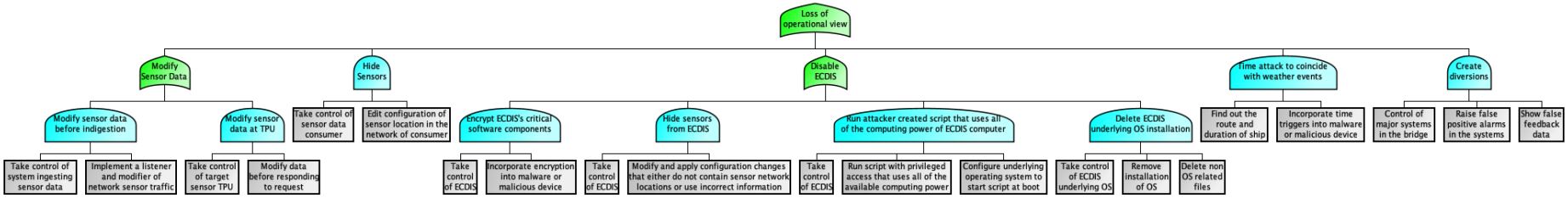

Figure 7. *Attack tree for creating loss of operational view.*

7.3 Crashing the ship

Out of the three goals, crashing a ship is the second most damaging. While it may not be as dangerous as capsizing a ship, crashing the ship can cause harm to lives and it is possible that as a consequence the ship capsizes, for example the Costa Concordia incident in 2012 [32]. The proposed attack tree for crashing a ship can be seen in Figure 8.

Broadly crashing of a ship can be separated into two: crash into another ship, iceberg or any other floating object and running the ship aground. For both options it would be necessary to for the attacker to create a situation where the captain or autopilot[4] made a decision to set the course of the ship with an object or landmass. The "simplest" way would be to use a GPS spoofer or a more difficult method would be to modify GPS data in the ship's network in real time as this method relies on the attacker having a foothold in the ship's network (SLR 2, 3, 25, 26, 39). However, usage of a GPS spoofer requires that the attacker be in the geographical vicinity of the ship but this could be solved by smuggling malicious hardware onto the ship's cargo area (SLR 43). Both methods rely on the same principal of moving the ship's location from its actual location persuading whatever/whoever, nodes "Force autopilot to change course" and "Force captain to change course" in Figure 8, is in control to take corrective measures that would actually move the ship away of its correct location. On its own the attack would be most successful in narrow canals where there are little landmarks to navigate by and especially locations where the crew has no prior experience navigating through, something that shift changes might affect (SLR 28). Still it would be possible to increase the chance of success by incorporating the use of malicious charts in ECDIS (SLR 12) as alarms should be raised, depending on the configuration, when ECDIS detects a collision course or in case the water depth reaches a critical limit. An attacker could make charts with incorrect depth readings, major landmarks/object removed from the charts, for example massive stones just below the surface that could damage the ship's hull. The attacker then could design the malware in way that if the ship reaches a certain area, the malware should gradually, so that it is not so noticeable to a human, start modifying GPS data so that the corrections taken by the controller, either captain or tracking autopilot (SLR 27), of the ship's wheel would result in a direct impact with the removed object. Another option would be to add an object to the chart that in reality does not exist together with incorrect depth readings. In this case, the captain of the ship would have to manoeuvre around, manually or plan the route in ECDIS accordingly, the fake object thinking that at either side of the object there is sufficient depth in water to accommodate the ship resulting in running aground. One other option was also identified for autopilot, node "Overwrite route in ECDIS" in

[4]Here the author specifically means a tracking autopilot as the most basic autopilot does not make decisions on its own and the course set depends on the captain.

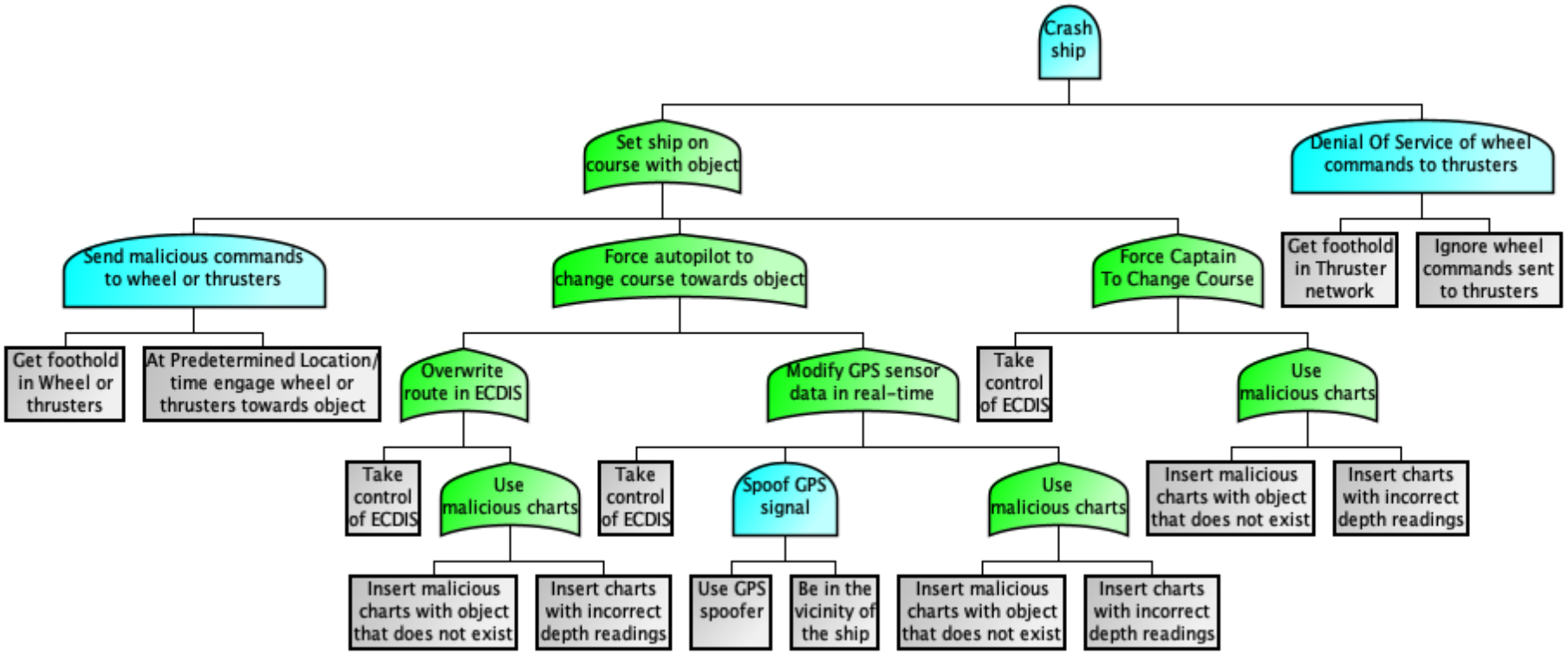

Figure 8. *Attack tree for crashing ship.*

Figure 8. It could be possible for the attacker to modify the route specified in ECDIS forcing the autopilot to take corrective measures. This should also be done gradually in order to avoid detection by the human eye. Finally, a possible attack without the input of crew or autopilot, node "Send malicious commands to wheel or thrusters" in Figure 8, was also identified predicating that the attacker has control of either thrusters or the wheel and knowledge of the ship's route. The malware could activate in a certain geographical location and send a command to the thrusters to turn towards the shore or an object, for example a dock. All of the proposed attacks can and should be incorporated with DoS of wheel commands if the attacker possesses the ability to detect that a collision course has been set, node "Denial of Service of wheel commands to thrusters" in Figure 8.

7.4 Capsize the ship

Capsizing the ship, displayed in Figure 9, follows an easy principle - direct all of the physical and malleable forces in a ship in the same direction (SLR 45). A simplistic example of the attack would be this: firstly, the attacker commands the ballast pumps to pump everything to the left side of the ship causing the ship to lean to the left, then the attacker commands the thrusters to engage at 100% and turn the right ship that would amplify the leaning of the ship and finally send similar commands to the anti-rolling system to add additional amplification to the lean in one direction. This should theoretically lead to the ship capsizing. Additionally the leaning effect can be enhanced with precise timing and gyroscope sensor data. An attacker using gyroscope sensor data could determine wavelength of the sea surface and execute the attack in the exact moment when the tilt of the ship is at its peak due to weather conditions. Moreover, the worse the weather conditions the more likely it is for the attack to succeed. To accomplish this, the attacker should have control of the thrusters, the ballast system, anti-rolling system of the ship (if applicable as all ships do not have this system) and sensor data of the affected systems so to limit the situational awareness of the crew. This attack is not as universal as crashing the ship in terms of applicability due to the systems attacked and difference in stability of ship types, for example the ferries operated by Port of Tallinn is not a viable target for this attack but cargo or cruise ships might be according to experts interviewed.

