TRANSNAV the International Journal on Marine Navigation and Safety of Sea Transportation
http://www.transnav.eu
Volume 15
Number 3
September 2021
DOI: 10.12716/1001.15.03.04

A Retrospective Analysis of Maritime Cyber Security Incidents

P.H. Meland[1], K. Bernsmed[1], E. Wille[1], Ø.J. Rødseth[2] & D.A. Nesheim[2]
[1] *SINTEF Digital, Trondheim, Norway*
[2] *SINTEF Ocean, Trondheim, Norway*

ABSTRACT: The maritime industry is undergoing a rapid evolution through the introduction of new technology and the digitization of existing services. At the same time, the digital attack surface is increasing, and incidents can lead to severe consequences. This study analyses and gives an overview of 46 maritime cyber security incidents from the last decade (2010-2020). We have collected information from open publications and reports, as well as anonymized data from insurance claims. Each incident is linked to a taxonomy of attack points related to onboard or off-ship systems, and the characteristics have been used to create a Top-10 list of maritime cyber threats. The results show that the maritime sector typically has incidents with low frequency and high impact, which makes them hard to predict and prepare for. We also infer that different types of attackers use a variety of attack points and techniques, hence there is no single solution to this problem.

1 INTRODUCTION

The maritime sector is a complex ecosystem, bringing together stakeholders and organizations of different sizes, maturity, complexity, and operational scope. During the last decade, the maritime industry has undergone a rapid evolution through the introduction of new technology and the digitization of existing services. While aiming to increase profit, these changes can also introduce new risks. In particular, the increased connectivity and the converging of Information Technology (IT) and Operation Technology (OT) systems will expose the maritime operations to new threats that may have severe financial and reputation repercussions. Further, the threat environment against the maritime sector is steadily becoming more hostile; cyber attacks are becoming more frequent and organized criminal networks and hostile nations are now targeting all actors in the digital value chain [65], including shipping companies, vessels, and their shore-side facilities.

In this paper we present a retrospective analysis of cyber security incidents from the last decade (2010-2020). Our analysis includes 46 reported incidents that have affected the stakeholders in the maritime sector in significant ways. Our work provides an overview attack points and shows a mapping between these and the incidents. We have also created a threat categorization based on the characteristics of the incidents. While the main driver of our analysis was to increase the awareness of cyber security threats towards Norwegian maritime interests, the maritime operations are international and malicious actors know no borders. Hence, the results should be equally relevant for the international maritime community.

The paper is organized as follows. In Section 2, we give an overview over relevant background work on threats and incidents in the maritime sector. Section 3 introduces the methodology that we have been

applied when gathering the data for this paper. In Section 4, we present the target description, which includes an overview of the special characteristics of maritime systems and a generalized representation of the shipboard and off-ship systems with annotated attack points. Section 5 contains an overview of incidents, while Section 6 we build a categorization of threats based on the incidents. Section 7 discuss the trend related incidents and threats, and what we can expect for the current and road ahead. Finally, in Section 8 we conclude our work and point to future opportunities.

2 BACKGROUND

Initial work on security threats to the maritime sector were mainly focused on terrorism [29, 81]. In 2011, ENISA released the report "Analysis of Cyber Security Aspects in the Maritime Sector" [18], which recognized the maritime sector as a critical infrastructure. The report identified the very low awareness of cyber security in the sector as being a major challenge and suggested that the low number of publicly known cyber security incidents could be the reason. In 2015, a Norwegian report [39] on digital vulnerabilities in the maritime sector was released. It identified the top 10 challenge in the sector and provided examples of both attacks and accidents that had been possible because due to these. The same year, the EU project MUNIN performed a risk assessment of safety and cyber security threats [37], in which jamming, spoofing and hacking of AIS, GPS and ship communication equipment were considered as the highest risks. Threats that are specific for maritime digital communication were identified in the Norwegian research project CySiMS [50]. Researchers from the University of Plymouth have over several years published papers related to vulnerabilities, threats and attacks to the maritime sector (e.g. [34, 70, 71]). There are further examples of security research on specific sub-systems or operations, e.g. autonomous shipping [76], ports and port systems [22] and IT/OT systems installed on vessels [13].

In 2017, the British Department of Transport published an overview over motivations for attacking ship systems, including potential threat actors [11]. The following year, ENISA published their report on the cyber threat landscape, claiming that cyber criminals and state-sponsored actors were taking over the scene, monetization was becoming one of the main drivers for cyber attacks [65]. Their standpoint has recently been confirmed by the Norwegian Police Security Service, who identifies state-sponsored intelligence operations against the maritime industry as a significant risk to Norway [56]. Further, the Norwegian National Security Authority (NSM) provides annual reports on the cyber threat picture against Norway [52, 53], which includes ransomware, digital intelligence operations and disturbance of positioning services.

The abovementioned sources provide a thorough analysis of cyber security vulnerabilities, threats and risks relevant for maritime operations, but most of them lack an anchoring in empirical evidence. Nevertheless, they have been a useful basis for analyzing, mapping and interpreting our results.

3 METHODOLOGY

To collect information about incidents, we have screened scientific publications, public and commercial reports, newspapers and other forms of grey literature, using key words, such as "cyber attack", "cyber incident", "cyber risk", "cyber threat", "cyber security" and "maritime" in popular search engines and indexing databases (Google, Google Scholar, IEEE Xplore and SpringerLink). We also searched in the Lloyd's List [42] database for cyber security events. Furthermore, we applied a snowballing technique [83], which means that we screened our sources' sources, to locate additional relevant literature that did not show up in our initial searches.

