DEPARTMENT OF INFORMATICS

Master Thesis

Safety and security of autonomous vessels

Based on the Yara Birkeland project

Marte Hvarnes Evensen

Supervisors: Roar Sønstebø Simensen, Øyvind Ytrehus

May 5, 2020

Abstract

Yara Birkeland will be the world's first fully electric and autonomous container vessel with zero emission. It is being developed by Kongsberg and Yara. This is one of the autonomous projects ongoing in the maritime sector. Even though autonomy is a familiar theme to many people, it brings new challenges when being used in the maritime sector. How will the ships be designed when there is no need for a crew onboard? How will tasks normally performed by the crew be solved? How will the rules and regulations be applied? What are the safety and security issues? Unmanned vessels need to be equally safe and secure as conventional vessels, or even safer and more secure. In addition to the challenges, there are many positive sides for bringing autonomy into the maritime sector. Some examples are improved health of the crew, costs savings on crew facilities, and a new vessel design which can result in less air resistance, less fuel consumption, and a greener business. Studies have shown that many accidents at sea could have been avoided if the vessel was unmanned. Most importantly, the crew will no longer have to risk their lives in the dangerous environment.

When assets and information become available online, the criminals also enter the digital arena. Attacks can be used for a lot of things, like gaining access to information and money, spreading propaganda and fear, stopping a nations critical infrastructure, and affecting elections. The maritime sector was isolated at sea, but ships are now interconnected with many devices and the shore. The communication and devices used have cyber vulnerabilities. Vessels should be robust against safety and security incidents that could occur. Measures need to be in place to ensure the integrity, availability, and confidentiality of data. Cyber security is an important part of autonomy. If the cyber security of these autonomous entities is not seriously considered, the consequences can potentially be major. This thesis will look at some of the challenges *Yara Birkeland* will face when it comes to cyber security. It is written in collaboration with Kongsberg Maritime.

Acknowledgements

Firstly, I would like to thank my supervisor Øyvind Ytrehus for all the help, guidance, and support he has given me through my master's degree. Thank you for helping me complete this thesis even in these strange times. I would also like to thank Kongsberg Maritime for giving me the opportunity to gain insight into this exciting project. A special thank you to Roar Sønstebø Simensen for being my supervisor and to An-Magritt Tinlund Ryste for wanting me to write about the project – it would not have happened without you. I would also like to thank all the employees at Kongsberg Maritime who have gladly provided me help and insight.

I am grateful for all the wonderful people I have gotten to know during my time at the University in Bergen. My time at the Department of Informatics has been tough, challenging, educational, inspiring, memorable, and great. It is truly a special environment for students, both academically and socially.

Finally, I would like to thank my family for giving me the idea that I could write about *Yara Birkeland*, proofreading, and all the love and support they have given me.

Contents

1 Introduction 8
1.1 Motivation 8
1.2 Similar projects 9
1.3 Structure of thesis part 1 11
2 Background 12
2.1 The Yara Birkeland project 12
2.2 Shore Control Center 13
2.3 Cyber security 14
2.3.1 Vulnerability and threat 14
2.3.2 Helhetlig digital risikobilde 2019 14
2.3.3 Authentication 19
2.3.4 Attacks 20
2.3.5 Information security 23
2.3.6 Cryptography 24
3 Safety and security of ships 28
3.1 Safety and security 28
3.2 Vulnerabilities 30
3.3 Threat actors 36
3.4 Attacks 37
3.5 Cyber security work 39
4 Autonomous vessels 42
4.1 Autonomy 42
4.2 Remote controlled and autonomous vessels 43
4.3 Vessels 43
4.4 Safety and security of unmanned and autonomous vessels 46
References 47

List of tables

Table 1 Schematic structure of modified risk categorization (Fjelldal, 2018, s. 45) 29

List of figures

Figure 1 Illustration of Yara Birkeland (Andersen, 2019b) 12
Figure 2 Illustration of Yara Birkeland (Yara, u.å.) 12
Figure 3 What a ship looks like to an attacker (Pen Test Partners, u.å.) 31
Figure 4 Attacks against IT and OT the last decade (Fosen, 2019) 38

PART 1

Chapter 1

1 Introduction

1.1 Motivation

We have moved into an era called Industry 4.0, or the Fourth Industrial Revolution (Fjelldal, 2019). From the first industrial revolution where the production was made mechanical and equipment was powered by water and steam, to the second with mass production assembly lines requiring labor and electrical energy, the fourth will enhance the developments from the third industrial revolution which was automation of production using IT and electronics and adoption of computers (Marr, 2018). Industry 4.0 will use data and machine learning for smart and autonomous systems. The production becomes intelligent, the use of cloud technology, big data, cyber-physical systems, and Internet of Things (IoT) expands, and the need for cyber security is significant.

Autonomy is a widely discussed theme these days. We hear about autonomous cars, ships, airplanes, and other processes. Autonomous cars have already been launched and according to Kongsberg Maritime's plans it will not be long until the first autonomous ship is ready. We can without doubt state that ships have different challenges than cars and the maritime industry is known to slowly adapt to changes. How will they be able to adapt to the great changes that will happen in the near future when ships become unmanned and what kind of challenges are autonomous oceangoing vessels facing?

Many people find autonomy scary, but many things are in fact autonomous today. New cars can provide assistance with lane control and cruise control among others. Tesla cars even have auto pilot. These processes are autonomous. Take-off and landing of airplanes are often associated as being the most crucial processes during a flight – these are also autonomous. Many tasks on ships take advantage of this help as well, either it operates on its own or as aid for the crew. Maritime autonomy does not necessarily mean that it is a ship moving without the need of a crew on board. It means that the ship is capable of thinking and making decisions for itself. These decisions are based on received data and parameters defined. People associate motors, pumps, and design of vessels to the shipping industry, but not IT, communication, connectivity, and data. The goal is not to remove and take away jobs of humans. The development will require lots of new and existing jobs. People's health and safety, the environment, and economy are factors taken in consideration.

This development requires, among others, a number of interconnected devices and ICT systems. The consequences of a cyber-attack can now be physical. It has been demonstrated that it is possible to remotely take over the controls of a Jeep Cherokee. Two security researchers managed to do so from far away through the vehicle's Internet-connected entertainment system in 2015. A video shows the driver's terrified expression as he is driving on a highway, powerless while the hackers turn on air-condition, wipers, change radio stations, and eventually kill the engine. Luckily for the driver, it was just a demonstration made by researchers and not a murder attempt. They could have taken control of the brakes or steering if they desired (Schneier, 2018, s. 1). Airplanes are also proven to have cyber weaknesses. There are no indications that vessels will not be as vulnerable. The maritime industry is a part of our critical infrastructure. Affecting a country's critical infrastructure can be a desired goal for attackers. It is important to take a close look at the cyber security before a serious incident with major consequences happen.

1.2 Similar projects

Bridges can be expensive and act as an obstacle for seagoing traffic. An electric ferry can be an alternative. It can be cheaper than a bridge, and it has a low environmental impact. At the Norwegian University of Science and Technology (NTNU) they are developing an autonomous ferry called *MilliAmpère*. It is a small ferry crossing Ravnkloa and Vestre Kanalhavn in Trondheim with at least 12 passengers as well as bicycles and strollers (Borkamo, Solvoll, and Wetting, 2018). It is a short crossing of under 100 meters and will only take one minute, but passengers will be spared of 10-15 minutes' walk by taking the ferry (Skoglund, 2018).

MUNIN is a collaborative research project that is co-funded by the European Commissions (MUNIN, 2016a). It is short for Maritime Unmanned Navigation through Intelligence in Networks. This project was the first to see if and how it is possible for unmanned and large merchant ships to have the same, or even higher, levels of safety as conventional ships. They will develop a concept for an autonomous ship that will be guided by automated onboard decision systems and controlled remotely by an operator in a control station ashore (MUNIN, 2016a). For those who are familiar with old Norse mythology might recognize the name. Munin was one of Odin's ravens. The idea is that a ship developed in this project will autonomously, safely, and independently bring cargo to its destination, just as the raven did (MUNIN, 2016b).

Rolls-Royce Commercial Marine and global towage operator Svitzer have successfully developed the world's first remotely operated commercial vessel (Rolls-Royce Commercial Marine, 2017). A demonstration took place in the beginning of 2017 in Copenhagen harbor in Denmark and the development is a part of the SISU project. *Svitzer Hermod*, as the tug is called, conducted multiple remotely controlled maneuvers safely. The captain controls the tug from a Remote Operating Center, which is similar to a Shore Control Center that will be discussed further in this thesis.

Rolls-Royce Commercial Marine has also developed an autonomous ferry. It was in collaboration with Finferries, which is a Finnish state-owned ferry operator (Finferries, 2018). The car ferry *Falco* is the world's first fully autonomous ferry and it travels in the archipelago south of the city of Turku in Finland. During the demonstration, *Falco* navigated autonomously between Parainen and Nauvo and was remotely controlled on the return journey (Finferries, 2018).

In September 2020, an autonomous version of *Mayflower* will cross the Atlantic 400 years after the original Mayflower did (Copestake, 2019). It will sail unmanned from Plymouth in the UK to Plymouth in Massachusetts, US, and the crossing is estimated to last for two weeks. This fully autonomous ship is being developed by the marine research organization Promare, American information technology company IBM, and the University of Plymouth, UK (World Maritime News, 2019). Mayflower will use wind and solar power as energy sources, and in case of an emergency, a diesel backup generator will be present. Three research pods will be carried on the vessel. It contains sensors and scientific instrumentations to help get a better understanding of sea level mapping, maritime cyber security, ocean plastics, and marine mammal monitoring (World Maritime News, 2019). Water samples taken during the crossing will be analyzed by the University of Plymouth. In addition to these research areas, it is an active test platform for machine learning algorithms and artificial intelligence for collision avoidance (Copestake, 2019).

Kongsberg has developed a substantial experience with autonomous systems. For instance, they have developed an electric Autonomous Underwater Vehicle called *Hugin*. *Hugin* is a collaboration between the Royal Norwegian Navy, Norwegian Defence Research Establishment (FFI), Kongsberg, and Statoil and was initiated in 1995 (Kongsberg Maritime [KM], u.å.b). It can conduct oceanographic and marine geological survey, inspection of geophysical sites, pipelines and subsea structure, and environmental monitoring, among others (KM, u.å.a). This can happen supervised, semi autonomously, or autonomously at depths down to 6000 meters. It is for instance used to search for mines on the seabed. *Yara Birkeland* will have the same brain as *Hugin* (Moll and Thuestad, 2019, 12:05-12:18). Other autonomous underwater vehicles developed by Kongsberg are *Munin* and *Remus*. They are also working on an Unmanned Surface Vehicle called *Odin* in collaboration with FFI (KM, u.å.d).

Kongsberg Maritime, also referred to as KM, is developing another autonomous vessel. This is a collaboration with Asko, and the vessel they are developing is called *AutoBarge* (KM, 2019). The project will end with two autonomous, electric and zero-emission vessels which will cross the Oslo fjord. *AutoBarge* will fit 16 semitrailers and replace 150 truck journeys a day between Moss in Østfold and Holmestrand in Vestfold (Stensvold, 2019). It will result in a reduction of CO_2 emission and improve road congestion and safety. Each of the vessels are built with a regular bridge but will later be monitored from a Shore Control Center, just as *Yara Birkeland* (Stensvold, 2019). The goal is to have autonomous and electric tractors made by Kalmar to push the semitrailers on and off the vessels. Asko has ambitions of driving the trailers electrically from the ports to Asko's storage (Stensvold, 2019). The plan is to start testing in 2021 and to be autonomous, electric, and have zero-emission from 2024.

1.3 Structure of thesis part 1

I have given a short introduction to the thesis by explaining my motivation, similar projects, and the research questions that I will be basing my thesis on. The thesis is divided in two. The first part consists of publicly available information in chapters one through four, while part 2 is based on secret information in chapters five through eleven. A structure of the thesis part 2 is found at page 51. The list of acronyms and abbreviations and a glossary are located at the end of my thesis. I will further give a short summary of the chapters in part 1.

Chapter 2 – Background

In this chapter the Yara Birkeland project and the concept of a shore-based control center are explained in more details. Additionally, cyber security themes are described. The themes are definitions of vulnerability and threat, the Norwegian National Security Authority's *Helhetlig digital risikobilde 2019*, authentication, cyber-attacks, information security, and cryptography.

Chapter 3 – Safety and security of ships

Different aspects of safety and security of ships are presented in this chapter. Firstly, the difference between safety and security is explained. Then common vulnerabilities in ships, threat actors, and attacks against the maritime sector are described. Lastly, different cyber security work is presented.

Chapter 4 – Autonomous vessels

This chapter focuses on autonomous vessels. Autonomy is defined and described, as is the difference between remote controlled and autonomous vessels. The following subchapter introduces the concepts of autonomous vessels. The chapter ends with some safety and security aspects of unmanned and autonomous vessels.

Chapter 2

2 Background

2.1 The Yara Birkeland project

Norway has come far in the development of autonomous vessels. Kongsberg, in collaboration with Yara, are developing the ship *Yara Birkeland*. According to the plans, it will be launched in 2020 and fully autonomous in 2022. Initially it will operate as a manned vessel. It will then be remotely operated and finally, it will become fully autonomous. The vessel will be the world's first fully electric and autonomous container ship, with zero emissions (KM, u.å.c).

Figure 1 Illustration of Yara Birkeland (Andersen, 2019b)

Yara Birkeland will sail between three ports – Herøya, Brevik, and Larvik. This is a sea area with high density. To transport the products from Yara's factory in Porsgrunn (Herøya) to Brevik and Larvik today, more than a 100 diesel truck journeys are needed (Skredderberget, 2018). The Yara Birkeland project has a potential to reduce 40,000 diesel truck journeys each year, meaning a reduction in NO_X and CO_2 emission (KM, u.å.c). The result will help meet the UN sustainability goals, in addition to improve road congestion and safety.

Figure 2 Illustration of Yara Birkeland (Yara, u.å.)

It is not just the voyage itself that will be autonomous. By using electric equipment and cranes, discharging and loading can be done automatically. Kalmar will deliver autonomous software, services, and equipment for a container handling solution for the port at Herøya (Yara, 2018). These elements make the supply chain fully electric and digitalized, and operations can be performed autonomous without emission. Berthing and unberthing will not need human intervention or require special implementations dockside, because *Yara Birkeland* will be equipped with an automatic mooring system (KM, u.å.c). To accomplish the desired result, the new systems have to use artificial intelligence (AI), machine learning, and digital twin technology (Ship IP LTD, 2018).