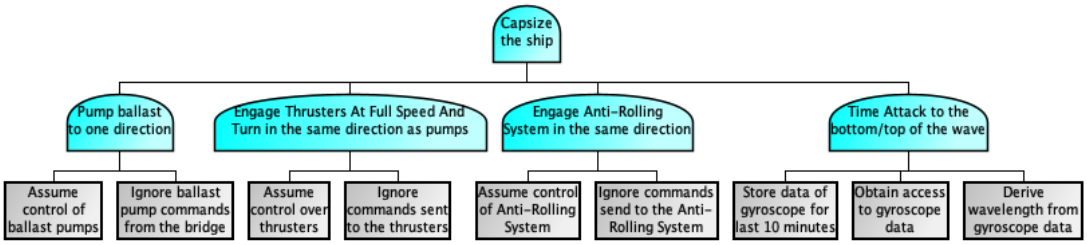

Figure 9. *Attack tree for capsizing a ship.*

The thing is that physical security and physical design features have been developed over centuries. And surely, the author is not the first to think of capsizing a ship by a "malfunctioning" system. The author's best guess is that when the stars align, it might be possible with extreme weather but ship designers and engineers make sure that such a scenario can never come into fruition. Another limitation is that ballast pumps are slow and usually have manual valves to override electronics, further difficulties are discussed in Section 6.6.1.

7.5 Immobilize the ship

Basic idea behind immobilizing the ship is to inhibit or completely make it impossible for the ship to keep moving or continuing normal operation. This goal can be achieved by making the critical systems unresponsive to the user input or induce a situation where mechanical failure occurs (SLR 33). In case of denial of service attack, the unresponsiveness might not be permanent depending on the attack vectors but it also must be taken into account that some ships do not contain personnel with sufficient IT-skills to solve the issue and the attacker might be able to disable communications with the outside world. In case of inducing mechanical failure, if the damage is sufficient it could leave the ship stranded and in need of towing. As with other attacks timing of the attack is extremely important in terms of actual damage done. A ship that is inoperable in stormy waters and/or remote waters make for a dangerous combination that may ultimately lead to the ship sinking and loss of human life not to mention economic damages that result in repairing the ship, time lost etc.

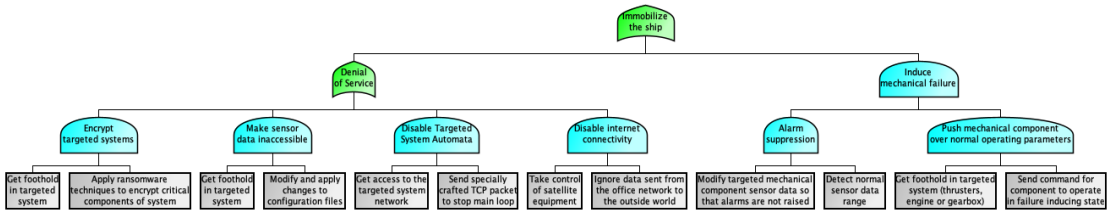

Figure 10. *Attack tree for immobilizing a ship.*

Disabling the automata that control the thrusters or PMS would be possible as it is possible to send specially crafted TCP packets that will stop the main loop, for the normal operation to continue the automata require a restart (SLR 31). In addition, researchers have demonstrated in a simulated environment that in some cases it is possible to write directly to the memory of the automata and ignore user commands (SLR 32). Another possibility is to attach a malicious device to the targeted system networks and ignore commands given to the systems. While this exactly does not immobilize the ship, it does make it

uncontrollable and that's as bad if not even worse than an immobile ship. Finding the cause and a rogue device on the network could provide to be difficult and time consuming for the crew due to the complexity of a ship. Moreover, it could be possible to attack and control certain systems similarly to ransomware attacks by encrypting the data on critical system persistent memory (SLR 44). In addition, an attacker could borrow ideas from Loss of Operational View. The attacker would in this case modify the configuration files and effectively blind the crew of the real-time state of the ship. There is a scenario that would result in immobilizing the ship as the crew would have enormous difficulties in navigating the ship and would have to rely on manual means which allow operation of the ship in some capacity but not full. It could result in having the crew take a decision to halt the ship and wait for assistance. Finally, the second round of interviews informed that certain documents must be sent to destination port before arriving. If the attacker could disable internet connectivity of the ship, specifically office network, then the crew would be unable to send the required documents which would result in extra time spent in port or in the vicinity of it. Either way the ship would be delayed and stay idle while the issue is being handled and immobilizing the ship.

Mechanical failure could be induced by the attacker having control over the mechanical parts of a ship and sending commands that would increase the load over certain thresholds and strain on the mechanical components. As it stands the author currently has no information about fail-safes for situations like this but it would be paramount for the attacker to be able to modify sensor data of the mechanical component affected. Most likely the damage would not occur immediately and would take time, time that could be used by the crew to stop the attack and implement countermeasures. Thus the attacker would have to modify the sensor data in a way that would not indicate to the crew that something is amiss. As to the target system for mechanical failure, most promising would be the engines/generators, thrusters or gearbox. Breaking the engine/generators would effectively create a domino effect where thrusters are unusable and would affect the rest of the ship as electricity generation might not match consumption but gearbox and thrusters are as good for immobilizing the ship.

8. Discussion

Even though the literature for maritime cyber security is scarce, there is still an abundance of information available. Processing of the content provides invaluable insight on how the ship should operate versus how it should not be operated. Yet the lack of centralized knowledge create a high glass ceiling for anyone interested in the field by requiring access to outside resources for information, specifically knowledge from industry experts. Fortunately, in this thesis experts as interviewees were accessible and provided a lot of knowledge in terms of the inner-workings of a ship. However, as stressed several times in the thesis, the number of ships, shipping operators etc is huge and widespread conclusions are hard to come by in such a diversified yet seemingly homogeneous field. The knowledge is distributed and requires resolve from the seeker of knowledge.

First of all, the attacks created in Chapter 7 provide as an excellent starting point for a risk assessment. However, the attacks should be fitted and modified depending on the actual ship. Moreover, duplication of systems, for example ECDIS, or sensors were also not included and mainly for these reasons the attacks should be adapted to concrete cases. The attacks are based on several assumptions and it was difficult to validate those assumptions mainly due to time limitations, for example the number of systems are most likely incomplete. Another facet of the attacks is that the actual network configurations might differ, they largely assume that best practice or at least some kind of network segregation exists. However, the issue of network segregation remains completely to be solved as some conflicting information was gathered. Although the topic of network segregation was not thoroughly discussed in this thesis, one of the experts said that the situation seems to be pretty woeful in general. Definitely something that should be further investigated. Autonomous, remotely operated or self-operating, ships should also be considered in future work as in the case of autonomous ships OT and IT systems are extremely interconnected whereas in this thesis they were mostly separated. The increased interconnection between IT and OT would mean that additional scenarios could be developed. Moreover, during the interviews some experts expressed their concerns about the application of autonomous ships and it is possible that an autonomous ship could be used as an attack vector against a so-called normal ship.

The created scenarios are most likely not complete but the author tried its best to include

every possible scenario by trying to include as much literature as possible and gathering input from industry experts. However, the limited number and homogeneity of experts are a limiting factor in the applicability of the attacks. The authored tried to make them as general as possible but they are best suited for passenger and cargo ships. They still can be applied to other ship types like cruise ships but for a complete picture experts from other ship types should be included and the scenarios enhanced with additional systems and attack surfaces, for example entertainment or cabin management systems. Moreover, widening the pool of experts would give an increased overview of the operational side of a ship whose importance can not be understated. As stressed several times during this thesis, experts are an invaluable source of information in creating potential attack scenarios due to the fact that existing literature is scarce and the knowledge base is extremely distributed. There is a reason why achieving the status of captain can take decades.

In terms of potential threat actors, a successful attack requires comprehensive knowledge about the inner-workings of the target ship and the opinion of the author is that this immediately disqualifies low-level skilled actors. The sheer number of different variables and factors that must be taken into account and planned for is humongous. Obviously they might try but the risk-to-reward ratio is high and they are better of focusing on other targets. The high risk-to-reward ratio and the lack of easily accessible knowledge, especially inner-workings of the ship and OT setup, realistically mean that state sponsored actors have the motivation, means and protection to execute the proposed goals. Lesser actors might be interested in the lower levels of the proposed attacks as in such circumstances it is easier to extract monetary gain due to the decreased complexity and ultimately lesser danger to human lives which might help the actors attract less attention. An example would be pirates using GPS spoofing or some kind of communication interference that could decrease response of the target ship. It is the author's opinion that techniques like usage of modified ECDIS charts should be out of their skill range and set of tools. Even with careful planning and vast resources, the attacks might not be possible due to the huge part of human factor that the attacks rely on, especially if the ultimate goal is capsizing the ship. Some examples range from procedures about physical security or cyber hygiene to effectively ignoring potential warning signs about a possible attack or malfunctioning and not enacting countermeasures in response.

The multivocal systematic literature review conducted in this thesis was a first for the author and could be improved greatly with a second iteration but as with many things in this thesis, time constraints are extremely limiting. However, even though there are existing literature that gather data of past events, for example [5], or other types of data gathering, the SLR was a first and can provide to be a valuable stepping stone for anyone interested in maritime cyber security. In hindsight, at the time of conducting the SLR, the

authors background knowledge was lacking a bit and may have caused the so-called "SLR net" being cast too thin which could be improved with an improved search query.