We did, whenever possible, strive to use several independent sources to confirm the validity of each of the reported incidents, and we revised our original sources by reading reports that compiled several of the previously reported incidents, such as Kapalidis [55], Jones et al. [34], KNect365 [51], Singh [68] and Cyberkeel [20]. The final selection of incidents that we included in our analysis were based on the following criteria:

- The incidents must have occurred during the last decade (2010 to 2020)
- The incidents must have been caused by "successful" attacks. We did not include mere attack attempts, or unsuccessful attacks.
- The incidents must have been caused by a real attack. We did not include any "white hat" experiments, performed by, for example, students, security companies or researchers.
- The incidents must have had a direct effect on any of the core systems in the maritime ecosystem. We did not include incidents that were only vaguely related to shipping, for example attacks on logistics companies or supply chains.
- The incidents must have had a significant impact on the maritime industry. Hence, we did not include any "minor" incidents (typically treated as "noise" by the security community) in our analysis.

In addition to looking for incidents in public literature, we collaborated with representatives from the Intelligence and Operations Centre at The Norwegian Shipowners' Mutual War Risk Insurance Association and the Norwegian Maritime Cyber Resilience Centre. They provided us with anonymized event data, which resulted in the identification of additional incidents. As far as we are aware, only a few these incidents have been mentioned in open reports.

3.1 *Limitations*

Shipping is a very diverse sector from small dry bulkers carrying sand and gravel along the coast to large container ships in intercontinental trade. It is highly unlikely that this study has captured all the different cyber incidents over the sector as most of the

quoted references tend to focus on larger ships and operations. The sources are also biased in that they are mostly from the western world, including a number of Norwegian reports. The reader should keep this bias in mind when reading this paper, but the authors still believe that this is a representative report on the general situation related to cyber incidents and threats in the maritime sector.

4 TARGET DESCRIPTION

To systematically analyze the incidents, there is a need to describe the scope and context of our study. Here we provide an overview over the specific characteristics of the maritime industry and models of the onboard and off-ship systems.

4.1 *The maritime threat profile*

The maritime industry has some special characteristics which result in a threat profile that differs significantly from the more traditional land-based systems:

1. It is a relative small industry, e.g. there are about 98 000 propelled seagoing merchant vessels of 100 gross tons and above operating internationally [74]. This puts limits on the industry's ability to do systematic analyses and to learn from others; hence making it difficult to improve its cyber security practices.
2. Ships are complex "sailing villages" with a wide range of information and communication technology (ICT) onboard. This ranges from office systems, via life support systems and engine automation, to navigation systems.
3. Ships will normally have a lifetime of 25-35 years and software upgrades are done on individual equipment using different time intervals. This means that most ships have a very mixed set of equipment, both for administrative functions and general information technology (IT) and for operational technology (OT).
4. It is a highly cost sensitive market, due to strong international competition, resulting in a large share of stakeholders not giving cybersecurity the required priority.
5. The ships are under international regulation, which have tended to focus on minimum technical requirements to ensure a level economic playing field.

These issues result in a complex, but highly inhomogeneous and sometimes poorly maintained ICT system. From a cyber security point of view, this may be an advantage, as the reconnaissance of the target system and the selection of a possible attack vector becomes more complicated. However, as digitalization in the maritime sector increases and more ships become connected to the Internet, it also means that a larger attack surface will be exposed. Shipping will hence become a more tempting target, for commercially motivated attacker, for state terrorism interested in damaging import- and export facilities, and for the more "adventurous" hackers.

The next two subsections describe models of onboard and off-ship systems with potential attack points. The taxonomy of identifiers should be seen as preliminary, and not all of these attack points have been mapped to actual incidents. However, they are still relevant for potential threats and future mapping of new incidents.

4.2 *Onboard systems*

Figure 1 shows a generalized representation of onboard systems with attack points classified as S1 to S7. S1 represents attacks on operational technology, usually located in a controlled environment. This may also include attacks via moveable external memory systems (MEMS or "memory sticks") which sometimes are used for updates to software or, e.g., electronic charts. S2 represents attacks on administrative systems onboard. S3 and S4 are attacks on mobile data/satellite communication or VHF radio digital communication respectively, S5 represents attacks on Global Maritime Distress and Safety Systems (GMDSS), S6 on Global Navigation Satellite Systems (GNSS) and S7 on peripheral devices to controlled systems. S0 is used for other onboard attacks.

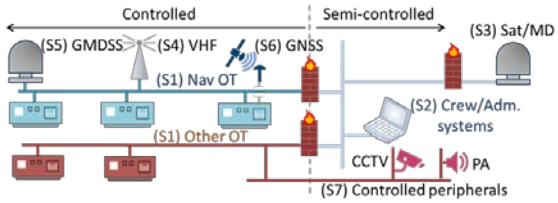

Figure 1. Attack points onboard the ship

Note that the topologies on different ships vary wildly and particularly older ships may have much less system separation in place.

4.3 *Off-ship systems*

The other group of attack points are communication links from ship to shore and the corresponding shore systems. These are illustrated in Figure 2.

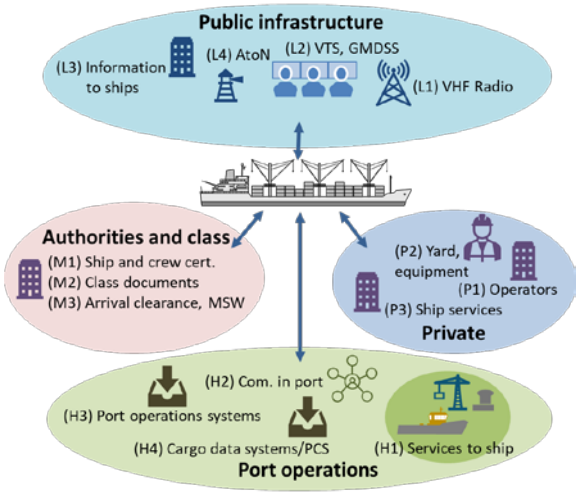

Figure 2. Attack points onshore and between ship-and-shore

The first group belongs to public infrastructure. The most relevant here are the VHF voice and data transmission infrastructure, including automatic identification system (AIS) services (L1); the vessel traffic services, maritime rescue and GMDSS services (L2); various information services to ship, including meteorological data, recommended routes and notices to mariners (L3); and digitalized aids to navigation (L4). Other attack points in this group are labelled with L0.