2.2 Shore Control Center

For unmanned and autonomous vessels, many functions which are traditionally located onboard a vessel are being transferred to a Shore Control Center (SCC). For instance, the crew will be removed from the bridge and moved here. It is almost certain that a SCC will be present for all autonomous ships. It will monitor and control the vessel and it has the potential to monitor multiple ships simultaneously. It can be compared to an air traffic control which monitors the airport traffic. There are multiple areas a SCC will be used for – to satisfy legal requirements that humans are in control of the ships, to reduce the required complexity of onboard detection and control systems, and as backup in case the ship encounters unexpected events (Nordahl and Rødseth, 2017). Signals from components onboard the vessel will be sent here, where it will be interpreted, and give the operator a clear overview of the surroundings. Even though autonomous vessels are operated without the need for human intervention, certain events outside the defined operational constraints may occur. In such events, an operator will assist the vessels and change the operating mode from autonomous to remotely controlled. If the ship has lost communication with SCC during an emergency, it is envisioned to activate fail-to-safe mode (Fjelldal, 2018, s. 34). The centers will handle exception and emergency handling, operational monitoring, condition monitoring, decision support, surveillance of the autonomous ships and its surroundings, and all other aspects of safety (KM, u.å.c). It should be noted that a SCC does not necessarily need to be located on shore. For instance, a convoy of unmanned ships being shepherded by a manned escort vessel (Nordahl and Rødseth, 2017).

The Shore Control Center was thoroughly analyzed in the MUNIN project, mentioned in section 1.2. It was concluded that designing a general autonomous ship system without a continuously manned SCC would be very challenging (Nordahl and Rødseth, 2017). Certain roles are likely to be implemented here, in order to satisfy current manning rules. When SCC is in control of the ship, it will take over the responsibilities of the ship's master and other persons with defined roles onboard. The flag state authorities determine exactly what the roles are. Some roles will according to (Nordahl and Rødseth, 2017) be:

> Master: A person in overall charge of the ship. The duties of a security officer may also be included.
>
> Chief engineer officer: A person in overall charge of the mechanical propulsion, and operation and maintenance of the electrical and mechanical installations.
>
> Officer of the watch*:* A person that is responsible for monitoring the ship at all times and intervene if needed.

2.3 Cyber security

2.3.1 Vulnerability and threat

A vulnerability is a weakness in an application. It can be a bug in the implementation or a design flaw which allows an attacker to harm the people relying on the application (Category: Vulnerability, 2016). When there is a potential for violating the security there exists a threat. Simply, a threat is a possible danger that might exploit a vulnerability (Cyberattack, 2020) and any vulnerability that has the potential of being exploited, is a cyber threat. Intentional threats are threats made by intelligent actors like a criminal organization, or an individual hacker. Alternatively, accidental threats are threats like malfunctioning computers or natural disasters like earthquake, fire, flood, or tornado (Cyberattack, 2020).

2.3.2 Helhetlig digital risikobilde 2019

Yearly, the Norwegian National Security Authority (NSM) publishes a report covering the current digital risks we are facing. It is called *Helhetlig digital risikobilde*, and it is made to raise awareness and as motivation for improving the digital security in both private and public companies. The report covers issues related to individuals, businesses, and society (Nasjonal Sikkerhetsmyndighet [NSM], 2019a, s. 2). In the 2019 report, themes like the risks of digitizing critical infrastructure, attack trends, challenges and opportunities that come with the major technology trends, Norway's dependence on the digital, international community, and individual's online security are elaborated (NSM, 2019a, s. 2). Information security is about controlling the confidentiality, integrity, and availability of the information you manage. As the amount of digitized information and information systems increases, it becomes more available (NSM, 2019b, s. 19).

New trends like Internet of Things (IoT), 5G, virtual and augmented reality, and artificial intelligence will further develop our society by giving us smart cities, houses, businesses, and services. It also makes Norway more dependent on the digital international community. At the same time as the digitalization evolves with a high speed, the security challenges become more complex. The value chains get longer and the amount of them increases, resulting in more dependency on digital solutions. These solutions depend on other, often foreign, services, businesses, and products. The foundation of digitalization consists of software and hardware, but only a small fraction of it has been developed in Norway (NSM, 2019a, s. 5).

Internet consists of a number of different devices, interconnected by an increasing number of networks and services. There are vulnerabilities within all areas – the software, hardware, protocols, algorithms, routines, value chains, organization, and people all have vulnerabilities. Unless done properly, new vulnerabilities are created when these elements are connected. Despite the effort put into closing security holes, new ones are constantly coming. It is important to see the whole picture – the organization, people, and technology. The world outside of the organization has a direct impact on their values, and it is increasing.

Change and development of organizations and Information and Communications Technology (ICT) systems will always come with certain risks, some which have to be accepted in order to achieve the possible gains. Alongside technological developments come new challenges, vulnerabilities, and consequences. This is why we have to focus on ensuring the best possible outcome, even against future challenges. It is possible for a secure digitalization. Through building resilience to sophisticated operations from threat actors and at the same time being prepared for incidental events, requires continuous work, ability, and determination (NSM, 2019a, s. 9).

Today, we live our lives online to a greater extent, which naturally increases the digital crime. We become victims of hate, harassment, identity theft, and abuse. Among others, businesses are exposed to director fraud, ransom virus, and crypto mining where malware recover cryptocurrency on the victim's ICT equipment (NSM, 2019a, s. 12). Yesterday's technological challenges will not disappear, they are accompanied by new vulnerabilities and attack methods. Also, the criminals whose motives are related to economic or material gain have become digital. Advanced tools and criminal services are for sale online and our money can be stolen without the perpetrator setting foot on Norwegian soil. It is often hard to find out who is behind it, but even more difficult to prove it. Different actors collaborate, use the same tools, try to impersonate other actors, lay out false leads, and use advanced anonymization techniques (NSM, 2019a, s. 15). Næringslivets sikkerhetsråd's *Mørketallsundersøkelse* from 2018 revealed that coincident and bad luck are stated as the cause of 2/3 of the incidents, followed by human error and lack of security awareness (NSM, 2019a, s. 13). A survey conducted by Norges vassdrags- og energidirektorat in 2017 about the state of ICT security in the power sector showed that around 50% of the responding companies had experienced undesirable incidents. Further, 40% of the companies that had events they categorized as their most serious incident, did not make any changes to improve their security (NSM, 2019a, s. 13).

We have the most to lose when important functions for the society are digitized and vulnerable to digital threats. In NSM's perception, these targets are vulnerable for serious digital attacks and it will have major consequences. The trends are the same as previous years - the digital risk increases. There are more values to look out for, and we are challenged by professional and targeted threat actors that are becoming more advanced. At the same time, there are significant digital vulnerabilities in Norwegian businesses and society. NSM (2019a, s. 6) says that the most important tool for a secure digitalization is: A secure digital Norway. According to NSM (2019a, s. 5), government intelligence agencies and criminal actors are the biggest digital threats to Norway right now. They see a steady number of digital attacks against Norwegian targets. This includes businesses that provide important functions for the society. Digital attacks become harder to detect and the methods are complex. The digitalization makes it possible to gain access into organizations in new ways, including via IoT devices and private equipment. Complexity makes it harder to see how impact on a subsystem can reflect elsewhere in the system. Businesses are often unprepared for serious incidents, which makes it hard to limit the damage and restore a reasonable level of security if one occurs (NSM, 2019a, s. 5).

Our most important, vital functions for the society are now controlled by computers. Computers make sure we have electricity in our houses, that the trains can move, airplanes can take off, cars can drive safely on the roads, goods are delivered, that we get health care, and that defense and emergency services can be there when needed (NSM, 2019a, s. 21). We are strongly dependent on these systems and incidents can have major consequences, whether caused by natural disasters or a digital attack. The Norwegian Police Security Service (Politiets sikkerhetstjeneste - PST) writes in their threat assessment that intelligence agencies in other countries will continue mapping operations to uncover functions and vulnerabilities within Norwegian critical infrastructure, crisis management, and security and emergency preparedness (NSM, 2019a, s. 21). Other events that are less serious and incidental, like a malware infection, may overload or disrupt critical systems. In the recent years, other nations' industrial control systems have been hit by serious digital operations. Such incidents can happen in Norway as well. Industrial control systems are often designed to ensure integrity and reliability, and not to resist digital attacks (NSM, 2019a, s. 21). They are often based on outdated and unsecure technology.

Foreign states especially look for highly technological developments and trade and state secrets, when they are conducting digital intelligence operations against Norwegian businesses (NSM, 2019a, s. 15). The Norwegian Intelligence Services (Etterretningstjenesten) and PST point out that the government, businesses in defense, space, maritime, medical research, petroleum, and power are exposed areas (NSM, 2019a, s. 15). In addition to information, foreign states want to have the opportunity to influence Norwegian decision-making processes through ownership, cooperation, and trade. These actors have great resources and are working towards a long-term goal.

Direktoratet for samfunnssikkerhet og beredskap has analyzed several crisis scenarios and says that one of the most critical is an attack against key nodes in Telenor's transport network, harming both hardware and software components (NSM, 2019a, s. 22). As a result, all commercial electronic communications will be paralyzed and can lead to deaths, critical injuries and illnesses, as well as losses of several billion kroner. Similarly, Nasjonal Kommunikasjonsmyndighet means that Denial of Service attacks targeted at key elements in the infrastructure of electronic communications can have major consequences (NSM, 2019a, s. 22). In the future, the consequences may potentially be greater. The next generation of emergency network is according to plans going to be implemented in the commercial mobile networks based on 5G (NSM, 2019a, s. 22). The Norwegian Armed Forces (Forsvaret) wants to use a part of their communication in a similar manner. 5G will lead to more secure systems, but also expose the mobile networks to a wider range of attack methods and threat actors (NSM, 2019a, s. 22). Therefore, security will be critical from the early stages of the development.

Areas like earth observation, communication, and position, navigation and time (PNT) are supported by the space sector (NSM, 2019a, s. 23). They are all important for civil and military purposes, in addition to keeping the government safe. Transportation, power supply, and electronic communication are some of the functions dependent on the space sector. This sector is important to protect. Ground stations that are connected to a network have the same cyber security challenges as other Information and Communications Technology (NSM, 2019a, s. 23). They can be exploited to compromise information and satellites. Being able to

prevent and handle unintentional and intentional interference with the satellite signals and provide digital and physical security for space-based infrastructure is important. The Allied and Norwegian aviation were affected of GPS jamming several times during the military exercise Trident Juncture in the fall of 2018 (NSM, 2019b, s. 11).

Only a few large providers deliver the wanted technology. This is true within multiple industries. There will be a need and desire to increase the use of data centers as applications and technologies become more complex (NSM, 2019a, s. 25). Most of the major providers do not have such data centers in Norway. The consequence is that Norwegian data is stored and processed abroad by foreign personnel. This kind of data will be of great value. It can be sensitive data about the society, businesses, and individuals. Norwegian businesses may require and, in some cases even have the right to demand, that data centers are located in Norway (NSM, 2019a, s. 26). As a result, several large vendors are in the process of doing so. It is likely that new real-time IoT devices will require that data centers are physically located close to the applications in order to avoid delays (NSM, 2019a, s. 26). For example, for self-driving, communicating cars. Norwegian companies should have architectures to protect us against external and internal incidents, whether they are national or international. Redundancy, alternative solutions, and the possibility of manually overriding functions and maintaining services with reduced quality and performance must be considered (NSM, 2019a, s. 26).

People are often the vulnerability being exploited. We develop, buy, set up, use, and maintain computers, networks, and services (NSM, 2019a, s. 18). We take shortcuts, are sloppy, allow ourselves to be pressured or bought, and do not acquire or receive training. We still click on links in emails, put memory sticks into machines, and choose bad, reusable passwords. The threat actors know this. It is easy to blame the user, but the systems make it possible. The technology has to contribute to help the user and avoid these mistakes, and prevent unwanted consequences (NSM, 2019a, s. 18). NorSIS conducted a survey called *Nordmenn and digital sikkerhetskultur*. Even though it has been pointed out that digital security training is an important mitigation, the survey concluded that 2/3 have not received any training the last two years (NSM, 2019a, s. 18).

Emails with malware or malicious links attached are still the most used input vector (NSM, 2019a, s. 16). Mass mailings are still used, but NSM sees in particular emails aimed specifically at individuals in an interesting business (NSM, 2019a, s. 16). They can be convincingly written in correct Norwegian or English. Email is an insecure communication tool given too much trust. NSM (2019a, s. 16) sees several attempts at digital burglary through Internet-exposed services. Many solutions are updated occasionally and can often have expired licenses. In almost every situation, older vulnerabilities are exploited.

A simple method to reduce the attack surface, is to remove standard passwords and utilize multi-factor authentication. Organizations should monitor their network traffic and the activities on their systems. Threat actors also use input vectors like creating malicious water hole websites, compromising other websites with malware script, and installing malware on mobile phones that the end user connects to the organization’s internal services (NSM, 2019a, s. 16). If the threat actor has gained access to the organization’s network, it is important to

prevent them from spreading and obtaining additional privileges. NSM's penetration testers can often see unsegmented and unsecured networks, servers, and network equipment that are not hardened or updated (NSM, 2019a, s. 16). They can also see connected machines that the organization does not have control over. New and updated software are often designed with security in mind. Whitelisting, multi-factor authentication, and fleet management solutions are important mitigations. Knowing that they can also be targeted, and when configured correctly, these mitigations are effective. Businesses should have automatic updates, configuration and user management, centralize logging solutions, and have the same requirements for authentication on internal services as on Internet-exposed services (NSM, 2019a, s. 18).

Digital security work is not just about the technical measures. It also requires good management, and organizational and procedural measures to prevent serious digital attacks. In January 2019, the government launched a new national strategy for digital security to meet the digitalization we are facing in a secure way. Also, a national strategy for digital security expertise came, focusing on strengthening research and education (NSM, 2019a, s. 9).

NSM has listed how an attack against a Norwegian business is typically conducted (NSM, 2019a, s. 17):

1. Actor finds login details through Internet mapping and gains access to an Internet-exposed server. Using multi-factor authentication, such as one-time passwords, smart cards, or certificates are possible mitigations.
2. Actor does not get access to the organization's values. A measure that should be established is a policy for access control where administrator accounts, end users, or service accounts are not given more privileges than necessary.
3. Actor maps and finds a server that can be exploited and gains full privileges. Segregating and segmenting the organization's ICT infrastructure into networks and zones are possible mitigations.
4. Actor has access to the organization's values. A mitigation is to segregate ICT infrastructure into security zones to separate information with different value and different need for user access.
5. Actor steals the organization's values. Firewalls with logging ability to filter and control traffic between the different security zones and the Internet is a mitigation.

Hydro was attacked by a ransomware in March 2019. It was called "LockerGoga" and encrypted files, including system files (NSM, 2019a, s. 19). The incident affected operations and production in multiple business areas. Hydro did not pay the ransom. NSM expresses that they are glad Hydro chose to inform about the incident. It brings attention to this type of attack and helped the Norwegian authorities to uncover preparations for other attempts (NSM, 2019a, s. 19). Ransomware attacks like this might affect more Norwegian businesses in the future. To prevent and limit the harm after similar incidents, it is important that the companies are open, share information, and cooperate with each other.

2.3.3 Authentication

The term authentication is used for the process of confirming a claimed identity, and for the process of confirming whether the information is legit and not altered (Knapskog and Nätt, 2019). Basically, it is establishing confidence in the truth of some claim (Hole, 2016). It can be challenging finding out who is who on the Internet. The process of authenticating people becomes harder, while identity theft becomes easier. It is challenging to provide secure authentication methods because people want a method that is easy to use and secure, but these two are contradictions. According to Bruce Schneier (2018, s. 45), a survey showed that 80% of successful attacks are a result of misused authentication. Authentication does not prove that a person is who he/she claims to be, it can only provide a certain level of confidence. The authentication system involves the following roles (Hole, 2016):

Issuer: Generates the credentials. It can be the police issuing passports to Norwegian citizens.