9. Summary

The primary goal of this thesis was to identify potential cyber based attack scenarios against a ship, a goal which was achieved using systematic methodology. Firstly, a Multivocal Systematic Literature Review was conducted to identify possible scenarios, vulnerabilities and exploits that could be used against a ship. From an initial pool of 497 papers, only 28 papers remained after applying criteria of the SLR in Section 5.2. Using the 28 papers a total of 46 scenarios, vulnerabilities and exploits were identified and classified. Alongside the SLR, the first phase of expert interviews was also initiated to gather operational and other background information related to the field of maritime helping to gap certain information shortages from existing academic and grey literature. In addition, it was helpful for the author to conceptualize knowledge accumulated from the SLR. After finishing the first phase of interviews, the author was able to create initial attack scenarios in the form of attack trees using information from the interviews and SLR. A total of three ultimate goals were identified - crash ship, immobilize ship and capsize a ship. All of the created attack scenarios start from methods on how to get initial foothold in the ship to initiate the attacks and end at on how to create the conditions as an attacker to achieve one of the goals. Finally, the created scenarios were presented to experts in order to gain their opinion and feedback in the second phase of interviews. Based on the feedback, the scenarios were improved and concluded. In total, 17 different high-level scenarios were identified for achieving the 3 goals.

The finalized scenarios are a great starting point for a risk-assessment but would need some tailoring to specific cases and additional enhancements. Moreover, this thesis did not deal with assessing the probability and impact of the attacks even though some aspects of likelihood were discussed based on the second phase of interviews. Although the scenarios most likely are not complete in terms of identifying every possible scenario, the author gave its all to ensure the inclusion of as many different scenarios as possible. In addition, potential threat actors were identified that could also be used as an input for a risk-assessment.

Primarily state sponsored actors would be the only one's interested and would have the means to conduct the attacks. The most limiting factors are the huge amount of resources required and the low possibility of extracting monetary gains. However, there is still the

argument that even in the case of motivation, opportunity and means the attacks would still be extremely difficult to execute due to the air-gapped nature of operational technology and requirement of knowledge about both technological and operational side of the target ship. As one of the experts pointed out, greater damage could be achieved by focusing on other targets with less resources that is required to successfully cause any meaningful harm to a ship.

Bibliography

[1] *Review of Maritime Transport 2018*. 2018. URL: https://unctad.org/en/PublicationsLibrary/rmt2018_en.pdf.

[2] Jordan Novet. *Shipping company Maersk says June cyberattack could cost it up to $300 million*. Aug. 2017. URL: https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html.

[3] O. Dinu and A.M. Ilie. "Maritime vessel obsolescence, life cycle cost and design service life". In: vol. 95. 1. cited By 11. 2015. DOI: 10.1088/1757-899X/95/1/012067. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84960351690&doi=10.1088%2f1757-899X%2f95%2f1%2f012067&partnerID=40&md5=15a4d5d684194e6ac48b16d7aec373e0.

[4] *MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS*. 2017. URL: http://www.imo.org/en/OurWork/Security/WestAfrica/Documents/Resolution%20MSC.428%2898%29%20-%20Maritime%20Cyber%20Risk%20Management%20in%20Safety%20Management%20Systems.pdf.

[5] M.S. Kaleem Awan and M.A.A. Ghamdi. "Understanding the vulnerabilities in digital components of an integrated bridge system (IBS)". In: *Journal of Marine Science and Engineering* 7.10 (2019). cited By 1. DOI: 10.3390/jmse7100350. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85074471348&doi=10.3390%2fjmse7100350&partnerID=40&md5=c9c206113be10ef9109317fdebde6f43.

[6] Bartlomiej Hyra. *Analyzing the Attack Surface of Ships*. 2019. URL: https://backend.orbit.dtu.dk/ws/portalfiles/portal/200738854/190401_Analyzing_the_Attack_Surface_of_Ships.pdf.

[7] K. Tam and K. Jones. "Cyber-Risk Assessment for Autonomous Ships". In: cited By 5. 2018. DOI: 10.1109/CyberSecPODS.2018.8560690. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85060497384&doi=10.1109%2fCyberSecPODS.2018.8560690&partnerID=40&md5=f2a9abd5e533ef2c0b73ac09b07c5602.

[8] Kimberly Tam and Kevin Jones. “MaCRA: A model-based framework for maritime cyber-risk assessment”. In: *WMU Journal of Maritime Affairs* 18.1 (2019), pp. 129–163.

[9] B. Svilicic et al. “A study on cyber security threats in a shipboard integrated navigational system”. In: *Journal of Marine Science and Engineering* 7.10 (2019). cited By 0. DOI: 10.3390/jmse7100364. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85074493968&doi=10.3390%2fjmse7100364&partnerID=40&md5=775e43c1c930905460e800012a91d73d.

[10] Kimberly Tam, Kevin Jones, and Maria Papadaki. “Threats and Impacts in Maritime Cyber Security”. In: *Engineering Technology Reference* 1 (Jan. 2012). DOI: 10.1049/etr.2015.0123.

[11] B. Svilicic et al. “Maritime Cyber Risk Management: An Experimental Ship Assessment”. In: *Journal of Navigation* 72.5 (2019). cited By 6, pp. 1108–1120. DOI: 10.1017/S0373463318001157. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85061241605&doi=10.1017%2fS0373463318001157&partnerID=40&md5=111c1fad9b7c375fde8b3d820574c0

[12] B. Svilicic et al. “Raising awareness on cyber security of ecdis”. In: *TransNav* 13.1 (2019). cited By 3, pp. 231–236. DOI: 10.12716/1001.13.01.24. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85068104756&doi=10.12716%2f1001.13.01.24&partnerID=40&md5=ac8fe110fb6a096041e859df4b0bb516.

[13] B. Svilicic et al. “Assessing ship cyber risks: a framework and case study of ECDIS security”. In: *WMU Journal of Maritime Affairs* 18.3 (2019). cited By 2, pp. 509–520. DOI: 10.1007/s13437-019-00183-x. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85074517102&doi=10.1007%2fs13437-019-00183-x&partnerID=40&md5=36418211e7170b4e0157bc4032fe2aa2.

[14] M.S. Lund et al. “Integrity of integrated navigation systems”. In: cited By 1. 2018. DOI: 10.1109/CNS.2018.8433151. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85052567868&doi=10.1109%2fCNS.2018.8433151&partnerID=40&md5=e3f46e36d8047d0f2a38b1d256ee6c3f.

[15] Marco Balduzzi, Alessandro Pasta, and Kyle Wilhoit. “A Security Evaluation of AIS Automated Identification System”. In: *Proceedings of the 30th Annual Computer Security Applications Conference*. ACSAC ’14. New Orleans, Louisiana, USA: Association for Computing Machinery, 2014, pp. 436–445. ISBN: 9781450330053.

DOI: 10.1145/2664243.2664257. URL: https://doi.org/10.1145/2664243.2664257.

[16] I. Botunac and M. Gržan. "Analysis of software threats to the automatic identification system". In: *Brodogradnja* 68.1 (2017). cited By 3, pp. 97–105. DOI: 10.21278/brod68106. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85032445051&doi=10.21278%2fbrod68106&partnerID=40&md5=53f13b22a0b222d11ec9edcc20e39c2d.

[17] MITRE. *attackics*. URL: https://collaborate.mitre.org/attackics/index.php/Main_Page.

[18] Harjinder Singh Lallie, Kurt Debattista, and Jay Bal. "A review of attack graph and attack tree visual syntax in cyber security". In: *Computer Science Review* 35 (2020), p. 100219. ISSN: 1574-0137. DOI: https://doi.org/10.1016/j.cosrev.2019.100219. URL: http://www.sciencedirect.com/science/article/pii/S1574013719300772.

[19] *ElectronicCharts Electronic Nautical Charts (ENC) and Electronic Chart Display and Information Systems (ECDIS) //*. URL: http://www.imo.org/en/OurWork/Safety/Navigation/Pages/ElectronicCharts.aspx.

[20] J. Direnzo, D.A. Goward, and F.S. Roberts. "The little-known challenge of maritime cyber security". In: cited By 6. 2016. DOI: 10.1109/IISA.2015.7388071. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84963860040&doi=10.1109%2fIISA.2015.7388071&partnerID=40&md5=7f45a9ce0d87013f04b708ff2f22a91f.

[21] *ECDIS Mandatory*. URL: https://www.furuno.com/en/merchant/ecdis/carriage/.

[22] *BIMCO: The Guidelines on Cyber Security Onboard Ships*. URL: https://iumi.com/news/news/bimco-the-guidelines-on-cyber-security-onboard-ships.

[23] Chitu Okoli and Kira Schabram. "A guide to conducting a systematic literature review of information systems research". In: (2010).

[24] Vahid Garousi, Michael Felderer, and Mika V Mäntylä. "Guidelines for including grey literature and conducting multivocal literature reviews in software engineering". In: *Information and Software Technology* 106 (2019), pp. 101–121.

[25] *Reisiparvlaev Tiiu - Praamid.ee*. URL: https://www.praamid.ee/wp/tiiu/.

[26] Catalin Cimpanu. *Ships infected with ransomware, USB malware, worms*. Dec. 2018. URL: https://www.zdnet.com/article/ships-infected-with-ransomware-usb-malware-worms/.