The next group are the authorities and class societies. M1 is related to ship and crew certificates, e.g., from flag state; M2 is services and documents issued by class societies; and M3 is authority services related to arrival and departure clearance, e.g., maritime single windows (MSW), passenger clearance, phytosanitary services etc. M0 is used for other attacks points in this group.

Port operations are services to ships, e.g., tugs, linesmen, etc. (H1); H2 labels attacks on internal communication and data exchange inside ports and terminals; and H3 labels attacks on port operations data systems such as harbor master's systems etc. H4 labels attack on cargo data systems in the port. This can also include port community systems (PCS). H0 is used for other attack points for port services.

Finally, private services are grouped into ship operators (P1). This includes owner, manager, charter etc.; P2 codes for technical services from yards, spare part or consumable suppliers; and P3 for other services such as weather routing, route optimization etc. P0 represents other services.

5 KNOWN INCIDENTS

Below we describe the incidents we have identified based on the methodology and criteria described in Section 3, are shown below. Each incident is given a unique identifier, which is presented in bold text together with the relevant year(s) and attack point referring to identifiers from the previous section.

- A1 - Year: 2010, Attack point: S1
  A drilling rig is infected by malware on its way from the construction site in South Korea to South America. Critical control systems are infected, requiring 19 days of downtime to clear the issue. Such shutdowns are estimated to cost 700 000 USD per day. Sources: [20, 66].
- A2 - Year: 2010–2011, Attack point: P1
  A Greek shipping company is hacked via its headquarters' WiFi network. For the next two years, information regarding vessels and sailing routes is exfiltrated and used by the attackers to plan physical pirate attacks in Gulf of Aden. Source [55].
- A3 - Year: 2011-2013, Attack point: H4
  The cargo tracking system at Port of Antwerp was infected to enable smuggling of drugs and weapons ("concealed" as bananas from South America). The smuggling operation went on for two years before being detected. The same port was subject to the same attack again in 2018. Sources: [39, 51, 55, 78].
- A4 - Year: 2011-2013, Attack point: P2
  A threat actor made known by Kaspersky [27] as "Icefog" conducts targeted cyber espionage attacks against various sensitive organizations in South Korea and Japan, including maritime and ship-building groups. The attacks rely on spear-phishing and the exploitation of known vulnerabilities. Source: [27].
- A5 - Year:2011, Attack point: P1
  A cyber attack against the Iranian shipping company IRISL (Islamic Republic of Iran Shipping Lines) damaged all the data related to rates, loading, cargo number, date, and place. The attack also crippled the company's internal communication network and caused severe financial losses and loss of cargo. Sources: [20, 73].
- A6 - Year: 2012, Attack point: S3
  Iranian officials report a cyber attack on communication networks on an offshore platform in the Persian Gulf. Source: [68].
- A7 - Year: 2012, Attack point: H4
  The cargo handling system used by the Australian Customs and Border Protection Service was infected, enabling the attackers to see if their shipments were flagged as suspicious. In such cases, the smuggled goods were never picked up. Source: [20].
- A8 - Year: 2012, Attack point: M1
  Chinese hackers are accused of a targeted attack against the Danish Maritime Authority, in which documents and information regarding network topology were stolen. The attack was initiated via email, through a virus infected PDF attachment. Sources: [20, 38].
- A9 - Year: 2013, Attack point: S1
  Crew onboard a drilling rig in the Gulf of Mexico accidentally connect virus infected PCs and USB devices to a local network on the rig. This enables the virus to infect the network and disturb the communication between the dynamic positioning system and the thrusters. As a result, drilling operation is halted. Sources: [5, 35, 51].
- A10 - Year: 2014, Attack point: P1
  Hackers intercept and alter emails with account numbers for money transfers, causing severe financial losses. The attacks target transactions between shipping lines and bunker suppliers and between shipping lines and shipyards. Source: [20].
- A11 - Year: 2012-2014, Attack point: S4
  A report from Windward [82] shows that between 2012 and 2014, 1% of all ships provide fake identification information (IMO numbers) in their AIS transmissions. In addition, more than 25% of vessels disable their AIS ("going dark") at least 10% of the time. Such techniques are often used in connection with smuggling, terrorism, human trafficking, illegal fishing or military conflicts. Source: [82]
- A12 - Year: 2016, Attack point: S6
  In South Korea, 280 ships have to return to port after experiencing problems with their navigation systems. North Korea has been blamed for the incident, but evidence is lacking. Source: [55].
- A13 - Year: 2014-2017, Attack point: S4
  An analysis from the Norwegian Coastal Administration on historical AIS data from 2014-2017 shows that civilian Russian vessels perform

regular stops along the Norwegian coast, which are not natural for their primary objectives. These irregularities tend to coincide in time and space with NATO operations, training or drills, and there is reason to suspect that the behavior of these vessels is linked to electronic espionage. Similar activity has been observed in the South China Sea and in the Black Sea. Sources: [62, 79].