Presenter: Presents the credentials. It can be a person holding a driver's license.

Verifier: Determines the validity of the credentials. This role is often combined with the issuer. It can be an immigration agent.

Individual does not only refer to a human, but also subjects, like computers, organizations, and other entities (Hole, 2016). In order to find this individual, an identifier is used to point to it. It might be a passport number or a serial number. Identity authentication is to establish a level of confidence that an identifier refers to an identity, which can be to verify if a password is associated with a username account. There are three fundamental types of authentication techniques:

Something you know: It can be a secret password, PIN, or security question. The combination of username and password is the most common authentication method. Password-based authentication is cheap, but unfortunately humans choose weak password and tend to reuse them in multiple systems, making it a weak authentication method. Possible attacks against such systems are Brute-Force/Dictionary, Social Engineering, and Man-in-the-Middle (Hole, 2016).

Something you have/possess: It can be a physical key or token, a digital certificate, or a text on your mobile phone. This authentication method is harder to forge. A possible attack is to steal or replicate the device, either by physical or digital means.

Something you are: Biometric is used to authenticate individuals. It can be a signature, fingerprint recognition, or iris scanner. This authentication method does not rely on secrets, and therefore stands out from the other methods (Hole, 2016). Instead it uses unique characteristics. The disadvantages to this method are noise that can occur in the measurement process, false negatives (erroneously rejection), and false positives (allowing unauthorized access) (Hole, 2016).

Authentication is also used between a client and a server, where the client is the presenter and the server is the verifier. The server should also authenticate itself and in this case the roles are switched. This is a two-way authentication and results in a high level of security. Such client-server systems can be used to hold individuals accountable for their actions. For example, by storing information in a log.

All of the authentication techniques mentioned above can be hacked, but the security is improved by combining them. Multifactor-authentication is an authentication method that combines the techniques of two or more classes. For example, a token followed by entering a PIN. In this example, there are two different techniques used and it is therefore called a two-factor authentication. Multifactor authentication is recommended for sensitive information as it is a more secure authentication method. The European Central Bank has defined strong authentication as “a procedure based on two or more of the three authentication factors” (Authentication, 2019).

2.3.4 Attacks

Attack is a word used for the techniques utilized by an attacker to exploit vulnerabilities in applications (Category: Attack, 2016). It can be confused with vulnerabilities. The difference is that a vulnerability is a weakness, while an attack is an action performed by an attacker. When it comes to computers and computer networks we are talking about cyber-attacks. Attackers perform cyber-attacks to try to alter, destroy, expose, steal, disable, or gain unauthorized access to a network, infrastructure, computer system, or any other smart device (Tunggal, 2020). It is any type of offensive maneuver to breach someone else’s, like an organization or individual, information system. A breached computer can also be used as a launch point for other attacks (Check Point, u.å.) or it can be used to gain access to sensitive information. Cyber-attacks have a big range. It ranges from installing spyware on a PC and making a botnet to destroying a nation’s critical infrastructure (Cyberattack, 2020).

Wikipedia defines an attacker as “a person or process that attempts to access data, functions or other restricted areas of the system without authorization, potentially with malicious intent” (Cyberattack, 2020). Normally, there exists a benefit the attacker wants to gain from disrupting a victim’s network (Cisco, u.å.). Cyber-attacks have increased in sophistication and seriousness. After Internet of Things have become a part of our lives, the impacts of an attack can have physical consequences. Alongside the evolvement of information technology are the criminals wanting new vectors for committing crime. The World Economic Forum has seen an increasing robustness and scale of cyberattacks. They wrote in their 2018 report "Offensive cyber capabilities are developing more rapidly than our ability to deal with hostile incidents." (Cyberattack, 2020). Such attacks hit businesses every day. John Chambers, the former CEO of Cisco, once said “There are two types of companies: those that have been hacked, and those who don’t yet know they have been hacked.” (Cisco, u.å.). Cisco’s Annual Cybersecurity Report showed that the number of incidents increased by four times from January 2016 to October 2017 (Cisco, u.å.).

Outside/inside attack

There are two types of attackers. It can either be an outside or inside attack. An inside attack is initiated from inside the organization’s security perimeter. It is performed by an insider, meaning someone who has authorized access to system resources and uses their access in a way not approved by the ones who granted it (Cyberattack, 2020). On the other hand, an outside attack is initiated from outside the organization’s security perimeter. Potential outside

attackers when it comes to the Internet, range from amateurs to organized criminals, international terrorists, and hostile governments (Cyberattack, 2020).

Targeted/untargeted attacks

Attacks can be divided into two. The first type of attack is the untargeted. In such attacks, the attacker does not target anyone specific, but he/she targets as many devices, users, or services as possible. There are many services or machines with vulnerabilities. The target is just one of many potential victims. It is likely that the attacker uses tools and techniques that are available on the Internet and that can locate companies or ships with known vulnerabilities (BIMCO mfl., 2016, s. 3). National Cyber Security Centre (2015) and BIMCO mfl. (2016, s. 4) have listed some techniques that may be used:

> Social Engineering: A non-technical technique used to manipulate an insider into breaking security procedures. It can be done through interactions via social media.
>
> Phishing: Emails sent to many people asking for sensitive or confidential information. It can also try to make them visit a fake website.
>
> Water holing: Compromising a website or making a fake one to exploit visitors.
>
> Ransomware: Malware that encrypts data on systems and it typically is not decrypted before a ransom is payed. Three recent examples are ‘LockerGoga’ from 2019 and ‘WannaCry’ and ‘NotPetya’ from 2017 (Check Point, u.å.).
>
> Scanning: Randomly attacking a large part of the Internet.

The other type of attacks is the targeted. An attacker has specifically targeted your organization. It can be because he/she has a particular interest in the company or is paid to do so. Usually, a targeted attack is more damaging than an untargeted. The reason is that the attack has been specifically tailored to attack your processes, systems, or people, either at work or home (National Cyber Security Centre, 2015). It can be a sophisticated attack that has been planned for a long time in order to find the best attack vector into the system. National Cyber Security Centre (2015) and BIMCO mfl. (2016, s. 4) have listed some techniques that may be used for a targeted attack:

> Spear-phishing: Individuals are targeted with personal emails and they can contain attachments with malicious software or links that automatically downloads a malicious software. It is similar to phishing explained above.
>
> Deploying a botnet: Botnets are used to deliver DDoS attacks.
>
> Subverting the supply chain: Attacking equipment or software that is being delivered to the organization.

Passive/active

There are both passive and active attacks. Passive attacks have the intention of learning, accessing, or making use of information, but it does not affect the system resources (Cyberattack, 2020). As a result, these types of attacks compromise confidentiality. Such cyber threats include computer and network surveillance, port scanning, keystroke logging, wiretapping, backdoor, eavesdropping, and vulnerabilities (Tunggal, 2020). An active attack on the other hand, attempts to alter the system resources or affect their operation

(Cyberattack, 2020). These attacks compromises integrity or availability. Examples of active cyber-attacks are DoS/DDoS, phishing, spoofing, Man-in-the-Middle, zero-day exploit, SQL injection, virus, privilege escalation, buffer overflow, and ARP poisoning (Tunggal, 2020).

Zero-day attacks

Zero-day attacks are based on exploits of bugs that are not yet identified by the software vendor (Koykov and Papazov, 2016a). This means that the vendor has not started working on a fix and the patch is in its zeroth day of development. Zero-day attacks are like 'silver bullets' for the attackers since there is no known mitigation, especially when working in environments with limited network (Koykov and Papazov, 2016a). Hopefully software vendors have quickly fixed the relevant vulnerability after the first successful attack. Of course, it is better if they find and fix the flaw before an attack is performed.

Stages of a cyber-attack

Cyber-attacks can be conducted in four stages (BIMCO mfl., 2016, s. 4-5; National Cyber Security Centre, 2015):

> Survey/Reconnaissance: Gaining information about the target that can be used to prepare for a cyber-attack. Investigating and analyzing available information to identify potential vulnerabilities.
>
> Delivery: Attacker may attempt to access the target's systems and data. A vulnerability can be exploited. Methods for gaining access can for instance be an email containing a malicious file/link or infected removable media as part of a software update.
>
> Breach: Exploiting a vulnerability to gain unauthorized access. The extent of the breach depends on how significant the vulnerability is, and the method chosen to deliver the attack.
>
> Affect: Attacker carries out activities within the system to achieve their goal. For instance, it can be expanding access, exploring the systems, or manipulating information.

Trends

Check Point has looked at the cyber-attack trends. 2019 was summed up as a mix of attacks where phishing emails remains a worry for organizations as it continues to be one of the biggest threats to cyber security, and the use of ransomware has grown (Check Point, u.å.). Especially in the southeast of US, small local and state government agencies have been targeted. The adoption of cloud-based subscription services, cloud computing, and the existence of mobile devices increases the attack surface and creates more ways into an organization. They saw an increase in attacks on the software supply chain. Typically, a threat actor modifies and infects a building block that a legitimate software relies on with malicious code (Check Point, u.å.). Another trend seen is attacks targeting cloud services. One of the main causes of data theft worldwide was misconfiguration of cloud environments (Check Point, u.å.). Both cloud cryptomining and exploitation of public cloud infrastructure have increased. The last trend mentioned is attacks against mobile devices. Threat actors have adapted their methods and techniques to fit mobile devices. Now, threats like malware

capable of stealing credentials, payment data, and funds from bank accounts are a common mobile threat. It has resulted in a significant increase of infiltration of banking malware by 50% compared to 2018 (Check Point, u.å.).

2.3.5 Information security

Information security is a term used for the requirements regarding reliability and security when transmitting and storing information (Nätt, 2018). It is traditionally illustrated with a triangle consisting of confidentiality, integrity, and availability, and it is referred to as the CIA-triad. They represent three actions that can be done with someone's data: steal a copy, modify data, or delete data.

Confidentiality is about protecting the privacy of our data from unauthorized viewers. It ensures that the information is kept private and only authorized people have access to it. It could be sensitive information like corporate secrets (source code, product plans) or personal information (credit card numbers, social security numbers) (Ellingsen and Gejibo, 2017). Encryption is a key component for ensuring confidentiality as it ensures that only the users having access to the appropriate key will get access. Other security mechanisms are physical security (Nätt, 2019a).

Integrity is about protecting information from being modified by unauthorized people during transmission and in storage. During the data's lifecycle, it should be complete and accurate. Integrity is used for maintaining and assuring this (Information security, 2020). Encryption is a method for assuring integrity, just like for confidentiality. Hashing is a commonly used method. Other than encryption, signatures and authenticators (checksum) are used as security mechanisms (Nätt, 2019b). Integrity is a term used for both authentication of the data's content and for message integrity. Content authentication guarantees that the information has not been altered between the sender and receiver, and that the receiver is who he/she claims to be (Knapskog and Nätt, 2019).

Availability will ensure that authorized parties are able to access the information when it is needed. It is important that the communication channels used to access the information is functioning correctly (Information security, 2020). There are many possible threats against availability. It can be DoS/DDoS attacks, user/software/hardware failure, and natural disasters like fire and power outage. Mechanisms to help ensure availability are antivirus, firewalls, backups (physical storage), redundancy, and Uninterrupted Power Supply (Nätt, 2019c).

An important step towards designing a secure system is to protect these three aspects. However, there is debate whether the CIA-triad is sufficient with the rapid development of technology (Information security, 2020). The extended standard model for information security includes five pillars. The first three pillars are the CIA-triad. The first of the extended pillars is authenticity, which ensures that the source of the information is who he/she claims to be (Koykov and Papazov, 2016d). Lastly, non-repudiation is to ensure that it is not possible to deny any performed actions or claim to have performed actions you have not (Nätt, 2019d). It can be especially important for e-commerce and financial applications (Guide to Cryptography, 2018). For instance, it should not be possible for someone to request a money

transfer from one bank account to another and then refuse that the request was made by him/her. By applying cryptography with non-repudiation, it is possible to prove, usually through digitally signing the transaction request, who authorized the transaction (Guide to Cryptography, 2018).

So far, most threats have affected confidentiality. Such attacks can be embarrassing (like the theft of pictures from celebrities' Apple iCloud in 2014), expensive, harmful (like when the Russians hacked the Democratic National Committee in 2016), and it can be a threat towards the national security (Schneier, 2018, s. 78-79). Computers today have the possibility of affecting the physical world, resulting in different consequences. Now the threats targeting integrity and availability are the most harmful. There are multiple examples that can be used as illustration, but here is one concerning cars with Internet connectivity. Someone may listen to your conversations through a Bluetooth connection (confidentiality threat), but there are more reasons to be concerned about someone deactivating the breaks (availability threat), or someone modifying parameters of the automatic lane-centering and following-distance systems (integrity threat) (Schneier, 2018, s. 79).

2.3.6 Cryptography

Different vulnerabilities make it easier for unauthorized access and manipulation of systems and information. It is necessary to adopt the best protection possible. Cryptography is an important aspect of information security. It was initially used by the military and areas of academia (Guide to Cryptography, 2018), but because of the Internet, cryptography is everywhere now. Passwords and mobile phones use cryptography. It can also be used for remote access such as IPsec VPN, securing confidential or sensitive information, obtaining non-repudiation using digital certificates, certificate-based authentication, email and secure messaging, or online orders and payments (Guide to Cryptography, 2018). There are multiple layers where a web application can apply cryptography: application, application server or runtime, operating system, and hardware (Guide to Cryptography, 2018). It requires a good understanding of different areas to select the appropriate approach. It can be areas of risk and the level of security strength it might require, application requirement, flexibility, and cost. Cryptography can be complicated and difficult to understand. A small mistake can make it useless against serious attacks. The majority of security breaches actually come from exploiting mistakes in the implementation (Guide to Cryptography, 2018).

A cryptographic protocol describes how a cryptographic algorithm should be used in order to allow secure communication (Cryptographic protocol, 2019). Simply put, a protocol contains a set of instructions or rules that determine how to act or interact in given situations (Kemmerer, 2015). To secure messages being transferred at the application level, cryptographic protocols are generally used (Cryptographic protocol, 2014). At least some of these features are included: key agreement or establishment, transfer of symmetrically encrypted messages, authentication, secret sharing methods, non-repudiation, entity authentication, confidentiality, integrity, secured application-level data transport, and secure multi-party computation. Algorithms can be more suited for some tasks than other. Current evaluation and certification schemes for cryptographic protocols are Common Criteria and FIPS 140-2 (NSM, 2016).

Key length of a cryptographic system gives an indication on how strong it is. Even if a large key length is used, most of the benefits will be eliminated if the unprotected keys are stored on the same server. Another common mistake is to make your own cryptographic algorithm. Many web applications were successfully hacked because the developers thought they could create their own cryptographic functions (Guide to Cryptography, 2018). Cryptographic functions are thoroughly tested and therefore it is always a good idea to use the ones that are proven to be secure. It should be noted that even though a secure algorithm is used, it might be vulnerable to reverse engineering, for instance.