[27] Nir Nissim, Ran Yahalom, and Yuval Elovici. "USB-based attacks". In: *Computers Security* 70 (2017), pp. 675–688. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2017.08.002. URL: http://www.sciencedirect.com/science/article/pii/S0167404817301578.

[28] D. Bothur, G. Zheng, and C. Valli. "A critical analysis of security vulnerabilities and countermeasures in a smart ship system". In: cited By 0. 2017, pp. 81–87. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85072836951&partnerID=40&md5=0dd6a42d372ebb1fcb13beff31dd87c2.

[29] T. Becmeur et al. "A Platform for Raising Awareness on Cyber Security in a Maritime Context". In: cited By 0. 2018, pp. 103–108. DOI: 10.1109/CSCI.2017.17. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85060601318&doi=10.1109%2fCSCI.2017.17&partnerID=40&md5=227f46ce57ad506e43d4f19106c5d86e.

[30] A. Alop. "The main challenges and barriers to the successful "smart shipping"". In: *TransNav* 13.3 (2019). cited By 2, pp. 521–528. DOI: 10.12716/1001.13.03.05. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85073373757&doi=10.12716%2f1001.13.03.05&partnerID=40&md5=b7423061e0f355bc00c0fbdafe42427b.

[31] N. Anand. *Voyage Data Recorder of Prabhu Daya may have been tampered with*. July 2016. URL: https://www.thehindu.com/news/national/tamil-nadu/voyage-data-recorder-of-prabhu-daya-may-have-been-tampered-with/article2982183.ece.

[32] *Costa Concordia disaster*. URL: https://en.wikipedia.org/wiki/Costa_Concordia_disaster.

[33] C.W. Johnson. "Using assurance cases and Boolean logic driven Markov processes to formalise cyber Security concerns for safety-critical interaction with Global Navigation Satellite Systems". In: *Electronic Communications of the EASST* 45 (2011). cited By 5. DOI: 10.14279/tuj.eceasst.45.679.697. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84926001102&doi=10.14279%2ftuj.eceasst.45.679.697&partnerID=40&md5=5bf823585750c06954fedaea39d737c0.

[34] Joseph Trevithick. *New Type Of GPS Spoofing Attack In China Creates "Crop Circles" Of False Location Data*. Nov. 2019. URL: https://www.thedrive.com/the-war-zone/31092/new-type-of-gps-spoofing-attack-in-china-creates-crop-circles-of-false-location-data.

[35] Matthew Griffin. *World's first GPS Spoofing attack puts 20 ships 32km inland at an airport*. Mar. 2018. URL: https://www.311institute.com/worlds-first-gps-spoofing-attack-puts-20-ships-32km-inland-at-an-airport/.

[36] *Stena Impero GPS spoofing attack shows shipping is 'driving with eyes closed'*. Aug. 2019. URL: https://www.rivieramm.com/news-content-hub/news-content-hub/oems-must-improve-cyber-security-to-prevent-gps-spoofing-56044.

[37] H. Onishi, K. Yoshida, and T. Kato. "GNSS vulnerabilities and vehicle applications". In: cited By 2. 2017. DOI: 10.1109/WPNC.2016.7822853. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85015232798&doi=10.1109%2fWPNC.2016.7822853&partnerID=40&md5=214bd111764e90a4f32e0856d6c49db9.

[38] M.R. Manesh et al. "Detection of GPS Spoofing Attacks on Unmanned Aerial Systems". In: cited By 3. 2019. DOI: 10.1109/CCNC.2019.8651804. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85063457249&doi=10.1109%2fCCNC.2019.8651804&partnerID=40&md5=1c00c8ec07be69302c4bd650421e2f57.

[39] T. Omitola et al. "Securing navigation of unmanned maritime systems". In: vol. 2331. cited By 0. 2018, pp. 53–62. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85063299429&partnerID=40&md5=bc1131e2f6229b96af0d12eee356649f.

[40] J.A. Larcom and H. Liu. "Modeling and characterization of GPS spoofing". In: cited By 18. 2013, pp. 729–734. DOI: 10.1109/THS.2013.6699094. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-84893229341&doi=10.1109%2fTHS.2013.6699094&partnerID=40&md5=cc74413ceaaf9d15d0f08ded1cc9e79b.

[41] C.G.L. Krishna and R.R. Murphy. "A review on cybersecurity vulnerabilities for unmanned aerial vehicles". In: cited By 21. 2017, pp. 194–199. DOI: 10.1109/SSRR.2017.8088163. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85040251361&doi=10.1109%2fSSRR.2017.8088163&partnerID=40&md5=d012d190e45387a82d40564014123827.

[42] B. Silverajan, M. Ocak, and B. Nagel. “Cybersecurity Attacks and Defences for Unmanned Smart Ships”. In: cited By 1. 2018, pp. 15–20. DOI: 10.1109/Cybermatics_2018.2018.00037. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85067864061&doi=10.1109%2fCybermatics_2018.2018.00037&partnerID=40&md5=30f6fffc2ee0562801895d17aca1cbfb.

[43] “Iran Oil Tankers Said by Zanzibar to Signal Wrong Flag”. In: *Bloomberg* (Oct. 2012). URL: https://www.bloomberg.com/news/articles/2012-10-19/iranian-oil-tankers-said-by-zanzibar-to-be-signaling-wrong-flag.

[44] Department of The Treasury. *OFAC Advisory to the Maritime Petroleum Shipping Community*. Nov. 2018. URL: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/syria_shipping_advisory_11202018.pdf.

[45] Jeremy Wagstaff FBI. “Federal Bureau of Investigation (5/15/14) – All at Sea: Global Shipping Fleet Exposed to Hacking Threat, Wed, Apr 23 2014, By Jeremy Wagstaff”. In: (). URL: https://www.sfmx.org/wp-content/uploads/2017/03/Cyber-Security-Newsletter-2014-1.pdf.

[46] Martyn Wingrove. *Security flaws open ECDIS to cyber crime*. June 2018. URL: https://www.rivieramm.com/opinion/security-flaws-open-ecdis-to-cyber-crime-24334.

[47] “A low-cost solution to GPS vulnerabilities”. In: *BC Shipping News* (Sept. 2014), pp. 50–51. URL: https://rntfnd.org/wp-content/uploads/BC-Shipping-News.pdf.

[48] NCC Group. *Preparing for Cyber Battleships – Electronic Chart Display and Information System Security*. Mar. 2015. URL: https://www.nccgroup.trust/uk/our-research/preparing-for-cyber-battleships-electronic-chart-display-and-information-system-security/.

[49] Leo Kelion. *Ship hack ’risks chaos in English Channel’*. June 2018. URL: https://www.bbc.com/news/technology-44397872.

[50] J. Kelley. “From super-yachts to web isolation”. In: *Computer Fraud and Security* 2017.12 (2017). cited By 0, pp. 5–7. DOI: 10.1016/S1361-3723(17)30106-9. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85038082383&doi=10.1016%2fS1361-3723%2817%2930106-9&partnerID=40&md5=e6afa562b66bef9ef2aa071364d2270f.

[51] J.E. Vinnem and I.B. Utne. “Risk from cyberattacks on autonomous ships”. In: cited By 1. 2018, pp. 1485–1492. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85058130447&partnerID=40&md5=7aa3416ad709eace9aa3388614e13b53.

[52] United States Coast Guard. *Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels*. July 2019. URL: https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf.

[53] James Rundle. *Coast Guard Details February Cyberattack on Ship*. July 2019. URL: https://www.wsj.com/articles/coast-guard-details-february-cyberattack-on-ship-11564133401.

[54] Allan E. Jordan. *Tests Show Ease of Hacking ECDIS, Radar and Machinery*. Dec. 2017. URL: https://www.maritime-executive.com/article/tests-show-ease-of-hacking-ecdis-radar-and-machinery.

[55] *More than 200,000 vessels sail exposed to cyber-attacks, This should be a wake-up call to the shipping industry.* URL: https://navaldome.com/threat.html.

[56] *White Paper on VDR Cyber Security*. Aug. 2016. URL: https://www.danelec-marine.com/wp-content/uploads/2017/02/Danelec_Cyber-Security-whitepaper-160216-web.pdf.

[57] *Secure Your ECDIS - Prevent a Cyber Attack*. July 2018. URL: http://preventionatsea.com/sites/default/files/2018-07/DCP-Circular%2007-2018%20-%20SECURE%20YOUR%20ECDIS%20%E2%80%93%20PREVENT%20A%20CYBER%20ATTACK!.pdf.

[58] O.S. Hareide et al. “Enhancing Navigator Competence by Demonstrating Maritime Cyber Security”. In: *Journal of Navigation* 71.5 (2018). cited By 9, pp. 1025–1039. DOI: 10.1017/S0373463318000164. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85046093901&doi=10.1017%2fS0373463318000164&partnerID=40&md5=79bdc0753fdc715347b1d237b

[59] In: URL: https://ti.arc.nasa.gov/m/profile/adegani/Grounding%20of%20the%20Royal%20Majesty.pdf.

[60] Ken Munro. *Crashing ships by hacking NMEA sentences*. Mar. 2018. URL: https://www.pentestpartners.com/security-blog/crashing-ships-by-hacking-nmea-sentences/.