- A14 - Year: 2017, Attack point: P3
  British ship broker Clarksons is hacked and the attackers demand a ransom for stolen data. Some sensitive information was stolen and the stock value decreased by 5% immediately after the incident (some sources claim a smaller stock value reduction). Sources: [3, 16, 51, 55].
- A15 - Year:2017, Attack point: P1
  Shipping giant Maersk's operations are severely crippled by the NotPetya ransomware, which was spread via an update patch for the tax accounting software MeDoc (widely used among tax accountants in Ukraine). The virus exploits vulnerabilities in Microsoft Windows and is based on EternalBlue; a cyber attack software developed by US NSA. The incident is seen as the most devastating cyber attack in history, causing problems for almost one fifth of global shipping operations, including 76 ports. Maersk has estimated their economic losses to near 300 million USD in the form of reduced income as a result of the incident. More than 4000 servers, 45 000 PCs and 2500 applications had to be reinstalled. Sources: [15, 28, 46, 51, 68].
- A16 - Year: 2017, Attack point: S6
  At least 20 ships in the Black Sea near Novorossiysk reported that their navigation systems were showing a position which was 32 km away from their actual positions. These observations were likely caused by GNSS spoofing. Source: [55].
- A17 - Year: 2018, Attack point: S6
  A ship is exposed to GPS spoofing in the Black Sea (in the same area as the incident above). The ship is at sea, but the geolocation system onboard claims that the ship is on land. During the course of 3 days this happens 4 times, with a duration of up to 30 minutes. Source: [75].
- A18 - Year: 2018, Attack point: P3
  Chinese hackers are accused of stealing information from subcontractors of the US Navy. In addition, it is presumed that 27 American universities have been attacked, in an attempt to steal research data related to maritime technology. Sources: [43, 76].
- A19 - Year: 2018, Attack point: H4
  Port of Barcelona reports a cyber attack, which turns out to be an infection of the Ryuk ransomware. The infection only affected internal IT systems, and not ship traffic. Sources: [17, 59].
- A20 - Year: 2018, Attack point: H4
  Port of San Diego reports severe disruptions in its IT systems. This is another Ryuk ransomware infection, and the consequences are limited to local functions at the port. The incident occurred only 5 days after the above event in Barcelona, but it is unclear whether these events were related. Sources: [17, 59].
- A21 - Year: 2018, Attack point: P2
  Iranian hackers are blamed for stealing ship designs and information about personnel from the Australian shipbuilder Austal. Austal delivers naval vessels to both Australia and the US. The stolen information was later offered for sale on the dark web. The hackers also attempted to extort money from Austal. Source: [58].
- A22 - Year: 2017-2018, Attack point: P1
  A Nigerian hacker group nicked "Gold Galleon" allegedly stole hundreds of thousands USD through compromising and spoofing business emails in maritime shipping businesses. The hackers have mainly targeted Japanese and South Korean companies, but companies from other countries have also been attacked. Sources: [58, 63].
- A23 - Year: 2018, Attack point: P1
  COSCO Shipping Lines were hit by a cyber attack which caused severe disruptions in their US office networks. Email and network telephone communication was unavailable for 5 days. According to internal emails, the incident was a ransomware infection. Sources: [15, 32].
- A24 - Year: 2018, Attack point: P3
  Italian oilfield services company Saipem detects a cyber attack against their Middle East servers. About 400 servers were hit in the attack, and the servers in Saudi Arabia and UAE were hit especially hard. The company had backups of the affected data, thereby avoiding permanent loss of data. No data was believed stolen. Source: [48].
- A25 - Year: 2019, Attack point: S1
  A large ship on its way to New York gets its onboard control system network infected with malware, resulting in limited functionality. Source: [41].
- A26 - Year: 2018-2019, Attack point: S6
  GPS jamming is observed on multiple occasions through 2018-2019 in northern Norway. The disruption has infected marine traffic to some extent, but severe consequences were fortunately avoided. Source: [53].
- A27 - Year: 2019, Attack point: H3
  An undisclosed American port is infected by the Ryuk ransomware. The infection came through a phishing email attachment and caused CCTV cameras, access control systems and critical process monitoring to become unavailable. Source: [17].
- A28 - Year: 2019, Attack point: P3
  British marine services provider James Fisher and Sons is infected by ransomware and is forced to shut down its digital systems. Share value drops 7% after the incident. Source: [25].
- A29 - Year: 2019, Attack point: S1
  A natural gas compression facility at an undisclosed US pipeline operator is infected with ransomware (presumably Ryuk) and has to shut down for two days. The attack came via phishing email and impacted both IT and OT systems. Sources: [12, 21].
- A30 - Year: 2019, Attack point: S2
  A tanker near the port of Naantali in Finland gets its administration server infected by ransomware. The backup disk is also wiped. Remote Desktop Protocol (RDP), a USB device or an email attachment are identified as probable attack vectors. The same vessel is infected again 4 months later near the same port. Source: [75].
- A31 - Year: 2019, Attack point: S2
  Two ships with the same owner are infected by the

ransomware Hermes 2.1. The infection came as a macro-enabled Word document attached to an email, and multiple workstations on the administrative networks were affected. Source: [75].