Authentication can make it possible to understand the identity of a remote user or system. For example, an SSL certificate of a web server can provide proof to the user that he/she is connected to the correct server. It is however not the identity of the user, but rather the identity of the cryptographic key of the user (Guide to Cryptography, 2018). Digital certificates can identify the server and client and must be verified before any secure connection can be established. The services a cryptographic function can provide is authentication, non-repudiation, confidentiality, and integrity. They are explained further in section 2.3.5.

As mentioned above, cryptography relies on keys to assure a user's identity and to provide confidentiality, integrity, and non-repudiation. Therefore, it is vital that the keys are adequately protected. If a key is compromised, it cannot be trusted anymore. All keys should be replaced if a system is compromised in any way. Keys should not be stored in the code (Guide to Cryptography, 2018). It makes it difficult to replace the keys if necessary. File system permissions can help protect the cryptographic keys and it should only be possible for the application or user that access them to have read rights (Guide to Cryptography, 2018). Changes in keys should at least be logged and monitored. An option for monitoring the access of keys is host based intrusion systems (Guide to Cryptography, 2018).

Cryptographic algorithms are typically divided into two classes. Firstly, symmetric algorithms are strong, but slow to run. Secondly, asymmetric algorithms are quick to run, but less secure. A combination of the two approaches is often used (Guide to Cryptography, 2018). The most traditional form is the symmetric cryptography (Guide to Cryptography, 2018). The involved share a common secret (password, pass phrase, or key), and the encryption and decryption is performed with the same key. Symmetric algorithms tend to be relatively fast, but they can only be used if keys have already been exchanged. The systems can have practical limitations when systems with multiples users each want to set up independent, secure communication channels. This is because of the requirement to securely distribute and manage large numbers of keys (Guide to Cryptography, 2018). Both AES and DES are symmetric algorithms. It is advisable to use AES. When DES was broken, the United States National Institute of Standards and Technology (NIST) hosted a selection process for a new algorithm. The winner was Rijndael with the cryptographic system that is now known as the Advanced Encryption Standard or simply AES (Guide to Cryptography, 2018).

Asymmetric cryptography is also known as Public/Private key cryptography. These algorithms use two keys, where one is used for encrypting the data and the other key is used for decrypting it. One of them is labelled the Public key and is not secret, while the other is labelled the Private key and must be kept hidden. Depending on how they are used, asymmetric cryptographic systems can provide different functions (Guide to Cryptography, 2018). For example, encryption, decryption, digital signature, and verifying a signature. RSA and ElGamal are examples of asymmetric cryptographic systems (Public-key cryptography, 2020).

Hash functions take some input of arbitrary length and generate a fixed-length hash. It is easy to a calculate the hash, but difficult or impossible to reverse to the original input if only the hash is known. Also, it is difficult to guess an input that will match the desired output. MD5, SHA-1, and SHA-256 are examples of hashing algorithms. The first two are considered weak algorithms and will likely be replaced after a similar process as AES (Guide to Cryptography, 2018). It is recommended to add a salt or random string to the input when generating the hash.

Cryptography relies on being hard to break, more specifically being computationally expensive. As computing power increases, brute force attacks will make cryptographic systems or the use of certain key lengths unsafe (Guide to Cryptography, 2018). Standard bodies like the National Institute of Standards and Technology (NIST) come with cryptography recommendations. OWASP's recommendations on how to choose an open, standard algorithm are (Guide to Cryptography, 2018):

Symmetric algorithms: For most applications, a key size of 128 bits are sufficient. Secure systems should consider using 168 or 256 bits. Message authentication code (MAC) should be included after encryption.

Asymmetric algorithms: Unless you need a big key size, do not use it. Bruce Schneier (2002) recommended the following key lengths for threats in 2005. For most personal applications, key sizes of 1280 will be sufficient. Key sizes of 1536 bits should be acceptable for most secure applications, while highly protected applications should consider using 2048 bits.

Hashes: For most applications, hash size of 128 bits are sufficient. Secure systems should consider 168 or 256 bits.

NSM (2016) recommends utilizing Transport Layer Security (TLS) when transferring information between different systems, as basic security. When the guidance *Sikring av kommunikasjon med TLS* (NSM, 2016) was written, under half of the communication on the Internet was secured. The protocol is recommended by NSM to be used for as much communication as possible for ensuring authenticity, integrity, and confidentiality. Standard TLS does not ensure non-repudiation (Cryptographic protocol, 2019). The person you contact (the server) must authenticate itself. In some cases, the client should also authenticate. When the authentication is confirmed, integrity and confidentiality protected communication can be established (NSM, 2016). Encrypted communication can hide compromised and exfiltrated information, and it is important to stop unwanted encrypted traffic and only allow approved.

TLS lies in the application layer and can be utilized by various protocols, applications, and services that need secure communication, and some common uses are HTTPS, SMTP over TLS, STARTTLS, and OpenVPN (NSM, 2016). The authentication process is based on the X.509 system. A symmetric encryption key is formed by applying public key cryptography (Cryptographic protocol, 2019). TLS is based on Secure Socket Layer (SSL) by further developing the protocol. SSL was published in 1995 but was broken in 2014, and rejected in 2015 through RFC 7568 (NSM, 2016). The newest TLS version is 1.3 and it was released in August 2018 (Transport Layer Security, 2020).

Chapter 3

3 Safety and security of ships

3.1 Safety and security

The Norwegian word *sikkerhet* translates to both safety and security. Safety is the protection against random incidents, meaning unwanted incidents happening as a result of one or more coincidences (Albrechtsen, 2003, s. 1). It is used to prevent accidents, and it protects from or makes it unlikely for injury, risk, or danger to happen. Loss due to a safety issue is usually related to human injuries or death, and reliability of industrial assets (Albrechtsen, 2003, s. 5). Considering code safety, the term is used to indicate that the software is safe and reliable to use (Foster, 2020). Security, on the other hand, is to protect an entity from threats like a possible attack or other crime (Security, u.å.). Such entities can be people, countries, organizations, buildings, or property. It is a measure to ensure that only authorized people have access to computer files. Security protects against intended incidents, meaning a wanted incident as a result of a deliberate and planned act (Albrechtsen, 2003, s. 1). Eirik Albrechtsen (2003, s. 7) has defined security as:

> A condition of being protected against planned, malicious and criminal incidents from a wide range of threats, where what is protected is all kinds of values to an organization/individual and incidents happen due to the wish for a wanted output/consequence for the attacker.

Loss due to a security incident is usually related to information and physical assets. According to Stuart Foster (2020), code security is to prevent illegal or unwanted activities in the software, which helps to ensure that the systems are secure during an attack, and it keeps unauthorized people from gaining access.

The knowledge about a risk's impact and the occurrence, can classify a risk. Risks can be either known or unknown. In 2002, there were not enough evidence to link the Iraq government to the supply of mass destruction weapons to terrorists. The former United States Secretary of Defense Donald Rumsfeld gave the following statement:

> ... because as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know. [...] it is the latter category that tend to be the difficult ones. (U.S. Department of Defense, 2002).

Table 1 shows four uncertainties that are important to manage. They are based on the knowledge of certainty and type of event (Fjelldal, 2018, s. 45).

<table>
<tr><td colspan="2" rowspan="2">Identification \ Certainty</td><td rowspan="2">Certain (Known)</td><td colspan="2">Uncertain (Unknown)</td></tr>
<tr><td>Impact</td><td>Occurrence</td></tr>
<tr><td colspan="2">Identified (Known)</td><td>Known known
(Identified knowledge)</td><td colspan="2">Known unknown
(Identified risk)</td></tr>
<tr><td rowspan="2">Unidentified (Unknown)</td><td>Consequence</td><td rowspan="2">Unknown known
(Untapped knowledge)</td><td colspan="2" rowspan="2">Unknown unknown
(Unidentified risk)</td></tr>
<tr><td>Event</td></tr>
</table>

Table 1 Schematic structure of modified risk categorization (Fjelldal, 2018, s. 45)

Known knowns is our knowledge and the risks we are fully aware of. These risks are possible to plan for in advance. Known unknowns are the risks you are aware that you do not know. It is the kind of risks that you know exist, but its potential impact is not known or fully understood. An example is a natural event, like an earthquake, which is unusually strong and in an unexpected location (Higgins and Perera, 2017).

Unknown unknowns are risks based on situations so unexpected that they would not be considered (There are known knowns, 2019). Basically, it is the risks we do not even know that we are not aware of, and which cannot be identified in advance. When such events occur, it can be identified and converted to a known unknown (Fjelldal, 2018, s. 46). The impact of a risk in this category can be serious and unexpected. As more unknown unknowns get identified, the likelihood that a surprise could affect something reduces. Unknown knowns are risks that exist and have been influencing us, but we are not aware of knowing them, do not realize their value, or refuse to acknowledge knowing them (Chalermpalanupap, 2014). It is possible the knowledge is repressed, suppressed, or forgotten.

A similar theory is Nassim Nicholas Taleb's Black Swan Theory. It is based on the presumption that black swans do not exist. Before it was sighted in Australia, all observations had been of white swans. It is about how unpredictable and rare outlier events can have extreme impact, and human's tendency to find simplified explanations for these events in retrospective (The Black Swan: The Impact of the Highly Improbable, 2020). Outlier can be explained as a data point that is significantly different than other observations (Outlier, 2020). There are three criteria that must be fulfilled for an event to be classified as a black swan (Fjelldal, 2018, s. 46):

The event comes as a surprise (to the observer)

The event has a major effect

After the first occurrence of the event, it is often rationalized by hindsight, like it could have been expected. The relevant data was available, but not accounted for in risk mitigation programs.

3.2 Vulnerabilities

There was a time when objects like toasters, refrigerators, cars, and vessels just performed the tasks they were originally designed to do. Today, they are also communicating with the Internet. The maritime sector has slowly realized that ships, as everything else, is now a part of cyber-space (Hopcraft and Martin, 2018). Cyber security cannot be an afterthought, it must be included in the architecture and planning of whatever is being developed, from the very beginning. There are multiple factors making cyber security difficult in the maritime industry. For instance, there are several different vessels which operate in different environments and have a tendency to use different computer systems. The systems are often built to last for many years, and as a consequence many are outdated and run operating systems that are no longer supported (Hopcraft and Martin, 2018). The modern maritime industry which uses IT systems in the operation of vessels, navigation, unloading and loading, communication, container tracking, cargo handling, and the computer systems used at ports and at shore, makes it more vulnerable to cyber-attacks. The consequences are no longer restricted to the vessel or cargo owner, but it can also affect other vessels. If a cyber-attack disables a vessel in the Panama Canal which blocks the Canal, it would affect the operation of nearby vessels with potentially huge losses (Bajraktari, 2019). It is more important than ever to address inherent vulnerabilities with the increased use of and reliance upon communication and digital technologies, in addition to integration of multiple electronic systems and advanced automation.

Sensitive information for a ship can include its position, cargo details, status of and readout from operational technology (OT), certificates, and authorizations. The CIA-triad can be used to assess the vulnerability and impact of (BIMCO mfl., 2016, s. 8):

> Confidentiality: Unauthorized access to information or data about the ship, passengers, crew, and cargo.
>
> Integrity: How the ship can continue safe and efficient operation after an unauthorized modification, where data and information has lost their integrity.
>
> Availability: Destruction of data and information or disruption to services results in loss of availability of data or information.

Human errors help attackers succeed in their attempts to gain access to a system. Futurenautics Ltd (2016) wrote that in 2015 60% of cyber-attacks were because of human failure. They did a survey of a crew consisting of 3000 people and it showed that 88% of them did not have any cyber awareness training (Futurenautics Ltd, 2016). Cyber security awareness training should be given to every employee. They should be trained and made aware of the cyber threats that exists. It will reduce the amount of attacks that are possible because of human errors.

Every company should perform a threat assessment that looks at potential and realistic threats they can be faced with. The maritime sector should look at the onboard procedures and systems regarding their robustness against the current threat level. Ship complexity continues to grow, and with that comes an increasing attack surface. In addition, ships become more connected to services provided from shore networks via the Internet (BIMCO mfl., 2016, s. 7). Figure 3 illustrates what a ship might look like to an attacker. Some digital onboard systems relevant to *Yara Birkeland* are explained below. Systems like passenger service and management systems, passenger facing public networks, and administrative and crew welfare systems are vulnerable onboard systems, but they are not relevant for *Yara Birkeland*.

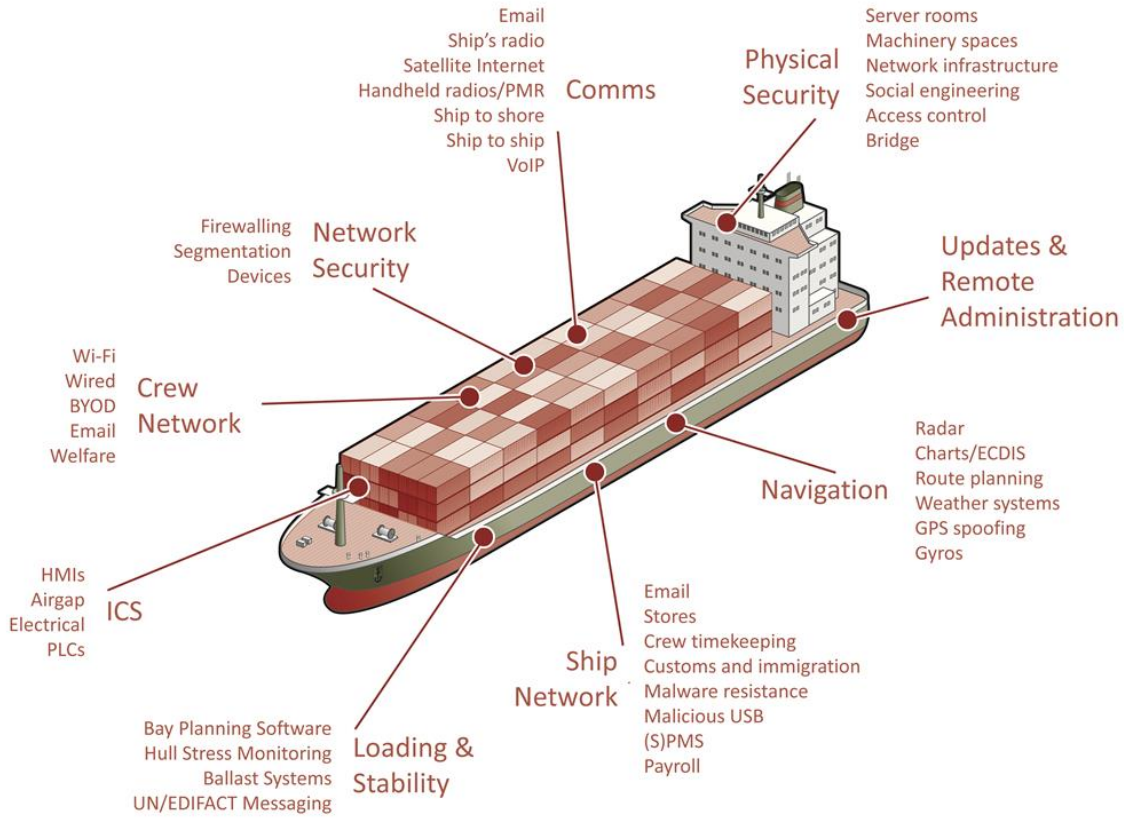

Figure 3 What a ship looks like to an attacker (Pen Test Partners, u.å.)