[61] R. Hopcraft and K.M. Martin. “Effective maritime cybersecurity regulation–the case for a cyber code”. In: *Journal of the Indian Ocean Region* 14.3 (2018). cited By 0, pp. 354–366. DOI: 10.1080/19480881.2018.1519056. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85053418444&doi=10.1080%2f19480881.2018.1519056&partnerID=40&md5=4d449c7cc961b76f9c1e44c054fc5145.

[62] L.R. Shapiro et al. “Trojan horse risks in the maritime transportation systems sector”. In: *Journal of Transportation Security* 11.3-4 (2018). cited By 1, pp. 65–83. DOI: 10.1007/s12198-018-0191-3. URL: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85046536379&doi=10.1007%2fs12198-018-0191-3&partnerID=40&md5=d8c1e5efd3328f218de1fb7c306c1b22.

[63] *ACCIDENT REPORT: Ship damaged due to incorrect ECDIS use*. Oct. 2017. URL: https://www.rivieramm.com/news-content-hub/news-content-hub/accident-report-ship-damaged-due-to-incorrect-ecdis-use-26796.

[64] *Ovit: Moody Crew, Dodgy ECDIS, Inexperience And A Shy Master*. Nov. 2014. URL: http://maritimeaccident.org/2014/11/ovit-moody-crew-dodgy-ecdis-inexperience-and-a-shy-master/.

[65] Maritime Accidents. *CSL Thames Grounding: Not Enough ECDIS Training*. Mar. 2012. URL: http://maritimeaccident.org/2012/03/csl-thames-grounding-not-enough-ecdis-training/.

[66] *NAVTEX problems in more detail*. URL: http://weather.mailasail.com/Franks-Weather/Navtex-Reception-Problems-And-Cures-Detailed.

[67] Tech. rep. URL: https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf.

[68] Ken Munro. *Sinking a ship and hiding the evidence*. Feb. 2019. URL: https://www.pentestpartners.com/security-blog/sinking-a-ship-and-hiding-the-evidence/.

Appendix A. Systematic Literature Review Data

#	Area	Class	Tactic	Precondition	Goal	Summary	Source
1	HA	V	Inhibit Response Function (Loss of View)	Alarms are created in the ship	Create confusion and increase workload of crew suddenly	Even with prior notice of the coming situation, crews might be overwhelmed by the amount of sudden work in the case of an attack (alarms etc)	[33]
2	N	V	Impact (Loss of Safety)	Usage of GNSS	Override GNSS signal	First generation GNSS provides little authentication and makes it possible to spoof location information. Russia is known to be conducting such attacks for several years, for example in 2017, ships in the Black Sea reported that their GPS showed them to be 32 kilometres inland [34, 35]. Iranians used GPS spoofing to lure a British ship into Iranian waters to seize it [36]. In 2019, researchers discovered a new attack against GPS where the Chinese in Shanghai spoofed multiple ships into a circular shape; something that is considered basically magic [34].	[33, 37, 38]

3	N	E	Impact (Loss of View)	Ability to capture and perfectly resend real broadcast signal; gradually replace authentic signal with signal with attacker's.	Override authentic GPS signal and send malicious data	Also called meaconing [39] Ability to lock the target's receiver to the attackers forged signal; Also see [40] chapter "Related Work" and additional examples presented by Murphy and Krishna [41] from the world of aviation.	[40, 41, 39, 42, 38]
4	C	V	Impact (Loss of Safety)	Access and control to an AIS transmitter	Spoofing a ship	Creating a fictitious ship with data (name, flag, identifiers, ship type, payload type, position, course, speed, destination). This has also been done intentionally by Iranian and Russian ships to avoid sanctions or other repercussions [43, 44].	[15, 16, 42]
5	N	V	Impact (Loss of Safety)	Access and control to an AIS transmitter	Spoof aids-to-navigation	Spoofing certain landmarks, threats to a ship (shipwrecks, shorelines, buoys) forcing the crew to take evasive maneuvers	[15]
6	N	S	Impact (Loss of Safety)	Ability to spoof AIS signal	Spoof an AIS signal so that the target vessel is on a course to collide with the spoofed ship	Spoof a ship in a way that the target vessel's system thinks that the two ships are on a collision course. This can result in automatic corrections by the target or alarms raised, depending on the configuration.	[15]

7	N	S	Impact (Loss of Safety)	Ability to spoof AIS signal	Generate fake distress signal and lure target into attacker controlled area	AIS transponders must generate an alert message when a distress signal is received. The attacker lures the target into hostile waters.	[15]
8	N	V	Impact (Manipulation of Control)	Ability to spoof AIS signal	Taking over the AIS signal broadcast by the target	Attacker overrides the target's AIS signal using a higher powered signal making it possible to alter the data etc.	[15, 7]
9	N	E	Impact (Loss of Safety)	Ability to impersonate maritime authority	Stop communication of all stations within communication coverage	By impersonation a maritime authority, it is possible to reserve the entire AIS transmission address space that will prevent all AIS stations from communicating with each other. Basically large scale disabling of AIS systems.	[15]
10	N	V	Impact (Loss of Safety)	Impersonation of maritime authority	Forcing AIS systems to change frequencies of operation	By impersonation a maritime authority, the attacker can force AIS transponder to switch frequencies of operation. Due to the protocol specification it is persistent even after rebooting the system. It is also possible to introduce geographical triggers when a target enters a specific area, the target is forced to use a different frequency practically making the AIS of the target useless.	[15]

11	N	V	Impact (Loss of Safety)	Ability to transmit AIS signal	Disabling a target's AIS communication	Attacker transmits a signal to an AIS transponder to delay its communication. Repeatedly transmitting this signal will practically eliminate all AIS related communications of the target.	[15]
12	N	S	Impact (Loss of Safety)	Access to ECDIS on ship or on shore	Modify ECDIS charts	Accessing the ECDIS to insert malicious charts. This process can happen on shore while transferring the maps to a ship or editing in the system itself. In some scenarios it would be possible to trap the vessel with a specifically designed chart i.e. removing shallow areas and making the ship run ashore. There is a practical example of this, albeit an unintentional mistake made by the issuer, when a minesweeper was grounded near the Philippines in 2013 [45]. Additional examples can be found from [5] where they gathered info about historical incidents	[20, 29, 10]

13	N	S	Impact (Loss of Safety/-Manipulation of View)	Access to ECDIS	Gaining access to ECDIS and services connected to ECDIS	Weak security measures might mean the possibility of gaining access via USB or through the download from the internet (charts). In addition, it would be possible to modify data in the ECDIS and interact with systems connected to ECDIS. Security researchers found that multiple models of ECDIS were extremely vulnerable even if the underlying OS was up-to-date and found that anti-virus software was useful in some scenarios but was largely ineffective against high-skill level attacks. Moreover they could reconfigure the ECDIS and pass malicious data.	[20, 46]
14	N	V	Initial access (Replication Through Removable Media)	Usage of main ECDIS and backup of ECDIS	Exploit both main and backup ECDIS	Researchers in 2019 conducted vulnerability scanning for 6 different ECDISs and found tens of vulnerabilities in each of the different variants. IMO also requires to have backup option for the main ECDIS but the researchers also found that most of the times the main and backup systems are identical in terms of configuration etc. This means that if the attacker is able to infect one, infecting the other one adds no additional complexity.	[12]

15	N	V	Impact (Loss of Availability)	GPS dependant systems and ability to conduct GPS jamming	Cause failure in AIS, gyro calibration system, digital selective system, the dynamic positioning system and ECDIS	A lot of different systems depend on GPS and its data thus jamming it might deprive those systems of crucial input causing them to stop functioning. For example, the ECDIS was screen in the bridge just remained static. The situation is even more dangerous considering that majority do not have an alternative positioning tool to GPS [47].	[20, 7, 47]
16	O	V	Initial access (Engineering Workstation Compromise)	ICSs from different vendors	Different systems bolted together to make them work	ICSs where security comes second after making things work provide fertile ground for attackers. ICSs are responsible for numerous thing thus vulnerabilities might have far reaching consequences. ICSs control and monitor parameters on board, including temperature, pressure, level, viscosity, flow control, speed, torque, voltage, current, machinery and equipment status.	[28]

17	O/N	V	Initial Access(Engineering Workstation Compromise)	Access to ECDIS machine	Vulnerable underlying operating system of ECDIS	Since ECDIS is not a separate machine but runs on a computer, security largely depends on the underlying operating system. Since Windows 7 is very largely still in use and often a lot of systems run on legacy computers (5 years ago a cyber security firm NCC Group released a report that most of the ECDIS machines run on Windows XP [48]), gaining access could provide to be simple due to the known number of vulnerabilities and support being low. Moreover, researchers scanned an air-gapped ECDIS configuration on a training ship and found 14 vulnerabilities of which half were critical but most of the critical vulnerabilities were related to remote services [11].	[28, 12, 11]