- A32 - Year: 2020, Attack point: S2
  A vessel anchored near Tynemouth, UK, has its ship server and multiple PC clients infected with the Ryuk ransomware. Two specialists from the IT service provider were sent onboard and found that all data were encrypted and lost. A full reinstall was necessary to restore the systems. Source: [75].
- A33 - Year: 2020, Attack point: S2
  Three ships sailing under American flag have their administrative systems infected by the ransomware Sodinokibi. This virus also threatens to leak information ("ransomtheft"), in addition to encrypting data. Source: [75].
- A34 - Year: 2020, Attack point: P1
  The shipping company MSC falls victim to a ransomware virus and their headquarters in Geneva are shut down for five days. Sources: [30, 46].
- A35 - Year: 2020, Attack point: H3
  Israel is blamed for hacking the Iranian port of Shahid Rajaee, causing all transportation and flow of goods to halt for a long time. The attack is claimed to have been retaliation after an attack on an Israeli water distribution system. Sources: [30, 80].
- A36 - Year: 2020, Attack point: P2
  Norwegian shipbuilder Vard is hit by a ransomware attack which causes severe operational disruption. Many of the employees are informed that the disruptions may lead to temporary job loss because of halted shipbuilding. Source: [26, 61].
- A37 - Year: 2019-2020, Attack point: P1
  Cruise operator Carnival Corporation & plc is hit by ransomware virus twice in two years, and personal information and credit card details for customers and employees have likely been stolen. Details regarding the type of virus and attack vector have not been made public, but the company states that they may receive compensation claims from the affected parties. Source: [44].
- A38 - Year: 2020, Attack point: M1
  Transport Malta (Maltese transport authority) suffers a cyber attack that shuts down its online systems for five days. Sources: [1, 7].
- A39 - Year: 2020, Attack point: P1
  Greek shipping company Diana Shipping falls victim to the Egregor ransomware. Little information is known about this incident. Source: [4, 40].
- A40 - Year: 2020, Attack point: P1
  The French container carrier company CMA CGM is hit by the Ragnar Locker ransomware. Several of its Chinese offices were affected, and some of its online services had to be shut down, including online booking. Source: [19, 67].
- A41 - Year: 2020, Attack point: M1
  UN shipping agency IMO has its website and intranet disabled by a cyber attack. To prevent further damage, several other key systems are shut down. The attack is described as "sophisticated", further details have not been provided. Sources: [36, 54].
- A42 - Year: 2020, Attack point: P1
  British ferry firm Red Funnel is hit by a cyber attack, causing severe disruption in their IT systems. Among other things, the booking systems were unavailable for several days, forcing customers to arrive well in advance of sailings to buy tickets on-site. Sources: [9, 72].
- A43 - Year: 2020, Attack point: P1
  US transportation and shipping company Matson reports system outage due to a cyber attack. The attack does not stop cargo operations, but some transactions are delayed since affected functions need to be replaced by manual processes. Source: [49].
- A44 - Year: 2020, Attack point: H4
  Port of Kennewick has its IT systems crippled by ransomware. The hackers demanded a ransom of 200 000 USD, which was not paid. Systems were unavailable for several days, as they had to be reestablished from offline backups. Sources: [14, 47].
- A45 - Year: 2020, Attack point: P1
  Norwegian cruise operator Hurtigruten suffers a severe ransomware attack, which has a severe impact on its IT infrastructure. Multiple key systems are unavailable for several days. Passenger data, such as passport information, were exposed and might have been stolen. Sources: [10, 45, 60].
- A46 - Year: 2020, Attack point: P1
  German cruise operator AIDA has its headquarters in Rostock hit by DoppelPaymer ransomware. The attack causes severe IT issues, forcing AIDA to cancel several cruises. Source: [77].

6 CYBER THREAT CATEGORIZATION

A threat is the potential cause of an unwanted incident, which can result in harm [33]. Based on the known incidents and related work, we have established a Top-10 list of maritime cyber threats. The categories are defined by similar characteristics among the incidents and are ranked based on frequency and severity. For each category we have described typical attack vectors and targets. Some incidents have been associated to more than one category, which is natural for attacks that consists of several stages and can affect more than one target. Hence, the categories are not mutually exclusive and can overlap for a single incident.

6.1 *Exposed shipping company/carrier IT-systems*

The IT-systems of shipping companies and carriers have had a burst of associated cyber incidents in the last year and can be linked to 25% of the total incidents for the last decade. We register that the most common attack vector is ransomware, usually in the form of email attachments or links. Just as in many other sectors, there is an increasing trend of ransomtheft viruses, that combine outages and information theft. There are also many examples of economic fraud from social engineering attacks.

Incidents: A2, A5, A10, A15, A22, A23, A34, A37, A39, A40, A42, A43, A45, A46

6.2 *Exposed IT-systems belonging to sub-contractors, shipyards, on-shore installations, service providers, regulators and research facilities*

The IT- and administrative systems of various onshore stakeholders supporting maritime operations have a similar threat picture as shipping companies.

The incidents typically involve theft of business-critical information, as well as more random cases of extortion. From the incidents we see that social manipulation, hacking and ransomware are commonly used attack vectors.

Incidents: A8, A14, A18, A21, A24, A28, A29, A36, A38, A41

6.3 *Exposed port IT-systems*

Ports have been popular targets and have a reputation of being poorly protected against cyber attacks. Outages are expensive, which makes them attractive for extortionists. Furthermore, information theft and manipulation have been used for smuggling operations. Some incidents only report that the port has been "hacked", and in conflict areas we can suspect that state-sponsored actors/cyber warriors are to blame.

Incidents: A3, A7, A15, A19, A20, A27, A35, A44

6.4 *Espionage on maritime operations*

In this category we find incidents characterized by extensive and targeted attacks related to espionage, tapping and surveillance of maritime operations. Mentioned attack vectors tend to be spear-phishing or general hacking, as well as communication tapping.

Incidents: A4, A7, A8, A13, A18, A21

6.5 *Exposed IT- systems onboard ships/offshore installations*

There have been several incidents where IT systems onboard ships have been struck by ransomware, but we suspect that these have been more coincidental than targeted. Typical attack vectors have been email attachments and links, and ship servers and clients have been rendered useless. There has been limited forensic evidence left afterwards as all data are usually wiped clean.

Incidents: A30, A31, A32, A33

6.6 *Manipulation of GNSS-signals used by ships*

This category is mainly related to jamming or spoofing of GPS/GNSS-signals that ships use for navigational purposes. State-sponsored actors tend to be put under suspicion for these events, and the consequences have been more of a disturbing than critical nature. This kind of threat typically manifests itself in geopolitical conflict areas, such as the Black Sea.

Incidents: A12, A16, A17, A26

6.7 *Exposed OT-systems onboard ships/offshore installations*

OT-systems are usually separated from other systems and have therefore been less exposed. Still, we can find examples of such incidents and the consequences have been critical. The attacks have typically entered the system via infected USB units or computers unintentionally connected to the wrong network. Examples of such systems are ECDIS (during map updates) and propulsion control systems.