The environment involves two different categories of technology. Firstly, Information Technology (IT) where data is used for information. It can be networks, accounts, emails, electronic manuals, permits, and administration for instance. Secondly, Operational Technology (OT) is where data is used for industrial processes (Cassi, Cavanna, and Scialla, 2018). OT systems can be SCADA, ECDIS, AIS, GPS, dynamic positioning, remote support, onboard measurement and control, for instance (Fosen, 2019). A cyber-attack on IT-systems can hurt a company's reputation or finance, while an attack on OT-systems can result in consequences harming life, environment, or property.

Information and Communications Technology (ICT) is bringing the maritime industry into the 'digital ship' era (Lloyd's Register Group, 2018b). The term is an extension from IT and covers any product that will retrieve, store, manipulate, receive, or transmit information electronically in a digital form (Information and communications technology, 2020). On traditional ships, ICT and OT used be separated by several human-centered processes and therefore allowed for a step by step approach to cyber ICT security (Lloyd's Register Group, 2018b).

Bridge systems are vulnerable to cyber-attacks, because navigation systems are digital, connected to a network, and has interfaces to networks ashore to perform updates and provision of services (BIMCO mfl., 2016, s. 7). Bridge systems that are not connected to other networks can be equally vulnerable. They often get updates through removable media from other controlled or uncontrolled networks. Results of a cyber event can be service manipulation or denial, affecting all associated navigation. This includes AIS, ECDIS, VDR, GNSS, Radar, GPS, and ARPA. They have significant cyber security vulnerabilities (Lloyd's Register Group, 2018b). These navigation systems do not have any method for authenticating or encrypting signals. The systems are often operated with administrator rights and without the need to enter a password (Cassi, Cavanna, and Scialla, 2018). They are for example susceptible for jamming.

Another bridge system is the Voyage Data Recorders (VDR). It can be compared to an airplane's black box. It collects data from different maritime systems for incident reporting. They have vulnerabilities like weak encryption, authentication, firmware update mechanisms, and other dangerous software vulnerabilities (Jones and Tam, u.å.). An attack can result in broken or missing data. A VDR might be able to save relevant data for cyber investigations in the future (Jones and Tam, u.å.).

GNSS is short for Global Navigation Satellite System and it utilizes multiple satellites for global positioning data. It is one of the most complex systems on modern bridges (Jones and Tam, u.å.). GPS is a GNSS system (European Global Navigation Satellite System Agency, 2017). Its signals have low energy and a simple overload or solar activity can make a significant impact. If GNSS is affected, it can result in failure of other systems, like AIS. Possible attacks with limited effort are jamming and spoofing. They are also vulnerable to package modification and MitM attacks.

AIS is short for Automated Identification System and it is a mandatory vessel tracking system for all passenger and commercial ships over 300 tons. It works by acquiring GPS coordinates and exchanging a vessel's identity, position, course, navigation status, and some other information, with nearby vessels, offshore installations, and base stations (Jones and Tam, u.å.). The information is broadcasted through maritime radio or satellite. Normally, a combination of GPS and VHF-radio communication is used (Jones and Tam, u.å.). AIS signals are relied upon to avoid collisions and for situational awareness. It is also used at the Vessel Traffic Service, for search and rescue operations, and accident investigations. Automated Identification System is vulnerable to many attacks.

There is a known weakness in the signals and protocols used to send data. Both implementation-based and protocol specific attacks are possible (Balduzzi, 2014). AIS does not have any authentication or integrity checks (Bothur, Valli, and Zheng, 2017). It makes it possible to create fake vessels, hijack communication of existing vessels, modify ship details, spoof signals, permanently disable AIS tracking, and trigger false SOS or collision alerts (Pole Star, u.å.). Since AIS data is transmitted through VHF-radio, it is received by anyone with an AIS receiver. Consequently, it could be exploited by criminals, pirates, or other attackers to gain information about the location of specific ships and cargo. Another possible consequence is to lose availability. In high-density areas where lots of ships transfer AIS messages, it is a challenge to efficiently collect, process, and download them all. It results in the loss of many messages due to data collision. Research has indicated that satellite AIS receive less than 50% of messages in medium to high density areas (Pole Star, u.å.). Providers have to clean or "de-collide" the data, which adds a significant latency to the delivery of messages. An attacker can exploit this vulnerability by launching a flooding attack. There are no validity checks included (Balduzzi, 2014). Therefore, it is possible to send an AIS message from any location for a vessel at another location. Another vulnerability is the lack of timing checks. Timestamps are not included in the messages which makes it possible to replay valid and existing AIS information. In addition, GPS failure/poor transmission (due to the nature of the system or installation), AIS malfunction (due to the nature of the system), AIS bit errors (due to the nature of the system), and data diddling (due to message modification) can affect availability and/or integrity (Craiger, Haass, and Kessler, 2018). Based on the content of AIS data, criminals and terrorists are probably most interested in performing an attack. It might also be interesting for competitors and activists. The probability of getting caught is lower if the attacker is able to confuse or hide their activities, by for instance a DoS attack on the surveillance (Jones and Tam, u.å.). There are no easy-fix mitigations for the AIS problems because they also exist in the core of the protocol. Future versions should include validity and authentication checks and encryption.

Electronic Chart Display and Information System (ECDIS) is an alternative to paper nautical charts. It is an electronic navigational chart system, which provides geographic information. In order to pinpoint the navigational points, ECDIS uses GPS and it interfaces with other navigational equipment like RADAR, ARPA, etc. (Bhattacharjee, 2019). The system needs to update its maps and sometimes this is accomplished by physical access through a USB stick to upload them (Cassi, Cavanna, and Scialla, 2018). An attacker could exploit the vulnerability by infecting the USB device.

Communication systems is another system onboard. The vulnerabilities of a ship increase because of the availability of Internet connectivity through satellite and other wireless communication (BIMCO mfl., 2016, s. 8). It includes satellite and terrestrial radio communication, and data communication (voice over IP, broadband, e-mail, and Internet access) (Lloyd's Register Group, 2018b). Unmanned vessels are more dependent on satellite-based communication to send and receive operational commands and data from sensors. They are especially vulnerable for Denial-of-Service, package modification, and Man-in-the-Middle attacks.

Control systems use control loops to manage, direct, command, or regulate the behavior of other devices or systems (Control system, 2020). It can be used for industrial control systems which control processes and machines. Onboard a vessel, it is used to control electromechanical systems like generators, main engine, ballast tanks, fuel and oil pumps, life support, fire alarms, power management, environmental control, and cargo hold fans, among others (Lloyd's Register Group, 2018b). Digital systems are used to control and monitor them and therefore they become more vulnerable. Their vulnerability increases when they are used with remote condition-based monitoring, and when they are integrated with communication and navigation equipment (BIMCO mfl., 2016, s. 7).

Supervisory Control and Data Acquisition (SCADA) is a control system used to control and monitor physical processes. It contains network data communications, computers, graphical user interfaces (GUI), and peripheral devices like programmable logic controllers (PLC) (SCADA, 2020). SCADA is used to analyze and monitor real-time data, interact with devices, control local and remote industrial processes, and log data and events for auditing and other purposes (Brook, 2018). Everything from power plants and water distribution to traffic lights uses SCADA systems. They were designed to be easily repaired and operated, open, robust, and not necessarily secure (SCADA, 2020). Security and authentication were not a concern during the design phase. As the systems get interconnected with the Internet and office networks, they become vulnerable to network attacks that are common in computer security, like downloading sensitive information and buffer overflow (SCADA, 2020). On modern ships, most installed machinery and systems are monitored and controlled by SCADA systems. They transfer data from sensors to processing units where sensors and control electrical, mechanical, and hydraulic components and actuators are combined (Cassi, Cavanna, and Scialla, 2018). The Human-Machine Interfaces (HMI) allow humans to interface with processes and machinery. It is used to inform an operator. Modern SCADA systems have many threat vectors. Vulnerabilities can be found in the HMI, mobile applications, web interfaces, protocols, and other components (Trend Micro, 2019). Critical processes often use SCADA systems which means that a weakness could cause severe real-world consequences. There are several examples of attacks against SCADA systems. The Stuxnet worm in 2010 is a well-known attack. It used weaknesses found in SCADA systems to target industrial facilities. Power outages were caused in Ukraine in 2016 by a malware called Industroyer (Trend Micro, 2019). In 2017, a Trojan Triton was discovered in the Middle East which targeted industrial safety systems and caused shutdown of the operations (Giles, 2019).

Internet of Things devices are according to (Cassi, Cavanna, and Scialla, 2018) "defined as the cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decisions." Interconnected networks of IT and cyber-physical systems using wireless and computer-based SCADA systems are parts of the cyber environment (Cassi, Cavanna, and Scialla, 2018). Tiers and loaders including cranes, winches, and similar mechanisms for physical operations, are especially relevant for *Yara Birkeland*. Exploitation can result in stealing, smuggling, physically interact with, or damaging nearby things. Vendors are assessing the risks and developing external SCADA monitoring and recording equipment, specialized industrial firewall and VPN solutions for TCP and IP-based networks (SCADA, 2020). According to Wikipedia, SCADA systems for electricity and gas addresses the vulnerabilities of wired and wireless communication links by using authentication and AES encryption (SCADA, 2020).

Another control system is access control systems. They are used to support access control digitally. It is to ensure both physical security and safety of a ship and its cargo. This includes security alarm, surveillance, and electronic “personnel-onboard” systems (BIMCO mfl., 2016, s. 7).

Equipment used by charters include survey equipment like SONAR, and seismic survey systems, IP ports and wireless access points, and phones (Lloyd’s Register Group, 2018b). Technologies like SONAR is used to detect object’s position under water by sending and receiving signals. Such technologies share vulnerabilities that can be exploited with a DoS-attack. For unmanned vessels, it may result in humans being locked out and unable to help, or that it is not possible to distinguish between which sensors are compromised, and which, if any, are still receiving reliable data (Jones and Tam, u.å.).

Cargo Management System is another example of an onboard system. It is a digital system that is used for management and control of cargo and can be interfaced with systems ashore (BIMCO mfl., 2016, s. 7). A system can be shipment-tracking tools that the shipper can access via the Internet. Interfaces like that make cargo management systems and data in cargo manifests vulnerable to cyber-attacks (BIMCO mfl., 2016, s. 7).

Systems can affect each other in unforeseen ways, which could potentially be harmful. Some vulnerabilities are not present in a particular system but can be exploited when systems are interconnected. Every computer can be infected with malware. Every computer can be commandeered with ransomware. Every computer can become a part of a botnet. Every computer can be remotely wiped clean. Attackers can take advantage of IoT devices in all the same ways they can exploit laptop and desktop computers (Schneier, 2018, s. 26). Bruce Schneier (2018, s. 211) used multiple pages to explain resilience in his book Beyond Fear from 2003: “Good security systems are resilient. They can withstand failures; a single failure doesn't cause a cascade of other failures. They can withstand attacks, including attackers who cheat. They can withstand new advances in technology. They can fail and recover from failure.” In the context of technology and tactic, resilience means a lot of different things, multiple layers of defense, redundancy, isolation, and so forth. Even with every precaution taken care of and thoroughly developed cyber security strategies in place, you might suffer a breach someday.

3.3 Threat actors

A threat actor or threat agent is an individual or a group with the potential to impact the safety or security of another entity (Threat actor, 2020) – someone posing a threat. In this case, it is a threat or malicious actor that can impact the security or safety of *Yara Birkeland*. It is normally used to describe someone performing or that could perform malicious acts against an organization. A threat actor performing cyber-attacks can be nation states, criminals, individuals, activists, or competitors. They have the skills and resources necessary to threaten a ship's safety and security, and the company's ability to continue their businesses (BIMCO mfl., 2016, s. 3). The categories unintentional/intentional and external/internal, mentioned in section 2.3.4, are often used to categorize a threat actor (Threat actor, 2020). Some threat actors relevant for the maritime sector are explained below.

Activists are often referred to as hacktivists, and a well-known group is Anonymous. Included in this category is unsatisfied employees. Their motivation is disruption of operations and reputational damage (BIMCO mfl., 2016, s. 3). Objectives for an attack can be publication of sensitive data, destruction of data, denial of access to the targeted system, or media attention (Monogioudis, 2019). *Yara Birkeland* might draw attention from activists. It can for instance be to make a statement about Kongsberg's military division, more specifically their development of weapons. It is less likely it will be targeted for environmental reasons since the vessel will have zero emission and be electric.

Criminals are motivated by things like industrial and commercial espionage, and financial gain. They might use blackmail and extortion through ransomware, and threats of Denial of Service attacks (Boyes and Isbell, 2017, s. 35). We have recently seen this in the LockerGoga attack against Hydro. Criminal's objectives for an attack is to sell or ransom stolen data, gathering intelligence for more sophisticated crime, exact location of cargo, ship handling and transportation plans, ransoming system operability and arranging fraudulent transport of cargo (Monogioudis, 2019). It might not be so attractive for criminals to use *Yara Birkeland* for transportation of illegal goods since it will only move between Herøya, Brevik, and Larvik. When autonomous vessels start going international, it will undoubtedly become an interesting target for criminals. That being said, criminals can target the vessel for other purposes.

Nation states, state sponsored groups, and terrorists are motivated by espionage and political gain. Gaining knowledge and disrupting economies and critical national infrastructures can be their objectives (BIMCO mfl., 2016, s. 3). Terrorists have already started using the Internet for their advantage when distributing propaganda and for communication purposes (Boyes and Isbell, 2017, s. 36). They can be able to enter the cyber-criminal market by support of nation states or by services offered by cyber-criminals. It can be used further by encouraging internal members to adopt the attacks or methods (Boyes and Isbell, 2017, s. 36). There are various toolkits available that can potentially be used to damage or disrupt ships by attacking either the ship itself or connected shore-based systems. Since *Yara Birkeland's* short, costal route is not a known target or location for terrorists and it is close to local authorities, it might not draw much attention from terrorists, neither domestic or foreigners. On the other hand, narrow canals can raise the possibility of land-based attacks or cause collision with other vessels or natural obstacles. Terrorists might crash the vessel into other boats/ships, but it is unlikely that crashing the boat on the shore will make enough damage for terrorists. There is no secret that some nation states are actively involved in cyber-attacks on a wide range of

organizations. They use the attacks to gather secrets of another state or other sensitive commercial information and intellectual property, or to influence a nation's political process (Tollefson, 2019). Some nation states have threatened the availability of critical infrastructure like the energy sector. Nationally motivated cyber fighters can be sponsored by a nation state.

Commercial competitors consist of corporations wanting to create a competitive advantage. It is usually by large corporations. They can act directly or through third parties, with the aim of harming a rival by collecting business intelligence, stealing intellectual property, gathering competitive intelligence on bids, or disrupting operations to cause financial or reputational loss (Boyes and Isbell, 2017, s. 35). The Yara Birkeland project gets attention from all over the world, which means both commercial competitors and nation states are aware of this project. Since it is the first of its kind, they might want to gain more knowledge about it through inside and sensitive information.