18	C	V	Discovery (I/O module discovery)	Access to internet	Discover VSAT device information	VSAT related hardware information can easily be found on the internet via different trackers. Moreover, default configuration is is usually uploaded to the internet by the manufacturer. Combine that with setups with default configuration (many terminals run in this way), attacking such devices could provide to be easy. This attack vector was demonstrated by an independent security researcher from France [49]	[28]
19	C	V	Initial access (Wireless compromise)	Ability to send VSAT signals	Send malicious data to the ship	In 2014 multiple VSAT interfaces were tested from different vendors and all of them were in some way vulnerable, either faults in the protocol or implementation level. Basic security mishaps were found such as plain text transfer without authentication, encryption or integrity checks [28]. Via a open VSAT it is possible to change GPS coordinates, settings and upload malicious software [28]	[28]
20	N	V	Impact (Loss of Safety)	Access to GPS jammer	Jam GNSS signal	Since GNSS signal power is extremely low (Wi-Fi is about 300 trillion times stronger), it it should be easy to use a jammer to disable GNSS and GNSS based systems on the ship.	[37]

21	N	S	Initial access (Spearphishing attachment)	None	Attack systems connected to the vessel's network that are not internet connected.	Obtain access to vessel's network and from there start lateral/vertical movement to cause damage. Whether by luring a user on the network to download malware or by tailing the vessels and being in the range of the wireless network.	[50]
22	O	V	Initial access (External remote Services)	Outsourced security critical systems	Access vessel using remote services	Statoil (Circle-K) outsourced some of their systems to a subcontractor in India and the technicians there accessed systems that they should not have several times, some of the systems were extremely critical of nature. Depending on the vessel, it could be possible to infiltrate an onshore system that has communication with the vessel and then move on from there.	[51]

23	O/N	S	Initial access (Supply Chain Compromise)	Ability to interfere with the supply chain of updates/-configurations	Inject malicious code to ICSs in the ship	Considering that most systems on a ship should be air-gapped [22], most updates whether to ECDIS or any other systems are usually done using removable media[12]. It would be possible to inject malicious code to updates if the attacker was able to interfere with the supply chain for updates. An incident report by the U.S. Coast Guard revealed that one cyber attack victim ship did not have cyber security policies in place and removable media used to update ECDIS was routinely not scanned for malware[52, 53]. In another example, an unscanned USB was inserted to a ship's system that was in dry docks and caused damages of hundreds of thousand of dollars due to delaying the deployment of the ship [26]. Further example is from an incident were a technician infected a power management system of a ship via USB that was trying to connect to the internet but luckily the IT department decided to scan the system before connecting the management system to the internet for data collection and updates [26]. A security company demonstrated that they were able to take control of Machinery Control System of a ship via infected USB stick, they were able to control auxiliary systems, such as ballast, generators, fuel system, all the while the displays were perfectly normal [54, 55].	[42, 14]

24	C/N	V	Initial Access (Internet Accessible Device)	Integrated Navigation System that receives updates from the Internet	Exploit the INS	Some vendor of INSs have the possibility of updating their systems, such as ECDIS, directly through the internet. Moreover the underlying operating systems tend to be Windows 7 or older, providing excellent opportunities for attackers to compromise it. In addition, in some cases it is possible to access VDR remotely [56].	[14]
25	N	S	Impact (Manipulation of Control)	Access to a switch in the network of INS	Send malicious data to the network	Researches demonstrated that they were able to send fake GPS coordinates to the network and the INS was unable to distinguish between valid and malicious data. The researchers achieved this by connecting a Raspberry Pi to the network. Moreover, they were able to override the actual sensor data so that the workstations only received malicious data. A security company used access to a local ethernet switch to take control of the ship's radar; they managed to remove objects from the radar screen used in the bridge effectively making the ship blind [54, 55].	[14]

26	N	S	Impact (Manipulation of Control)	Physical access to the INS	Read and alter INS data	Researchers infected an INS workstation by inserting a USB device that pretended to be a mouse and keyboard and installed malware. The USB device logs out of the ECDIS software and then enters the underlying operating system. After entering the OS, the malware is deployed and the computer infected. From there the malware will act as a man-in-the-middle resulting in the ability of reading and altering data between sensors and ECDIS. In terms of Command and Control, the researchers programmed the malware to start altering data after the ship crossed a certain geographical boundary (GPS line/data). During a inspection of tanker in Cyprus, it was found that a malware was feeding false sensor data to the ECDIS [57].	[14, 58]

27	N	S	Impact (Manipulation of Control)	Vessel in "track mode" **and** ability to manipulate input data of ECDIS	Force autopilot off the pre-planned route	Researchers demonstrated that by feeding ECDIS manipulated data the autopilot will automatically correct the course of the vessel to stay on the pre-planned route. However, as to the crew it looked like the ship was on the correct course, an attacker could use this to run the ship aground. There is an example from 1995 when a ship was grounded due to malfunctioning GPS signals (see more at [5] page 8) that caused the autopilot to take corrective action resulting in grounding the ship [59]. Another method for achieving the same goal would be to modify GPS NMEA sentences in the ship's GPS receiver or autopilot controller rather trivially since the sentences are plain text and have no authentication [60].	[58, 59]

28	O/HA	V	Evasion (Masquerading)	None	Confusion and lack of knowledge in dealing with systems or security related incidents	Since a humans need rest from work, it is beneficial to the employer to have different crews operate the ship for it to be used as effectively as possible. However, changing crew poses a risk when systems on a ship are operated by unfamiliar and inexperienced personnel. This can induce different protocol breaches or inadequate responses to security incidents. Moreover, the crew might have little knowledge of the systems that make a ship tick.	[61]
29	HA	V	Impact (Theft of Operational Information)	Knowledge of people working on the ship or people with knowledge of the inner-workings of a ship	Acquire inside, trojan horse, asset	Disgruntled employees or any other personnel that may have something against the company, country etc would provide to be a valuable asset. The asset can be useful in terms of knowledge or the attack. Disgruntled employees might help the attacker smuggle a malicious USB media to the bridge and infect critical computer systems. Quite frankly, the options are limitless (for more information read [62]).	[62]

30	O	V	Evasion (Indicator Removal on Host)	Access to VDR	Cover tracks	VDRs are analogous to airplane black boxes and collect data from several sources for reporting purposes. They have also shown to use weak encryption and other dangerous vulnerabilities that could make it possible for the attacker to affect integrity of data. In India the VDR's files were overwritten after the crew inserted an memory drive into it [31]	[7]
31	O	S	Impair Process Control (Change program state)	Access to automata (ICS, SCADA) network	Stop automata functioning	A specially crafted TCP packet is sent to the automata network that tells the automata to stop loop of the automation. This would cause the interface to become unfunctional and unresponsive, even when operated directly from the hardware buttons. In such cases the automation must be restarted and debugging such an incident is complex in a diverse system that a ship is. The correct SCADA must be located etc and during high-stress situations other circumstances may apply and worsen the response. However, this was done in a low cost simulated environment that the authors say was quite accurate to the actual design of a ship it is hard to say if this is actually possible considering the vulnerability part of this scenario.	[29]

32	O	S	Impair Process Control (Change program state)	Ability to write data directly to the memory of the automaton.	Override authentic commands	The researchers in their simulated environment wrote data directly to the memory allowing them to take control of the automaton. This enabled them to ignore commands, feed invalid data to the operator and inhibit response.	[29]
33	HA	S	Impact (Denial of View)	Overreliance on interface data and ability to modify interface data	Cause damage to physical systems	The attacker is able to modify data in terms of operator input and data shown to the operator that causes (overreliance) the operator to introduce a situation where some sort of physical system is pushed to its breaking point, may cause the physical system to malfunction or break, for example the engine. This attack can be combined with the one above this to destroy the transmission axis and kill the engine in a complex attack. Moreover, overreliance on interface data in dangerous conditions such as heavy fog may lead to severe consequences. A security company demonstrated this attack by manipulating 4 important parameters of the ship - position, heading, depth and speed; they also conducted the attack in the middle of the night and while the ship was travelling through a narrow canal for maximum effect [54, 55].	[29, 30]

34	O	V	Discovery (Control Device Identification)	Outdated equipment	Vulnerable equipment	In a cyber risk assessment done on a training ship researchers found several critical vulnerabilities to some systems of the ship. Moreover, the ECDIS was using Windows XP for its operating system while still being compliant with the IMO [11]. In another assessment conducted on another ship by the same researchers they found services that are either no longer supported by the vendor (Apache web server) or ignore vendor recommendations to replace with a more secure service (SMB version 1)[13]. In addition, the ECDIS was running on Windows 7 Pro SP1. This means that when cyber security is ignored or is in the background, ship owners have no real incentive to upgrade systems as long as the ECDIS is functionally satisfactory. Furthermore, the researchers conducted another study and found the same SMB related vulnerability in another ship's ECDIS [9]. In the same research they found Remote Desktop Service running that is known to be vulnerable and provides remote access trivially to the attacker.	[11, 13, 9]

35	O	S	Inhibit Response Function (DoS)	Control over ship's computing power	Introduce computing load that will overwhelm the system and make it unresponsive or at least slower.	Consider the scenario of the ship's systems being compromised and the attacker has almost full access to the systems, for example the ECDIS. An attacker might introduce complex mathematical computations to render the system unusable while still maintaining enough level of access to conduct the attack. In such a case it might take a while to notice the true intentions behind the attack.	[30]
36	O	V	Execution (Change Program State)	Enabled, vulnerable and redundant software	Exploit vulnerable services	In a cyber risk assessment of a ship, researchers found an outdated and unused service (SMB v1) that was vulnerable in the underlying OS of the ECDIS. In the case that the ECDIS is configured incorrectly (enabled redundant services), crew or IT personnel, unless strict audit techniques/rules are in place, might not notice the service being enabled potentially lengthening the vulnerable period and providing amble opportunity for the attacker to exploit it.	[13]