Incidents: A1, A9, A25, A29

6.8 *Exposed communication systems*

There have been a few examples of attacks against communications systems for land-based operations and offshore installations. Ship communications have not been so much affected, however, with many different and necessary communication systems onboard, they are still potential victims. The incidents show that the consequences tend to be loss of availability caused by generic hacking or ransomware.

Incidents: A5, A6, A13, A23

6.9 *Economic fraud*

These incidents tend to be caused by targeted and specialized attacks, where counterfeit emails or hacked user accounts are used as attack vectors to initiate or manipulate economic transactions. For instance, account information is altered, or fake invoices are sent.

Incidents: A10, A22

6.10 *Misuse of AIS and positioning data*

There are several known events where AIS-systems onboard ships have been unlawfully manipulated or deactivated. These are usually related to smuggling operations, trafficking, illegal fishing or military conflicts. Potential consequences could at worst be collisions, but more likely that other ships are forced to alter their course unnecessary.

Incidents: A11 (several)

7 DISCUSSION

This section gives our interpretation to the findings related to incidents and threats, as well to their relevance for the present and future maritime cyber security.

7.1 *Incident analysis*

Our look into the rear-view mirror tells us that the maritime industry has not had an overwhelming number of incidents, at least not ones that have been so significant that they have been publicly reported or made it to the news headlines. To put our number of 46 incidents in perspective, there were 41 158 cyber incident claims in the "service industries" between 2010 and 2020 according to a dataset we have received from the insurance data provider Advisen, a Zywave company (dated 25th of February 2021). Within "transportation, communications and utilities" there were 4 088 cyber incident claims during the same period. At the same time, some of the most severe consequences in any sector can be tied to maritime. This goes to show that these incidents with low frequency and very high impact indicate challenging cyber risks. They are difficult to predict and prepare for based on history, and in hindsight often considered as black swans [6, 69].

Considering the incidents per year as shown in Figure 3, we can see that this number has multiplied by seven from 2010 to 2020. This growth has not been linear, as there was a noticeable dip during the years 2013-2016. This slumber-period may have given a false sense of security, as some of the incidents in 2017 (especially A14 and A15) seemed to take the affected organizations by surprise and resulted in quite severe consequences.

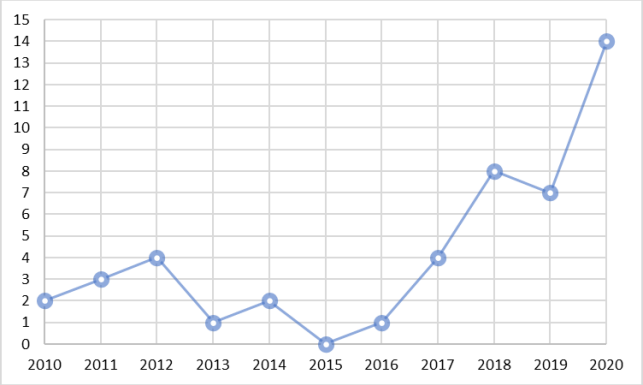

Figure 3. Incidents per year.

When we take a closer look at which attack points have been used over the years, we can see that these are fairly distributed over axis time and attack points, see Figure 4. There is one obvious peak for P1 in 2020, caused by many exploited IT-systems for private onshore operations. Other than this, there are no particular concentrations. We can see that with an increasing number of incidents, there is also a wider exploitation of the attack surface. This means that there is probably no single cause to the incidents that can be eliminated, and there is a need to implement a variety of risk modifiers.