How severe and sophisticated the threats of an individual is, depends on his/her capabilities. An individual can for instance be a 'script kiddie' or an insider. The goal of a threat actor in this category can vary a lot. Maybe he/she wants to steal or leak sensitive information, disrupt or sabotage a ship's operation, or maybe he/she just wants to prove their skills. An insider is any person that exploits their legitimate access to an asset to cause harm or loss to the business. It can be a current or former employee, consultant, or another person who has or has had access to the company's information, objects, or other assets (NSM, 2019a, s. 18). Since insiders are familiar with the systems, they are often able to bypass most of the implemented security mechanisms. 'Script kiddies' is used for an individual hacker with limited knowledge who uses techniques and tools developed by other people and which are available online (Boyes and Isbell, 2017, s. 35). The potential damage an individual can cause depends on several factors like IT skills, cyber security measures implemented, and system access rights.

3.4 Attacks

Although many companies choose to keep information about cyber-attacks secret, there are incidents that can be found in the media. These are some of the well-known incidents from the past decade (Lloyd's Register Group, 2018a):

2010: Oil platform shutdown by malware hitting their industrial control system.

2011: Hackers target IRISL, resulting in damaged cargo numbers and destinations. IRISL is the maritime fleet of the Islamic Republic of Iran Shipping Lines (IRISL Group, 2020).

2012: Malicious GPS signals affect over 100 oceangoing vessels.

2014: GPS jamming against US shipping port, resulting in shutdown.

2016: Ransomware hits bulk carrier SWB and results in shutdown (Fosen, 2019).

2017: 'NotPetya' ransomware hits the maritime industry.

2018: Cyber-attack against COSCO resulting in 'network breakdown'.

In 2017, 'NotPetya' became well-known across the globe. It was an untargeted ransomware that hit shipping giant Maersk hard (Lloyd's Register Group, 2018a). The ransomware impacted most of their important systems. Consequently, every critical function for the organization was disrupted. According to Lloyd's Register Group (2018a), as many as 45 000 PCs and 4 000 servers were infected, resulting in shutdown of 76 global port terminals. It was an aggressive and damaging ransomware. Once access was gained, it used highly advanced infiltration and lateral movements to infect systems and gain persistence in the network (Lloyd's Register Group, 2018a). The access to the device and its functions were locked-down and payment of cryptocurrency was demanded. It has been associated with cyber-warfare around Ukraine and was probably because of conflicts between Ukraine, Russia, and NATO (Lloyd's Register Group, 2018a). UK and US law enforcement forces said that the attack was launched by some state-funded actors of Russia (Goud, u.å). 'NotPetya' got access to Maersk through a local accounting software package (Lloyd's Register Group, 2018a).

About a month later, in July 2017, the BW Group was attacked. BW Group is one of the largest shipping companies in the world (Mohindru, 2017). There are not many details about the incident, just that a hacking attack had happened. It resulted in gained access to their computer systems. It affected Group Policy Object (GPO) and Active Directory (AD) systems and caused both intranet and Internet to be closed down temporarily (Mohindru, 2017). BW Group says that it was not a ransomware attack as Maersk had experienced.

On the 24th of July 2018, COSCO was hit by a cyber-attack (Safety4Sea, 2018). It affected their operations in the US. The attack affected COSCOS' digital assets and forced them to shut down connections to regions outside of the US, and disable their telephone and email systems (Goud, u.å). The company said their vessels were not impacted by the attack and only COSCO's terminal at the Port of Long Beach was affected, meaning their main business operation systems continued to perform stably (World Maritime News, 2018). It could have been a ransomware attack, but it has not been confirmed.

Only after a few weeks in 2020, a cyber-attack against the maritime sector was identified. The London Offshore Consultants were hit by a cyber-attack (Safety4Sea, 2020). There has been an increasingly number of attacks against OT systems the last decade. It can be seen figure 4 made by AV-TEST Institute, Germany & IBM Managed Security Services (Fosen, 2019). The left shows malware against IT systems and on the right, there are attacks against OT systems.

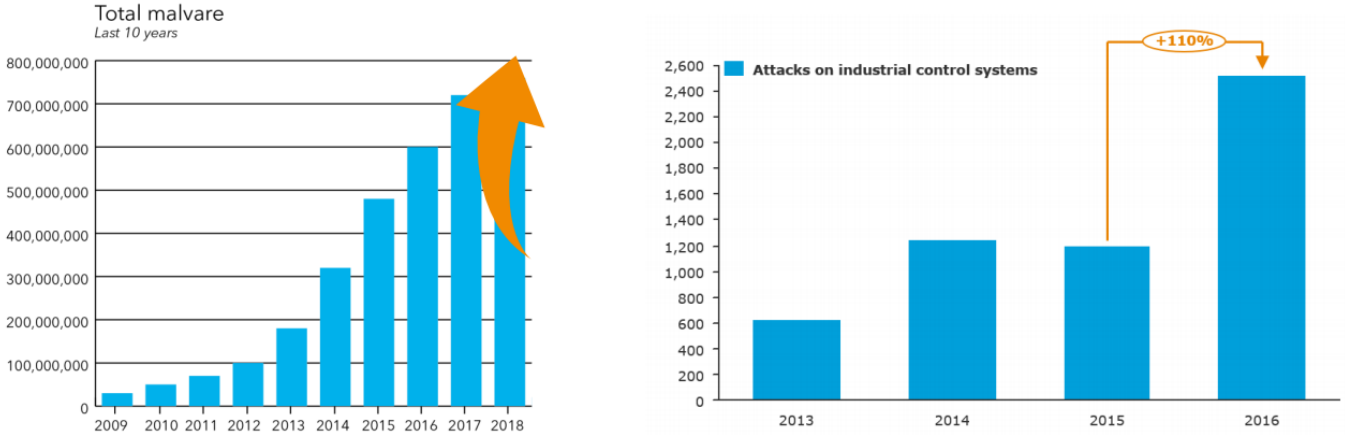

Figure 4 Attacks against IT and OT the last decade (Fosen, 2019)

3.5 Cyber security work

Cyber insecurities cost a lot of money. It is hard to get correct numbers on exactly how much it costs, but there are some estimates. It was concluded that one in four companies will be hacked with an average cost of $3.6 million each in a report from Ponemon Institute from 2017 (Schneier, 2018, s. 102). A report from Symantec estimated that 978 million people in 20 countries were affected by cybercrime in 2017, at a cost of $172 billion (Schneier, 2018, s. 102). Luckily, cyber security is a topic with a lot of ongoing research and development. Governments, companies, and organizations around the world are working to improve the cyber security.

The Council of Europe has developed a Convention on Cybercrime called the Budapest Convention. It is the first international treaty on cybercrime and provides a framework for international police and judicial cooperation (Schnieier, 2018, s. 157). The Budapest Convention has been ratified by 64 countries, though not by significant players like China, Russia, India, and Brazil (Council of Europe Portal, 2020).

Barack Obama, the previous President of the United Stated, issued an Executive Order on the 12th of February 2013 to improve the cyber security of critical infrastructure (Cassi, Cavanna, and Scialla, 2018). A voluntary, risk-based cyber security framework needed to be developed to enhance resilience and security, and it should follow best practice and industry standards. The private sector and the government collaborated to create the framework. It was issued by NIST (Cassi, Cavanna, and Scialla, 2018). In order to make cyber security an integrated part of the risk management process, it focuses on the use of business drivers.

In Europe a Network and Information Security (NIS) Directive was issued, which was by the Council of the European Union and the European Parliament (Cassi, Cavanna, and Scialla, 2018). They wanted to ensure that information systems and networks across Europe keep a high common level of security. The initiatives were because countries recognized that the critical infrastructures make wide use of an amount of communication and digital technologies and they require security measures. One of those critical infrastructures is the water transport sector, which includes seagoing traffic and port operations (Cassi, Cavanna, and Scialla, 2018).

In May 2018, the General Data Protection Regulation (GDPR) came into force. From now on, all security breaches involving other people's data is required to be reported to the authorities within 72 hours (Cassi, Cavanna, and Scialla, 2018). However, an early detection is difficult. It is legally required to have an incident response plan. GDPR also require organizations holding data from EU subjects to have an effective response plan in case of a data breach in order to contain damage and prevent future events (Cassi, Cavanna, and Scialla, 2018).

The need for improved cyber security in the maritime sector has been recognized by the International Maritime Organization (IMO). They have issued a guideline called Guidelines on maritime cyber risk management, which provide recommendations on how to be better protected from current and emerging cyber vulnerabilities and threats (International Maritime Organization, u.å.). It is possible to incorporate it into the company's existing risk

management process. This guideline follows the cyber security lifecycle that is outlined in the NIST cyber security framework. It recommends the following actions (Cassi, Cavanna, and Scialla, 2018):

> Identify: Define roles and responsibilities for cyber risk management, and also identify data, assets, capabilities, and systems that pose risks to the shipping operations if they are disrupted.
>
> Protect: Implementation of risk control measures and processes, and contingency planning to protect against a cyber event and ensure the continuity of shipping operations.
>
> Detect: Develop and implement necessary measures for fast detection of cyber events.
>
> Respond: Activities and plans need to be implemented to restore and provide resilience to systems necessary for shipping services or operations affected by a cyber incident.
>
> Recover: Measures to restore and back-up essential systems impacted by a cyber incident needs to be identified.

IMO altered two of their security management codes in 2017 in order to explicitly include cyber security. It was International Security Management Code (ISM) and International Ship and Port Facility Security Code (ISPS) which describes how risk management processes should be conducted by ship and port operators (Hopcraft and Martin, 2018). The International Maritime Organization has given ship owners and managers until January 1st, 2021 to include risk management for cyber security and make it an integrated part of the ship's safety and security (Hopcraft and Martin, 2018). To be specific, the amendments to ISM and ISPS regarding cyber-security are also included in the deadline. There is a risk of having the vessel detained if it is not included.

BIMCO stands for Baltic and International Maritime Council and has over the years taken a role in researching the potential risks associated with the increasing amount of technology onboard ships. The company collaborated with other leading shipping organizations to launch a set of cyber security guidelines for ships. It was launched in July 2017 with the intention of helping the global shipping industry to prevent future events caused by cyber incidents onboard a vessel (Lloyd's Register, u.å.). Events could for instance be related to safety, commercial, or environmental reasons.

Nippon Kaiji Kyokai is a Japanese ship classification society and is known as ClassNK (ClassNK, u.å.). They are actively involved in many areas of the maritime sector. Ensuring safety of property and life at sea and preventing pollution of the marine environment are important to them, and in order to achieve this they develop classification services, procedures, guidance, and relevant rules (ClassNK, u.å.). They also continue their technological and scientific research and development. ClassNK know that cyber security is a big threat now. In a press release in March 2019, they said:

> In the ClassNK Cyber Security Approach, ensuring navigational safety is regarded the most important goal of onboard cyber security. To achieve it, it is of high priority to ensure availability of systems in terms of operation technology (OT) as well as information technology (IT) systems, which support operation of ships (Lo, 2019).

ClassNK have developed a five layered cyber security approach with a combination of technical, physical, and organizational measures. The first three layers are hardware and software equipment controls, operational controls to ensure the health of equipment controls, and controls to ensure the health of operational controls (Lo, 2019). It is to secure potential vulnerabilities of onboard systems and to confirm that protocols are running as they should. The electronic systems onboard are categorized into three categories where Category 1 systems are not directly related to the safety of the vessel, crew, or environment, Category 2 systems could eventually lead to dangerous situations, and Category 3 systems could present an immediate threat to human life, vessel safety, and the environment (Lo, 2019). The latter includes dynamic positioning, navigation systems, and steering control. The fourth layer is organizational controls for onboard systems. For a ship and company to ensure safety, it needs a good cyber security management. This fourth layer includes activities to maintain, establish, and continually improve the system, and the goal is to assess all identified cyber risks to crew, ship, and the environment, provide a safe working environment, and continuously improving personnel's cyber security management skills (Lo, 2019). Lastly, the fifth layer is to reduce the cyber risks of shipboard products. Important aspects are to reduce the attack surface of software architecture, eliminating unnecessary software privileges, establishing secure defaults, and keeping the system as simple as possible (Lo, 2019). ClassNK mean it is as important for the software to be resilient against external threats, as its intended functions. This layer is also for the equipment supply chain, meaning the shipboard equipment manufacturers and personnel involved in equipment acquisition.

Chapter 4

4 Autonomous vessels

4.1 Autonomy

Autonomy has had several interpretations in different areas during history. The terminology is used in psychology, philosophy, political science, and technology. According to Store Norske Leksikon, autonomous means self-governing (Gisle, 2019). It is being independent and having the power to make your own decisions. In regards of a system or machine, it is about being able to operate without the direct control of humans (Autonomous, u.å.). In a technological perspective, autonomous technological systems are able to demonstrate free will to a certain level by making its own decision without an operator or external system having to be involved (Fjelldal, 2018, s. 5). The decisions are about which actions to perform for different tasks. Torgeir Fjelldal (2018, s. 6) writes about certain capabilities a system has to possess in order for it to be autonomous:

> Learning: Improvement through practice, experience, or by teaching.
>
> Reasoning: Generate conclusions from available knowledge.
>
> Planning: Construct a sequence of actions to achieve a goal.
>
> Decision making: Select a course of action among several alternative scenarios – including a perception of expected outcome.
>
> Situational awareness: The ability to perceive its surroundings.
>
> Actuation: The ability to physically interact with its environment.
>
> Human Machine Interface (HMI): How the autonomous system interacts with humans.

There are some processes that can be difficult to distinguish, among them are autonomy and automation. An automated system is often pre-programmed and digital, and operates in structured, known, and repetitive environments. Even though the tasks are executed without a human controlling it, its capabilities are very limited and cannot handle unforeseen situations and changes to the environment (Fjelldal, 2019). Autonomous systems have the capability to sense their surroundings and finding out how to solve problems and issues they will be faced with. These systems have automated functions embedded in them (Fjelldal, 2019). That makes an autonomous vessel a vessel with some level of autonomy. Maritime Autonomous Surface Ship (MASS) is a terminology used for any autonomous ship (Nordahl and Rødseth, 2017). A system can operate with different levels of autonomy which can be found in chapter 7 in the second part of this thesis.

4.2 Remote controlled and autonomous vessels

Before I continue, I would like to clarify the difference between remote controlled and autonomous vessels. Remote controlled ships will be unmanned, smart, and have autonomous elements, but they are controlled from a Shore Control Center. These vessels will be closer to traditional ships in regards of regulations and legislations. The ship and SCC will be connected wireless. Employees in SCC receive all information and data from radar, sensors, satellite, and other systems onboard (Deketelaere, 2017, s. 2). They will interpret, make decisions, and aid the ship to its destination. Smart ships use machines and systems, but humans have the last words and makes the decisions, while autonomous ships are operated by machines and systems that makes their own decisions.