37	HA	S	Inhibit Response Function (Utilize Operating Mode)	Irresponsible operator	Operators ignoring procedures	In 2016 a carrier named Muros was grounded due to incorrect and poor usage of the ECDIS [63]. Another example is when a Maltese tanker ran aground due to ECDIS alarm output being not configured, the training given to the crew was affected by the pride of the captain (he was embarrassed, due to cultural background, to ask questions in front of junior officers) resulting in him having insufficient skills and relying on junior officers who also suffered from the same fault [64]. A third example is from another Maltese ship that ran aground due to misconfiguration of the ECDIS (sound alarms were not configured), lack of general knowledge of the ECDIS system and "... lack of support for an inexperienced third officer ..." [65].	[63, 64, 65]
38	C	V	Impact (Loss of View)	Usage of NAVTEX	Disabling of NAVTEX	NAVTEX is intended for navigational aid by providing weather and navigational warnings. NAVTEX has sometimes been affected by high and low water with signals not being received during low water. In addition, other sources of radio waves have known to heavily affect NAVTEX reception.	[66]

39	C	V	Impact (Loss of View)	GMDSS usage	Infect GMDSS	A technical report discovered that the Global Maritime Distress and Safety system is vulnerable to cyber-attacks that could possibly enable the attacker to control onboard devices, affect data integrity and availability of communications.	[67]
40	C	V	Impair response function (Alarm Suppression)	Vulnerable SSAS	Modify SSAS alerts	SSAS is used for sending security/emergency alerts to relevant authorities during times of distress. If the system is compromised, the attacker could modify or altogether delete the messages. Data that could be affected are weather warnings, distress calls and even "receiving" fake weather information to force the ship to alter its course.	[67]
41	HA	V	Discovery (Control Device Identification)	Unaware people	Source information about systems from social media	A passenger uploaded detailed information about the vessel's safety measures to Facebook. The breach was corrected after discovery.	[5]

42	C	V	Initial access (Exploit public-facing application)	Vulnerable satellite communication terminal	Take control of communication systems	A technical white paper found that some satellite user terminal are vulnerable and via a specially crafted SMS the attacker is able to assume control of the terminal. From that point the attacker could install malicious firmware and control the communication system.	[67]
43	C	S	Impair Process Control (Rogue Master Device)	Ability to smuggle malicious hardware aboard a ship	Interfere with the communications of a ship	The idea is for the attacker to obtain equipment and transport them to the target ship to disrupt the communications of a ship. Smuggling can be achieved by various means using a cyber attack - "... altering invoices, control cargo loading machinery, or by infecting port software using social engineering". For a greater effect, the attacker might execute the attack when the ship is at sea.	[10]

44	C/N/P	S	Impact (Denial of Control)	Unsecured network connection to the ship	Control or Encrypt critical systems of a ship	If the attacker had access to the ship, it would theoretically be possible to encrypt (ransomware) the digital systems that are used to control the ship, disabling control of the ship. Moreover, the attacker could control the ship's navigation and propulsion systems to run the ship ashore. However, ships tend to have back up systems but the attack could still create problems.	[10]
45	P/S	S	Impact (Loss of Safety)	Persistence in the ship's network	Capsize the ship	If the attacker has access to the ship's network it would be possible to locate and infect a serial to IP converter or a serial endpoint, from there it would be possible to send commands to ballast pump controllers that would cause the pumps to pump all of the ballast to one side of the ship, for example from port to starboard tanks. Moreover, modern solutions for ballast control systems usually offer remote monitoring and operation from the bridge. At the same time it could be possible to modify NMEA messages to force the autopilot to turn in the same direction as the pumps worsening the effect. Finally, the attacker could modify the VDR to remove traces of the attack.	[68]

46	C	V	Collection (Automated collection)	Access to vessel's computer network	Listen in to communications and possibly modify	In 2018 researchers analyzed 22 Integrated Navigational Systems and found that only 9 of the analyzed systems had redundant or dual means of communications for sensor data. The existence of only one communication method lowers the difficulty of fully compromising the ship (eavesdropping, DoS or compromising integrity of data).	[14]

Table 3. *Results of the Systematic Literature Review*

Appendix B. Structured interviews material in Estonian

Esialgse ligipääsu saamine

Kuna laeva näol on tegemist täiesti eraldiseisva süsteemiga, on vajalik enamike rünnakute läbiviimiseks esialgset tugipunkti, millest rünnakut alustada. Selleks on kolm peamist viisi: rünnata välismaailmaga suhtlevat süsteemi (ECDIS/VSAT), saada füüsiline ligipääs rünnatavale süsteemile või rünnata laeva mõne vahepealse seadme, näiteks nakatada hoolduseks kasutatav arvuti. Siin peatükis on kirjeldatud üldist viisi, kuidas süsteemile X ligi saada, ning reaalne lähenemine sõltub süsteemi olemusest, näiteks kas süsteem suhtleb välismaailmaga.

Füüsilise ligipääsu all mõeldakse seda, et kas ründaja leiab mõne rahulolematu töötaja ja maksab talle või tasustab mingil viisil selle eest, et töötaja läheb rünnatava süsteemi, näiteks ECDIS, juurde ja ühendab ründaja poolt antud seadme rünnatava süsteemi külge. Teine variant oleks ründajal seda kõike ise teha, aga antud viis eeldaks, et ründaja teab kuhu minna ning võõras nägu jääb palju lihtsamini laevameeskonnale silma. Seade, mis kinnitatakse rünnatava süsteemi külge, on ründaja poolt loodud ja on võimeline pealt kuulama süsteemi sisemist info liikumist ning võimeline ka ise käske saatma rünnatud süsteemile või temaga ühendatud süsteemidele.

Nii öelda vahepealse seadme nakatamine peaks välja nägema nii, et ründaja peab välja selgitama hooldustööde tegija (firma, isik) ning nakatama tema seadme, mida kasutatakse hoolduseks (USB või arvuti). Ja siis ideeliselt hooldust tehes ühendab hooldaja oma seadme rünnatava süsteemi külge ning selle kaudu liigub kurivara edasi juba laeva süsteemidesse, kust on võimalik rünnakut jätkata. ECDISe puhul oleks ründajal võimalik saada ligipääs kaartide uuendusteks kasutatavale mälupulgale ning asetada mälupulgale kurivara.

Mõned ECDISe lahendused kasutavad interneti kaartide uuendusteks ja teoreetiliselt võiks olla võimalik kaartide faili sisse/külge ehitada kurivara (viirus) ning kui uus kaart laaditakse ECDISsse, siis käivitatakse ka kurivara, mis võimaldaks pahalasel kontrollida ECDISt ning sealt edasi liikuda. Lisaks on kirjanduses olemas näiteid, kuidas internetist (MarineTraffic)

leiti laeva VSAT seadete mudel ning selle põhjal leiti vaikeseadistus, mida omakorda kasutati andmete saatmiseks laeva ning lõpuks ka ründamiseks.

Küsimused:

- Kui tõenäoline oleks, et ründaja suudab ise laevale hiilida, pääseda süsteemi juurde, sisestada oma seade ning teha kõike seda märkamatult (ECDIS, PMS, Thrusterid/Põtkurid)?
- Kas teil tuleb pähe mõni teine viis kuidas mõnele süsteemile ligi saada? Mõni teine liides/koht, kust ründaja võib väljastpoolt ligi saada.
- Kuidas erineb laeva opereerimine sadamas vs merel? Kas on mõni ühendus laevas sisse lülitatud?
- Mis olukorras võõrast seadet võib märgata mõni meeskonnaliige? Kas hooldaja või laevatöötaja võib visuaalselt vaadates aru saada, et mõne süsteemi küljes on võõras seade? Kas sellele üldse pööratakse tähelepanu?

Õnnetuse põhjustamine

Õnnetuse all mõeldakse seda, et laev sõidab karile või põrkab teise objektiga (laev, kivi jne) kokku. Sisuliselt peab ründaja mõjutama laeva trajektoori viisil, et hetkeks, mil meeskond märkab, pole võimalik enam õnnetust vältida.

Kujutame ette olukorda, kus laeva juhib autopiloot (tracking-mode) ning ründajal on võimekus muuta GPS andmeid. GPS andmeid muutes väikeste sammudega pika aja jooksul võib olla võimalik seada trajektoor mõne objekti suunas. Muutes GPS andmeid väikeste sammudega suurendab tõenäosust, et GPS andmete nihe ei ole nii silmatorkav meeskonnaliikmetele ning meeskonnale tunduks nagu kõik oleks korras. Lisades GPS andmete muutmisele laeva juhtiva isiku hajameelsuse ning ründaja kontrolli ECDISe üle (alarmid välja lülitatud), peaks tekkima olukord, kus on kokkupõrke trajektoor objektiga. Antud rünnaku õnnestumist saaks suurendada võltsitud ECDISe kaartide kasutamisega, näiteks eemaldatud mõni veepinna all olev suur kivi või väärad sügavused.