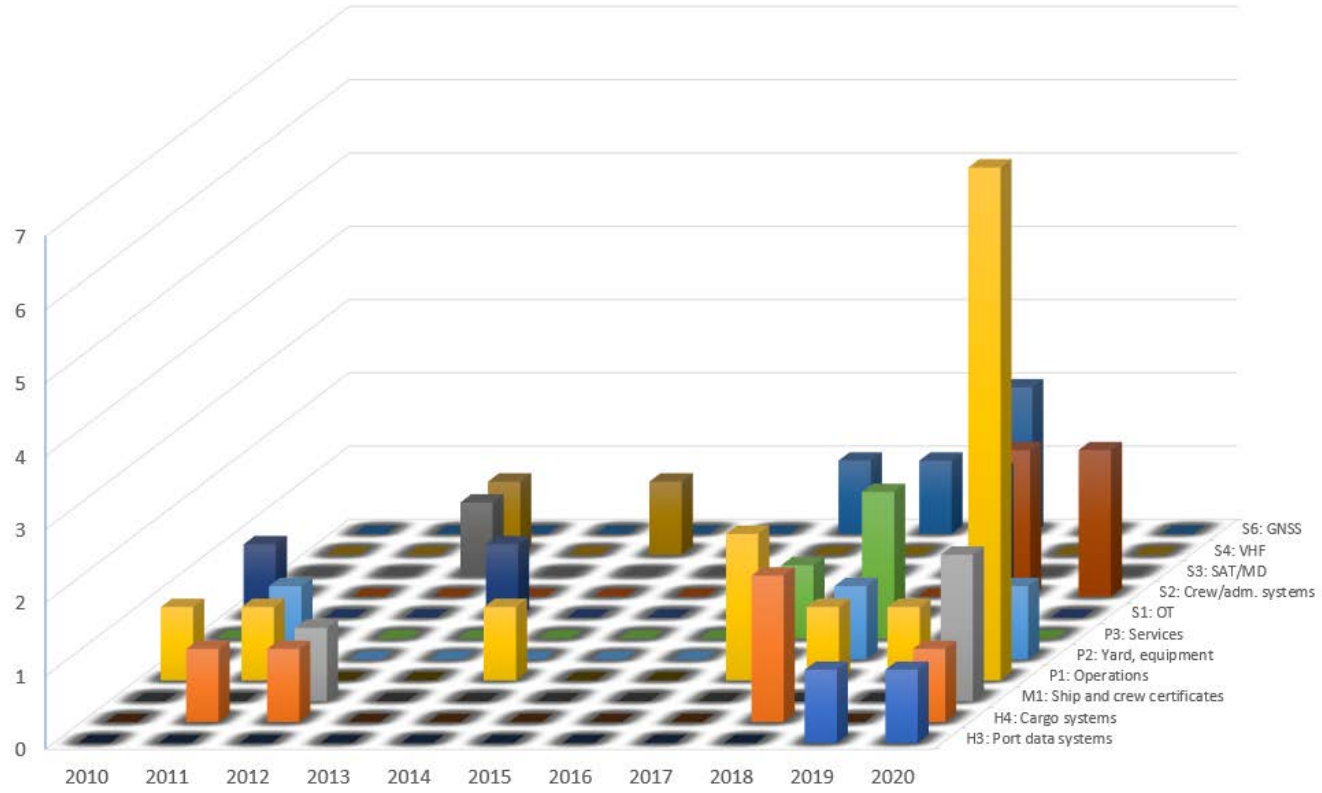

Figure 4. Incidents by year and attack point.

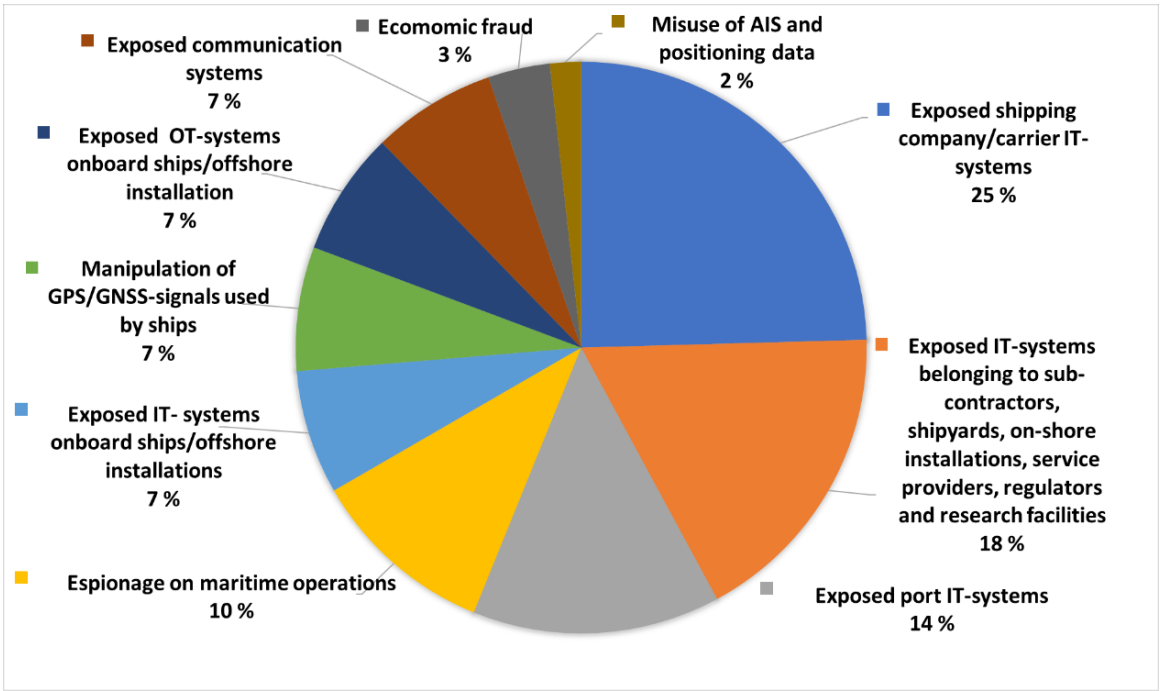

Figure 5. Top-10 cyber threats pie chart.

In addition to the limitations already mentioned under Section 3.1, we acknowledge that there are several weaknesses to our incident data. First of all, there is a reporting bias by the industry itself, as there has been little incentives to disclose incidents to the public. Still, we believe that many of the incidents we have seen have been too big to hide, and that there are not many others of the same magnitude that are unreported. Second, there is now more attention towards cyber incidents than in the past, which increases the chance that an incident will get news coverage. This might lead to a greater number of reported incidents in the last years of the study period. Third, the numbers of incidents related to year and attack point do not have the statistical significance to reveal clear trends. Hence, we have to give a qualitative interpretation of the results, and it is not really possible to extrapolate from this data material. Fourth, some of the incidents spanned over multiple years, and in some cases a single report represented a collection of smaller incidents. The distribution over time is therefore somewhat skewed.

7.2 *Threat analysis*

Figure 5 shows how the incidents sort under the top-10 threats. The three largest slices are all related to exposed land-based IT-infrastructures that the maritime industry depends on. This should not come as a surprise since they have high network connectivity and to a large degree suffer from the myriad of "ordinary" vulnerabilities that are shared between all sectors depending on digital COTS technology. At the same time, ENISA [22] have described a number of cyber security challenges specifically related to ports, such as lack of digital culture, awareness, training, budget and qualified people that are amplified for the maritime sector. More recently, Alcaide and Llave [2] confirm this view by showing that experienced maritime professionals think there is a lack of general knowledge in the field of maritime cyber security.

Malware insertion, in particular ransomware and ransomtheft, has been the prevalent attack method, just as in every other sector and among ordinary citizens. There are also many examples fraud, using social engineering techniques, fake invoices and theft of user accounts. These attacks stem from cybercrime actors with "pure" economic motives. Taking down the value chain behind these attacks might be better than trying to protect every attack point at all times. This requires an international collaboration between law enforcement agencies, CERT/threat intelligence organizations and the industry.