4.3 Vessels

There is a rapid evolvement in the use of autonomous systems in the maritime shipping industry. Giving the shipping industry systems that are able to make their own decisions and performing actions in cooperation with or on behalf of a human. This opens up the possibility of unmanned and autonomous vessels. Unmanned vessels come with many advantages – massive amounts of data from equipment onboard, improving the crew's health who would normally be isolated for a long time and having to work in extreme conditions, money and space can be saved on crew facilities which results in more space for cargo, less weight and air resistance, and less fuel is needed. Most of the autonomous projects under development are going to use sustainable energy. Climate and pollution are hot topics these days and it is a big advantage if these ships can contribute to a greener industry.

It is difficult to foresee exactly the benefits unmanned and autonomous vessels will bring. However, they will need to be at least as safe as conventional vessels. Human error is likely the reason for most maritime accidents. A research from March 2017 analyzed 100 accidents that happened between 1999 and 2015. It showed that the likelihood of collisions or groundings would have been significantly less if the vessel had been unmanned (Matthews, 2017).

The introduction of autonomy into the maritime world brings some additional challenges. It is important to consider the constrains. Some constrains defined in (Fjelldal, 2018, s. 30) are mentioned below. These mostly have a technical point of view, but it is also important to be aware of other relevant areas where challenges may occur.

Always on – the ship has no "safe state".

High reliability – the system must behave according to the operation's intentions.

Unreliable communication – handle limited or dropouts when communicating with an operator.

Unstructured environment – the ship must be able to avoid collisions in complex environments.

Own energy-supply – the ship must be in control of own energy production and consumption.

Cost focus – solutions must be efficient and have a low risk during development and use.

Time focus – well known methods that work now are better than unknown methods that might not work at all.

Specific operations will be more sensitive to disturbance, latency, malfunctions, or other vulnerabilities in the data communication, and it is therefore extremely important that the connectivity between SCC and the vessel is available with the required capacity (Fjelldal, 2018, s. 46-47). Even though sensors onboard the vessel will provide a lot of information regarding the real-time situation of the ship's condition, it might not be able to give the operator in SCC the same perception as if he/she was physically present. For instance, some maneuvering decisions are based on the behavior of the ship, like rocking, and the captain's experiences with the vessel (Fjelldal, 2018, s. 47). A captain's experiences and interpretations can be difficult to recreate. The huge amount of data can work against its intentions. Fusing large amounts of data from different sensors can lead to an overwhelming amount of information for the operator, resulting in an increased possibility for inaccurate decisions or important information is overlooked.

Delay and up time can affect the efficiency of a vessel and put the safety at risk. These are critical factors. For unmanned vessels, the time it takes for a signal to travel between the vessel and operator through satellites or by other means, has to be minimal. The onboard systems for navigation, collision avoidance, and situational awareness must always be reliable to ensure safe operations and to achieve a well-functioning, highly automated vessel. Increasing the amount of software-based systems makes the vessel more vulnerable to system failure. For the operating system of conventional computers, errors introduced through software repair, updates, and revisions, might have insignificant impact for a user. When it comes to autonomous vessels, these errors can have major consequences during operation. They can impact the performance of the system immediate or later.

With a higher amount of connected onboard information and ICT systems, there is always a risk of unauthorized people trying to access the systems with malicious intentions. Concerns about the vulnerability of unmanned vessels regarding hijacking, piracy, and cyber-attacks are understandable (Jalonen, Tuominen, and Wahlström, u.å., s. 60). Breaches have been made of autonomous road vehicles and in other fields of new technology. There have been raised questions whether such systems can effectively resist cyber-attacks with a malicious intent, launched remotely through the ICT infrastructure. Any protection against cyber related threats needs to include elimination of vulnerabilities in the ICT infrastructure, and implementation of effective security measures for intrusion prevention, detection, damage control, and safe recovery in case the implemented prevention measures fail (Jalonen, Tuominen, and Wahlström, u.å., s. 66). It is important that every security measure is persistent, dynamic, and can resist the attackers even when their skills and techniques evolve. Some cyber security methods that are foreseen to be needed for autonomous vessels are data encryption, classification, protection against unauthorized use, integrity protection, user authentication, authorization and identification, activity logging, auditing, and connectivity protection (Jalonen, Tuominen, and Wahlström, u.å., s. 66). A couple of functions that must be performed on a ship, and therefore also unmanned ships, in regards of security are access control for passengers and crew, network firewalls and data protection for onboard security,

and monitor and control attempts to board or otherwise interfere with ship operations for antipiracy (Nordahl and Rødseth, 2017).

The problem domain that all control and monitoring functions in the system need to be able to handle is defined in the Operating Design Domain (ODD) (Nordahl and Rødseth, 2017). The maneuverability of the ship, environmental conditions, expected contributions from any humans, and complexity of the operation are defined. Other functions like the capabilities of situational awareness, sensors, and navigation are also specified (Nordahl and Rødseth, 2017). An autonomous vessel is restricted to operate under equal or less complexity, not higher. However, it is not possible to always guarantee that the conditions will stay between the limits defined in ODD. Sometimes exceptions like sudden weather changes or technical failure occur. A Dynamic Navigation Task (DNT) Fallback needs to be defined to take care of such situations and bring the ship to a situation as safe as possible under the given circumstances (Nordahl and Rødseth, 2017). Tasks assigned to the onshore or onboard automation system is defined in the automatic DNT. For instance, requirements for object detection and classification, sensor systems, and anti-collision systems are defined here. Tasks assigned to the operator is defined in the Operator Exclusive DNT (Nordahl and Rødseth, 2017).

Two mobile teams, the On-board Control Team (OCT) and Emergency Control Team (ECT), are able to enter the ship in particular situations (Nordahl and Rødseth, 2017). A certain situation can be after a critical breakdown of some ship systems or to take a ship into/out of a port. The OCT team is only appropriate for periodically unmanned ships (Nordahl and Rødseth, 2017) and will therefore not be appropriate for *Yara Birkeland*.

The Norwegian Forum for Autonomous Ships (NFAS) has defined some common maritime entities that any ship must relate to in Definitions for Autonomous Merchant Ships (Nordahl and Rødseth, 2017). There might be other external entities that a ship needs to relate to, depending on the type of ship and geographic location.

> Vessel Traffic Service/Ship reporting areas: where the ship needs to contact a shore operator for guidance or reporting.
>
> Aids to Navigation and AIS*:* systems providing real-time information about other ships or the fairways.
>
> Maritime Rescue Coordination Center and Global Maritime Distress and Safety System*:* radio services used for ships in distress or emergencies. Autonomous ships may also need to use them and are required to respond.
>
> Other ships: VHF data communication system and AIS can be used to communicate with other passing ships.
>
> Pilots, tugs, and linesmen: will communicate with the ship to provide mandatory or requested services.
>
> Port services: logistic and supply services in port will have to be arranged, including any automatic mooring systems and electrical connections.

In the Definitions for Autonomous Merchant Ships (Nordahl and Rødseth, 2017), there are mentioned some optional shore infrastructure in areas that autonomous ships operate. In certain high traffic areas or ports, a Local Monitoring Service can be used. It is an automated and voluntary information management system and could distribute information about current traffic and weather conditions to the ship. It could also send information about the ships' activities to other vessels in the area (Nordahl and Rødseth, 2017). Operations in areas where there is sufficient shore coverage, Shore Sensor System can partly replace or complement ship sensors. It can give better instruments, locations, or overlapping sensor coverage (Nordahl and Rødseth, 2017).

Autonomous and unmanned vessels must link its communication equipment to the SCC in order to facilitate the voice communication present in the shipping sector. The bridge, in this case in a Shore Control Center, needs to be able to communicate with other ships and shore entities. A possibility is to connect the SCC directly to other shore entities or ships through digital communication since SCC will often be located on land and have communication lines with high capacity (Nordahl and Rødseth, 2017).

4.4 Safety and security of unmanned and autonomous vessels

The safety issues an autonomous vessel will face, are most of the same threats as conventional vessels regarding other vessels, the sea environment, and its own operation. Mitigation strategies for these areas are well defined (Fjelldal, 2018, s. 46). When it comes to security threats related to marine transport, theft of cargo, piracy, human trafficking, smuggling of goods, sabotage and vandalism, damaging of port facility or ship, use of ship as weapon for terrorist activity, and hijacking of ship or persons onboard are frequently listed (Jalonen, Tuominen, and Wahlström, u.å., s. 65). New safety and security risks and hazards regarding the operation of autonomous vessels are expected to appear. Some or maybe even most of the new risks and hazards can be predicted, but the deployment of new technologies can create unexpected events – unknown unknowns and black swans (Fjelldal, 2018, s. 46).

Cyber-attacks against autonomous vessels are expected to be a serious concern and one of the largest known risks. It can have major consequences if any unauthorized gets access to huge amounts of connected onboard ICT systems. Cyber security measures should be implemented to protect systems from theft and damage to their software, hardware, or information, and from abuse or disruption of the services they provide (Fjelldal, 2018, s. 48). It could result in annoyance or demonstration by changing maneuvers or grounding or colliding into a vessel causing serious damage. Attackers can also cause damage without having access to the onboard systems. The AIS or GPS data link between the Shore Control Center and vessel can be jammed for instance.

References

Albrechtsen, E. (2003) *Security vs safety*. Trondheim: Norges teknisk-naturvitenskapelige universitet. Tilgjengelig fra: https://www.iot.ntnu.no/users/albrecht/rapporter/notat%20safety%20v%20security.pdf (Hentet: 07.02.20)

Authentication (2019) i *Wikipedia*. Tilgjengelig fra: https://en.wikipedia.org/wiki/Authentication (Hentet: 19.01.20)

Autonomous (u.å.) i *Cambridge Dictionary*. Tilgjengelig fra: https://dictionary.cambridge.org/dictionary/english/autonomous (Hentet: 01.02.20)

Bajraktari, I. (2019) *Cyber security and cyber risks in the shipping industry*. Tilgjengelig fra: https://www.penningtonslaw.com/news-publications/latest-news/2019/cyber-security-and-cyber-risks-in-the-shipping-industry (Hentet: 16.02.2020)

Balduzzi, M. (2014) *AIS Exposed – Understanding Vulnerabilities & Attacks 2.0*. Tilgjengelig fra: https://www.blackhat.com/docs/asia-14/materials/Balduzzi/Asia-14-Balduzzi-AIS-Exposed-Understanding-Vulnerabilities-And-Attacks.pdf (Hentet: 25.02.20)

Bhattacharjee, S. (2019) What is Electronic Chart Display and Information System (ECDIS)?, *Marine Insight*. Tilgjengelig fra: https://www.marineinsight.com/marine-navigation/what-is-electronic-chart-display-and-information-system-ecdis/ (Hentet: 17.02.20)

BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO (2016) *The guidelines on cyber security onboard ships*. Bagsvaerd: BIMCO. Tilgjengelig fra: https://10a4adff-267b-483c-8bea-93a8e5be67fb.filesusr.com/ugd/0c0cb0_114e06b3750d4a5d918508e3aee308dc.pdf (Hentet: 04.12.2019)

Borkamo, R., Solvoll, G. and Wetting, K. B. (2018) Autonome skip er på vei. *Samferdsel*. Tilgjengelig fra: https://samferdsel.toi.no/forskning/autonome-skip-er-pa-vei-article34004-2205.html (Hentet: 02.02.20)

Bothur, D., Valli, C. and Zheng, G. (2017) *A critical analysis of security vulnerabilities and countermeasures in a smart ship system*. Edith Cowan University, Australia. Tilgjengelig fra: https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1209&context=ism (Hentet: 25.02.20)

Boyes, H. and Isbell, R. (2017). *Code of Practice – Cyber Security for Ships*. ISBN 978-1-78561-577-1. London: Institution of Engineering and Technology. Tilgjengelig fra: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf (Hentet: 06.02.20)

Cassi, E., Cavanna, J. P. and Scialla, P. (2018) *Tackling complexity: Protecting against cyber risk in the marine industry*. Lloyd's Register.

Category: Attack (2016) i *OWASP Foundation Wiki*. Tilgjengelig fra: https://wiki.owasp.org/index.php/Category:Attack (Hentet: 22.01.20)

Category: Vulnerability (2016) i *OWASP Foundation Wiki*. Tilgjengelig fra: https://wiki.owasp.org/index.php/Category:Vulnerability (Hentet: 22.01.20)

Chalermpalanupap, T. (2014) Known Knowns, Known Unknowns, Unknown Unknowns, and Unknown Knowns in the South China Sea Disputes, *Kyoto Review of Southeast Asia*, issue 15. Tilgjengelig fra: https://kyotoreview.org/issue-15/known-knowns-known-unknowns-unknown-unknowns-and-unknown-knowns-in-the-south-china-sea-disputes/ (Hentet: 11.02.20)

Check Point (u.å.) *What is a Cyber Attack?*. Tilgjengelig fra: https://www.checkpoint.com/definitions/what-is-cyber-attack/ (Hentet: 22.01.20)

Cisco (u.å.) *What Are the Most Common Cyber Attacks?*. Tilgjengelig fra: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html (Hentet: 22.01.20)

ClassNK (u.å.) *AboutNK – Introduction*. Tilgjengelig fra: http://www.classnk.com/hp/en/about/aboutNK/index.html (Hentet: 13.02.20)

Control system (2020) i *Wikipedia*. Tilgjengelig fra: https://en.wikipedia.org/wiki/Control_system (Hentet: 10.03.20)

Copestake, J. (2019) Unmanned ship to go on 400-year-old journey across the Atlantic, *BBC*, 16. oktober 2019. Tilgjengelig fra: https://www.bbc.com/news/technology-50047449 (Hentet: 06.02.20)

Council of Europe Portal (2020) *Chart of signatures and ratifications of Treaty* 185. ETS No.185. Tilgjengelig fra: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=exhG7iJ7 (Hentet: 12.02.20)

Craiger, J.P., Haass, J. C. & Kessler, G.C. (2018) A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System, *International Journal on Marine Navigation and Safety of Sea Transportation*, 12(3), s. 429-437.

Cryptographic protocol (2019) i *Wikipedia*. Tilgjengelig fra: https://en.wikipedia.org/wiki/Cryptographic_protocol (Hentet: 22.11.19)

Cyberattack (2020) i *Wikipedia*. Tilgjengelig fra: https://en.wikipedia.org/wiki/Cyberattack (Hentet: 22.01.20)

Deketelaere, P. (2017) *The legal challenges of unmanned vessels*. Masteroppgave. Universiteit Gent.

Ellingsen, P. and Gejibo, S. (2017) *INF226 – Software Security*. Department of Informatics, University of Bergen. Upublisert.

European Global Navigation Satellite System Agency (2017) *What is GNSS?*. Tilgjengelig fra: https://www.gsa.europa.eu/european-gnss/what-gnss (Hentet: 17.02.20)

FinFerries (2018) *Finferries' Falco world's first fully autonomous ferry*. Tilgjengelig fra: https://www.finferries.fi/en/news/press-releases/finferries-falco-worlds-first-fully-autonomous-ferry.html (Hentet: 02.02.20)

Fjelldal, T. (2018) *Autonomous Systems Design - An Exploratory Research Study in the Context of Maritime Shipping*. Masteroppgave. Trondheim: Norges teknisk-naturvitenskapelige universitet.