Teine stsenaarium oleks autopiloodi teekonna muutmine ründaja poolt. Eeldades, et ründajal on kontroll ECDISe üle, võiks ründaja inkrementaalselt muuta autopiloodile seatud teekonda nõnda, et tekib kokkupõrke trajektoor. Ka seda stsenaariumit saab kombineerida võltsitud kaartidega ning ECDISe alarmide väljalülitamisega suurendamaks rünnaku tõenäosust.

Kolmas stsenaarium on olukorras, kus laeva juhitakse manuaalselt ja ECDIS kasutab

ründaja poolt võltsitud kaarte. Kasutades koos eemaldatud objekte ning vääraid sügavusandmeid võib tekitada olukorra, kus laeva juhtiv inimene valib teekonna läbi kitsa kanali, mis reaaluses pole ohutu ning võib põhjustada kokkupõrke.

Neljas stsenaarium eeldab ründaja kontrolli rooli ja/või thrusterite üle. Antud stsenaarium töötaks koostöös ründaja etteplaneeritud ajastusega, kui kriitilisel hetkel saadab ründaja käsu thrusteritele, et pööra mingi objekti suunas. Lisaks käsu saatmisele ründaja saaks ignoreerida käske rooli küljest, mis tagaks võimetuse kontrollida thrustereid sillast. Thrustereid on võimalik avariirežiimis kontrollida, aga hea ajastus võib tähendada, et ajaliselt ei jõua meeskond reageerida ning lõpptulemuseks on kokkupõrge. Roolist/autopiloodist tulnud käskude ignoreerimist võib kasutada ka eelnevate stsenaariumite korral suurendamaks rünnakute õnnestumise tõenäosust.

Kõiki eelnevaid stsenaariumeid peaks kombineerima reaalolukorra ülevaate vähendamisega ründaja poolt. Ründaja piisava kontrolli puhul ning teatud ajahetkel võiks ründaja muuta reaalajas abistavate sensorite/süsteemide infot. Näiteks, kui rünnak kasutab võltsitud kaarte, siis peaks ründaja ka samal ajal muutma sügavussensoreid, radarit või ka AISi. Kõigele lisaks oleks võimalik ka muuta ECDIS kasutamatuks kas lunavara võtteid krüpteerides ECDISe tarkvaralised komponendid või jooksutada ECDISe arvutis programmi, mis kasutab kogu arvutusliku võimsuse ära ja ei jäta piisavalt ressursse ECDISe teenindamiseks.

Küsimused:

- Kui reaalne tundub neljas stsenaarium? Mõistagi oleneb laevast ja suunamuutmise võimest.
- Kas on midagi, mida ründaja saaks teha, et rünnaku õnnestumise tõenäosus sureneks?
- Kas on mõtteid mõne alternatiivse stsenaariumi kohta, mis samuti lõppeks kokkupõrkega?

Laeva kummuli keeramine

Laeva kummuli keeramiseks on minimaalselt vaja kontrolli ballastipumpade üle. Ideeliselt peaks ründaja suunama kogu ballasti ühele küljele nõnda, et laev läheb ühele poole kreeni. Antud kallet saaks ka võimendada saates käsu thrusteritele suunata laev ballastile vastassuunas. Omakorda, kui laeval on kasutusel rullumise vastane süsteem (Anti-Rolling System), saaks ründaja saata käsud rullumise vastasele süsteemile nõnda, et laev kalduks veelgi enam ballasti suunas. Kõike eelmainitud võiks ka veel kombineerida güroskoobi sensori andmetega - ründaja kasutab güroskoobi andmeid selgitamaks veekogu lainepikkust ning alustada rünnakut laineharja miinimumis/maksimumis, mis omakorda võimendaks

kreeniefekti ning lõppude lõpuks tähendaks laeva kummuli minekut.

Arvesse peab võtma ka seda, et kui ründaja saadab pahatahtlikke käske mõnele süsteemile, siis meeskonna reageerimise võimaluse vähendamiseks peaks ründajal olema võimekus tühistada nii-öelda autentseid käske meeskonna poolt.

Küsimused:

- Mis faktorid takistaks antud rünnaku õnnestumist? Mida peaks ründaja arvesse võtma?

Laeva immobiliseerimine

Laeva liikumisvõimetuks tegemiseks on kaks viisi: kaotada meeskonna poolne kontroll liikumiseks vajalikke süsteemide üle või tekitada süsteemides olukord, kus mõni mehaaniline komponent läheb katki.

Kontrolli kaotamiseks on omakorda kolm viisi: lükata välja kontrolliv automaatika, piirata meeskonna ülevaadet reaalolukorrast või krüpteerida laeva liikumiseks kasutatavad süsteemid. Kui ründaja suudab välja lükata automaatika, mis kontrollib PMSi või thrustereid, tekitaks omakorda olukorra, kus meeskonnal puudub täielik võimekus kontrollida laeva. Antud lähenemine otseselt ei immobiliseeriks laeva, aga kontrollimatu olukord on sama hea kui liikumatu laev eriti kui rünnak algatati tormises meres. Sarnane olukord tekib reaalolukorra ülevaate kaotamisel, sensorite andmete muutmine. Eriti tänapäevased laevad on mõeldud opereerimiseks võrdlemisi väikese meeskonna poolt ja kui IT-süsteemide töö on peatatud, siis laeva pole võimalik juhtida täismahus. Samuti saab sama olukorda tekitada ka lunavara tehnikaid kasutades - krüpteerides navigatsiooniga seotud süsteeme või krüpteerides automaatikat, mis kontrollib mehaanilisi komponente. Kõige juures tuleb arvesse võtta, et meeskonnas tihti puudub IT inimene või meeskonna üldised IT teadmised pole piisavad olukorraga tegelemaks ilma välise abita.

Mehaaniliste komponentide rikke esile kutsumiseks peab olema ründajal võimekus kontrollida antud mehaanilist komponenti ning kuna komponendid ei rikne kohe, siis peaks olema võimekus muuta sensorite andmeid, et meeskonnal poleks ülevaadet olukorrast. Teoreetiliselt peaks teatud aja möödudes mehaanilises komponendis tekkima rike ning olenevalt komponendi tähtsusest peaks ka laev immobiliseeritud olema, vähemalt mingil määral.

Küsimused:

- Mis mehaaniline komponent on kõige haavatavam? Millises mehaanilises komponendis võiks rikke esile kutsuda? Millised väiksemaid rikkeid on võimalik laevas koheselt ära parandada?
- Milline oleks meeskonna reaktsioon, kui avastatakse, et mingid mehaanilistes komponentides on rike tekkimas ning meeskonnal puudub kontroll tavapäraste kontrollmehhanismidega?
- Kuidas käitutakse laevas kui IT-põhised navigatsiooniabid ei tööta enam?
- Mis on peamised olukorrad, kui otsustatakse, et kutsuda puksiir või laeva ei saa enam juhtida?

Reaalaja olukorrast ülevaate kaotamine

Hetkeolukorrast ülevaate omamine on äärmiselt tähtis ning ründajal on teatud võtteid kasutades võimalik piirata ülevaadet, mis omakorda võib suurendada rünnaku õnnestumise tõenäosust ja ka tagajärgi.

Ründaja võiks oma kasuks ära kasutada erinevaid alarme, mida näidatakse meeskonnale. Olenevalt eesmärgist - kas valepositiivseid alarme luua või alarmide näitamist piirata. Valepositiivsete alarmide loomine võiks vähendada meeskonna enesekindlust IT-süsteemidesse ning käituda kui petterünnakuna ja juhtida meeskonna tähelepanu tegelikkust rünnakust eemale. Lisaks saaks alarme ka piirata sensorite tasandil, muutes andmeid nõnda, et need ei peegeldaks tegelikku olukorda või üldse sensorite andmed muuta kättesaamatuks. Viimasena oleks võimalik ründajal piisava planeerimise ja võimekusega ajastada rünnakuid tormidega ning üldiselt halva nähtavusega aegadel.

- Mis on reaalolukorrast ülevaate omamiseks peamised tööriistad?
- Mis süsteemide rikete korral otsustatakse peatada laeva normaaltöö?
- Kuidas erineb töö laeval hea ja halva ilma korral nii koormuse kui protseduuride poolest?

Üldised küsimused

- Kui teie mõtlete laeva õnnetusele, mis tüüpi õnnetusi te silmas peate? Kas tuleb pähe midagi, mida pole eelnevalt mainitud?
- Oletades, et ründajal on võimekus sensorite andmeid muuta viisil, et puhtalt sensorite andmeid vaadates pole võimalik eristada. Kuidas tavaolukorras avastatakse, et sensorite andmed ei vasta tegelikkusele?
- Kuidas laeva kontorivõrk ja laeva sisemine võrk on eraldatud? Kuidas laeva sisemises

võrgus on erinevate süsteemide võrgud eraldatud? Firewallid, VLANid? Mis juhtub kui pingida ühest seadmest teise võrku?

- Kas te olete nõus, et teie nimi avaldatakse selles lõputöös?