Fjelldal, T. (2019) *Autonomy @ Kongsberg*. Kongsberg Maritime. Upublisert.

Fosen, J. (2019) *Cyber Security Awareness - in the maritime industry*. Tilgjengelig fra: http://www.gard.no/Content/25634225/Cyber%20Security_Presentation%20(ID%201418279).pdf (Hentet: 05.12.19)

Foster, S. (2020) *Software Safety vs. Software Security: Understanding the Difference*. Tilgjengelig fra: https://www.perforce.com/blog/kw/software-safety-vs-security-whats-different (Hentet: 07.02.2020)

Futurenautics Ltd (2016) *Autonomous Ships*.

Giles, M. (2019) Triton is the world's most murderous malware, and it's spreading, *MIT Technology Review*. Tilgjengelig fra: https://www.technologyreview.com/s/613054/cybersecurity-critical-infrastructure-triton-malware/ (Hentet: 18.03.20)

Gisle, J. (2019) autonom, i *Store Norske Leksikon*. Tilgjengelig fra: https://snl.no/autonom (Hentet: 01.02.20)

Goud, N. (u.å) Cyber Attack on COSCO. *Cybersecurity Insiders*. Tilgjengelig fra: https://www.cybersecurity-insiders.com/cyber-attack-on-cosco/ (Hentet: 02.02.2020)

Guide to Cryptography (2018) i *OWASP Foundation Wiki*. Tilgjengelig fra: https://wiki.owasp.org/index.php/Guide_to_Cryptography (Hentet: 22.11.19)

Higgins, D. and Perera, T. (2017) *Theoretical overview of known, unknown and unknowable risks for property decision making*. United Kingdom: Birmingham City University & Australia: RMIT University. Tilgjengelig fra: https://www.researchgate.net/publication/320943325_Theoretical_Overview_of_Known_Unknown_and_Unknowable_Risks_for_Property_Decision_Makings (Hentet: 11.02.20)

Hole, K. J (2016) *Authentication.* Department of Informatics, University of Bergen. Upublisert.

Hopcraft, R. and Martin, K. (2018) Why 50,000 ships are so vulnerable to cyberattacks, *The conversation*. Tilgjengelig fra: https://theconversation.com/why-50-000-ships-are-so-vulnerable-to-cyberattacks-98041 (Hentet: 06.11.2018)

Information and communications technology (2020) i *Wikipedia*. Tilgjengelig fra: https://en.wikipedia.org/wiki/Information_and_communications_technology (Hentet: 17.02.2020)

Information security (2020) i *Wikipedia*. Tilgjengelig fra: https://en.wikipedia.org/wiki/Information_security (Hentet: 20.01.20)

International Maritime Organization (u.å.) *Maritime cyber risk*. Tilgjengelig fra: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx (Hentet: 12.02.20)

IRISL Group (2020) i *Wikipedia*. Tilgjengelig fra: https://en.wikipedia.org/wiki/IRISL_Group (Hentet: 02.02.20)

Jalonen, R., Tuominen, R. and Wahlström, M. (u.å.) *Remote and Autonomous Ships – The next steps*. Rolls-Royce.

Jones, K. and Tam, K. (u.å.) *Cyber-Risk Assessment for Autonomous Ships*. England: University of Plymouth.

Kemmerer, C. (2015) *What is a «Cryptographic Protocol?»*. Tilgjengelig fra: https://www.ssl.com/faqs/what-is-a-cryptographic-protocol/ (Hentet: 22.11.2019)

Knapskog, S. J. and Nätt, T. H. (2019) autentisering, i *Store Norske Leksikon*. Tilgjengelig fra: https://snl.no/autentisering (Hentet: 19.01.2020)

Kongsberg Maritime (u.å.a) *Autonomous Underwater Vehicle, Hugin*. Tilgjengelig fra: https://www.kongsberg.com/maritime/products/marine-robotics/autonomous-underwater-vehicles/AUV-hugin/ (Hentet: 02.02.20)

Kongsberg Maritime (u.å.b) *HUGIN – Best at great depths*. Tilgjengelig fra: https://www.kongsberg.com/maritime/about-us/news-and-media/our-stories/hugin--best-at-great-depths/ (Hentet: 02.02.20)

Kongsberg Maritime (u.å.c) *Autonomous ship project, key facts about Yara Birkeland*. Tilgjengelig fra: https://www.kongsberg.com/maritime/support/themes/autonomous-ship-project-key-facts-about-yara-birkeland/?OpenDocument= (Hentet: 16.09.19)

Kongsberg Maritime (u.å.d). *Autonomous future.* Tilgjengelig fra: https://www.kongsberg.com/maritime/about-us/news-and-media/our-stories/autonomous-future/ (Hentet: 11.02.20)

Lloyd's Register (u.å.) *Assessing compliance to the BIMCO guidelines*. Tilgjengelig fra: https://www.lr.org/en/bimco-guidelines/ (Hentet: 05.12.19)

Lloyd's Register Group (2018a) *Cyber threat briefing: Essential guidance for shipowners and operators.*

Lloyd's Register Group (2018b) *Cyber Security? You're right, it's a hot topic*.

Lo, C. (2019) Protective layers: key points from ClassNK's Cyber Security Approach, *Ship Technology*. Tilgjengelig fra: https://www.ship-technology.com/features/ship-cyber-security/ (Hentet: 12.02.20)

Marr, B. (2018) What is Industry 4.0? Here's A Super Easy Explanation For Anyone, *Forbes*. Tilgjengelig fra: https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/#35f6d2769788 (Hentet: 10.03.20)

Matthews, C. (2017) Unmanned 'ghost' ships are coming, *The conversation*. Tilgjengelig fra: https://theconversation.com/unmanned-ghost-ships-are-coming-83324 (Hentet: 06.11.2018)

Moll, J.B., Melin, S. (Tilretteleggere), & Thuestad, E.B. (Redaktør). (2018). Varer levert utan sjåfør [Episode fra TV-serie]. I Pedersen, H. (Produksjonsleder), *Framtidas superframkomstmiddel*. Tilgjengelig fra: https://tv.nrk.no/serie/framtidas-superframkomstmiddel/sesong/1/episode/3/avspiller (Hentet: 11.02.20)

Monogioudis, I. (2019) Maritime cyber security: A widening net, *Safety4sea*. Tilgjengelig fra: https://safety4sea.com/cm-maritime-cyber-security-a-widening-net/ (Hentet: 25.01.20)

MUNIN (2016a) *Welcome to the MUNIN Project web page.* Tilgjengelig fra: http://www.unmanned-ship.org/munin/ (Hentet: 10.02.20)

MUNIN (2016b) *About MUNIN – Maritime Unmanned Navigation through Intelligence in Networks.* Tilgjengelig fra: http://www.unmanned-ship.org/munin/about/ (Hentet: 10.02.20)

Nasjonal Sikkerhetsmyndighet (2016) *Sikring av kommunikasjon med TLS.* Oslo: Nasjonal Sikkerhetsmyndighet. Tilgjengelig fra: https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger/veiledning-for-systemteknisk-sikkerhet/sikring-av-kommunikasjon-med-tls/ (Hentet: 22.11.19)

Nasjonal Sikkerhetsmyndighet (2019a) *Helhetlig digitalt risikobilde 2019.* Oslo: Nasjonal Sikkerhetsmyndighet. Tilgjengelig fra: https://www.nsm.stat.no/globalassets/rapporter/2019---nsm-helhetlig-digitalt-risikobilde.pdf (Hentet: 01.12.2019)

Nasjonal Sikkerhetsmyndighet (2019b) *Risiko 2019 Krafttak for et sikrere Norge.* Oslo: Nasjonal Sikkerhetsmyndighet. Tilgjengelig fra: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf (Hentet: 01.12.19)

National Cyber Security Centre (2015) *How cyber attacks work*. Tilgjengelig fra: https://www.ncsc.gov.uk/information/how-cyber-attacks-work (Hentet: 22.01.20)

Nordahl, H. and Rødseth, Ø. J. (2017) *Definitions for Autonomous Merchant Ships*. Norwegian Forum for Autonomous Ships (NFAS).

Nätt, T. H. (2018) informasjonssikkerhet, i *Store Norske Leksikon*. Tilgjengelig fra: https://snl.no/informasjonssikkerhet (Hentet: 20.01.20)

Nätt, T. H. (2019a) konfidensialitet – informasjonssikkerhet, i *Store Norske Leksikon*. Tilgjengelig fra: https://snl.no/konfidensialitet_-_informasjonssikkerhet (Hentet: 20.01.20)

Nätt, T. H. (2019b) integritet – datasikkerhet, i *Store Norske Leksikon*. Tilgjengelig fra: https://snl.no/integritet_-_datasikkerhet (Hentet: 20.01.20)

Nätt, T. H. (2019c) tilgjengelighet – informasjonssikkerhet, i *Store Norske Leksikon*. Tilgjengelig fra: https://snl.no/tilgjengelighet_-_informasjonssikkerhet (Hentet: 20.01.20)

Nätt, T. H. (2019d) ikke-benekting, i *Store Norske Leksikon*. Tilgjengelig fra: https://snl.no/ikke-benekting (Hentet: 20.01.20)

Outlier (2020) i *Wikipedia*. Tilgjengelig fra: https://en.wikipedia.org/wiki/Outlier (Hentet: 11.02.20)

Pen Test Partners (u.å.) *Maritime Cyber Security Testing*. Tilgjengelig fra: https://www.pentestpartners.com/penetration-testing-services/maritime-cyber-security-testing/ (Hentet: 10.03.20)

Pole Star (u.å.) *How sole reliance on AIS data could undermine your organisation's gBMP.* Tilgjengelig fra: https://www.polestarglobal.com/media/1163/documents2fhow_sole_reliance_on_ais_data_could_undermine_your_organisationsplusgbmp.pdf (Hentet: 25.02.2020)

Public-key cryptography (2020) i *Wikipedia*. Tilgjengelig fra: https://en.wikipedia.org/wiki/Public-key_cryptography (Hentet: 20.01.20)

Rolls-Royce Commercial Marine (2017) *Rolls-Royce demonstrates world's first remotely operated commercial vessel*. Tilgjengelig fra: https://www.rolls-royce.com/media/press-releases/2017/20-06-2017-rr-demonstrates-worlds-first-remotely-operated-commercial-vessel.aspx (Hentet: 02.02.20)

Safety4Sea (2018) 2018 Highlights: Major cyber attacks reported in maritime industry, *Safety4Sea*. Tilgjengelig fra: https://safety4sea.com/cm-2018-highlights-major-cyber-attacks-reported-in-maritime-industry/ (Hentet: 01.02.20)

Safety4Sea (2020) Cyber-attack at UK marine engineering consultancy, *Safety4Sea*. Tilgjengelig fra: https://safety4sea.com/cyber-attack-at-uk-marine-engineering-consultancy/ (Hentet: 02.02.20)

SCADA (2020) i *Wikipedia*. Tilgjengelig fra: https://en.wikipedia.org/wiki/SCADA (Hentet: 10.03.20)

Schneier, B. (2002) *Crypto-Gram: Is 1024 Bits Enough?*. Tilgjengelig fra: https://www.schneier.com/crypto-gram/archives/2002/0415.html#3 (Hentet: 21.01.20)

Schneier, B. (2018) *Click here to kill everybody*. USA: W. W Norton & Company, Inc.

Security (u.å.) i *Cambridge Dictionary*. Tilgjengelig fra: https://dictionary.cambridge.org/dictionary/english/security (Hentet: 07.02.20)

Ship IP LTD (2018*) Maritime cyber security ECDIS will be at the heart of autonomous shipping*. Tilgjengelig fra: https://shipip.com/maritime-cyber-security-ecdis-will-be-at-the-heart-of-autonomous-shipping/ (Hentet: 06.11.2018)

Skoglund, U. (2018) Førerløse ferger kan erstatte gangbruer, *Gemini.no*. Tilgjengelig fra: https://gemini.no/2018/06/forerlose-ferger-kan-erstatte-gangbruer/ (Hentet: 02.02.20)

Skredderberget, A. (2018) *The first ever zero emission, autonomous ship*. Tilgjengelig fra: https://www.yara.com/knowledge-grows/game-changer-for-the-environment/ (Hentet: 16.09.19)

Stensvold, T. (2019) Asko får Enova-støtte til å utvikle autonome transportferger, *Teknisk Ukeblad*. Tilgjengelig fra: https://www.tu.no/artikler/asko-far-enova-stotte-til-a-utvikle-autonome-transportferger/460645 (Hentet: 16.02.20)

The Black Swan: The Impact of the Highly Improbable (2020) i *Wikipedia*. Tilgjengelig fra: https://en.wikipedia.org/wiki/The_Black_Swan:_The_Impact_of_the_Highly_Improbable (Hentet: 11.02.20)

There are known knowns (2019) i *Wikipedia*. Tilgjengelig fra: https://en.wikipedia.org/wiki/There_are_known_knowns (Hentet: 11.02.20)

Threat actor (2020) i *Wikipedia*. Tilgjengelig fra: https://en.wikipedia.org/wiki/Threat_actor (Hentet: 25.01.20)

Tollefson, R. (2019) *Security+: How To Explain Threat Actor Types And Attributes [Updated 2019]*. Infosec. Tilgjengelig fra: https://resources.infosecinstitute.com/category/certifications-training/securityplus/sec-domains/threats-attacks-and-vulnerabilities-in-security/how-to-explain-threat-actor-types-and-attributes/#gref (Hentet: 06.02.20)

Transport Layer Security (2020) i *Wikipedia*. Tilgjengelig fra: https://en.wikipedia.org/wiki/Transport_Layer_Security (Hentet: 20.01.20)

Trend Micro (2019) *One Flaw too Many: Vulnerabilities in SCADA Systems*. Tilgjengelig fra: https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/one-flaw-too-many-vulnerabilities-in-scada-systems (Hentet: 18.03.20)

Tunggal, A. T. (2020) *What is a Cyber Attack?*. Tilgjengelig fra: https://www.upguard.com/blog/cyber-attack (Hentet: 22.01.20)

U.S. Department of Defense (2002) *News Transcript – DoD News Briefing – Secretary Rumsfeld and Gen. Myers*. Tilgjengelig fra: https://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636 (Hentet: 07.02.20)

World Maritime News (2018) COSCO Shipping Lines Falls Victim to Cyber Attack, *World Maritime News*. Tilgjengelig fra: https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/ (Hentet: 02.02.2020)

World Maritime News (2019) IBM Joins Mayflower Autonomous Ship Project, *World Maritime News*. Tilgjengelig fra: https://worldmaritimenews.com/archives/284829/ibm-joins-mayflower-autonomous-ship-project/ (Hentet: 06.02.20)

Yara (2018) *Corporate Releases – Yara and Kalmar to develop world's first fully-digitalized and zero emission cargo solution for Yara Birkeland*. Tilgjengelig fra: https://www.yara.com/corporate-releases/yara-and-kalmar-to-develop-worlds-first-fully-digitalized-and-zero-emission-cargo-solution-for-yara-birkeland/ (Hentet: 18.02.20)