Threats related to espionage on maritime operations, attacks on sub-contractors, shipyards and research facilities, as well as attacks on GNSS-systems, may be linked to another breed of actors, particularly state-sponsored actors or cyber warriors. These are well-funded, motivated by political factors or acquiring foreign technology, and can be extremely difficult to defend against. Active involvement of national security authorities/intelligence offices are necessary to support the maritime industry facing these threats.

7.3 *Present and prospective threats*

Looking backwards does not provide an accurate idea about the present and future threats. Just as most other sectors, the maritime industry is undergoing rapid digitalization and technology development, which increases the digital attack surface. At the same time, digital value chains and dependencies can cause one industry to suffer when another is hit hard.

The ongoing COVID-19 pandemic has for instance showed that events not directly tied to cyber or maritime interests can cause a wave of consequences all through our society. Both ENISA [24] and INTERPOL [32] point to changes in the threat

landscape caused by the pandemic, and in particular vulnerabilities due to work from home offices. According to McAfee, there was a 605% increase in COVID-19 themed threats in Q2 2020. Naval Dome [64] and WorkBoat [57] have also shown a severe increase in such attacks specifically targeting maritime interests. Examples are malicious emails with subject fields such as "Maersk New Shipping schedule details due to COVID-19-Shipment notification" and "COVID-19 SUSPECTED CREW /VESSEL" [23]. The attackers take advantage of the fact that people put under a lot of strain tend to forget their regular cyber hygiene. It has also become more difficult for maintenance and inspection crew to visit ships in ports around the world, and a quick fix has been to enable remote access methods so they can do necessary work. This can easily backfire and create attack openings in traditionally closed systems.

It has been outside the scope of this study to create future threat estimations, but to quote Hoo [31]: "despite the fact that the road ahead may bend with human whim and technological advance, ...it does not appear to bend too sharply too often". We are not likely to get rid of the many threats we have seen in the last decade, and we should build our systems to tackle unforeseen ones as well. This is in accordance with what Ben Densham from Nettitude has stated [8], that ship systems "need constant attention in operation to guard against the speed and agility of threats and attacks in the cyber arena".

8 CONCLUSION AND FURTHER WORK

Our retrospective analysis of maritime cyber security incident shows that even though this sector has not had the most, it has had some of the most severe consequences from cyber attacks. A wide variety of attack points against complex systems onboard and off-ship have been used. Most of them have attack vectors that typical for any land-based IT infrastructure and tend to be economically motivated where the goal is to hit as many targets as possible. At the same time, we can find more sophisticated, targeted attacks, where the goals seem to be disruption or espionage. We therefore have high complexity in both the systems themselves and the threat environment. These factors make cyber risk management very difficult and potentially costly for individual maritime organizations to handle alone Furthermore, current knowledge about incidents and emerging threats is fragmented and somewhat unavailable. We encourage further work and international collaboration on threat intelligence sharing, so that updated information about attack attempts, incidents, techniques and the people behind can support cyber security decision making, technology development and operations.

ACKOWLEDGEMENTS

This work has been supported by the Research Council of Norway through the projects "Cyber Security in Merchant Shipping - Service Evolution" with contract number 295969 and "Digital Ecosystems for Smart and Autonomous Ships" with contract number 309255. We thank the anonymous reviewers for critically reading the manuscript and suggesting improvements.

REFERENCES

1. Agius, M.: TM mum on whether cyber-attack affected ship, air registries, https://newsbook.com.mt/en/tm-mum-on-whether-cyber-attack-affected-ship-air-registries/, last accessed 2021/04/25.
2. Alcaide, J.I., Llave, R.G.: Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia. 45, 547–554 (2020). https://doi.org/10.1016/j.trpro.2020.03.058.
3. ASCStaff: Cyberattack on Clarkson's shipbroker reaffirms industry's vulnerability, https://www.logisticsmiddleeast.com/article-13696-cyberattack-on-clarksons-shipbroker-reaffirms-industrys-vulnerability, last accessed 2020/08/11.
4. Asplem, A.: Norwegian Maritime Cyber Resilience Centre (NORMA Cyber), (2021).
5. Athens Group: Cybersecurity – There Is No Silver Bullet, https://athensgroup.com/cybersecurity-there-is-no-silver-bullet/, last accessed 2020/08/11.
6. Aven, T.: On the meaning of a black swan in a risk context. Safety Science. 57, 44–51 (2013). https://doi.org/10.1016/j.ssci.2013.01.016.
7. Azzopardi, K.: Transport Malta cyber attack investigation has not yet determined whether data was stolen, http://www.maltatoday.com.mt/news/national/105593/watch_transport_malta_cyber_attack_investigation_has_not_yet_determined_whether_data_was_stolen, last accessed 2021/04/25.
8. Bartlett, P.: Cyber security – more focus required, says expert, https://www.seatrade-maritime.com/technology/cyber-security-more-focus-required-says-expert, last accessed 2021/04/25.
9. BBC: Red Funnel ferry firm's IT system hit by "malicious attack," https://www.bbc.com/news/uk-england-hampshire-54368110, (2020).
10. Bøe, E., Jordheim, H.: Politiet etterforsker dataangrepet mot Hurtigruten, https://e24.no/i/7KPeEK, last accessed 2021/04/25.
11. Boyes, H., Isbell, R.: Code of Practice: Cyber Security for Ships. IET Standard, Department for Transport (UK) (2017).
12. Buurma, C., Sebenius, A.: Ransomware Shuts U.S. Natural Gas Compressor Facility for Two Days, https://www.carriermanagement.com/news/2020/02/20/203485.htm, last accessed 2021/04/25.
13. Caprolu, M., Pietro, R.D., Raponi, S., Sciancalepore, S., Tedeschi, P.: Vessels Cybersecurity: Issues, Challenges, and the Road Ahead. IEEE Communications Magazine. 58, 6, 90–96 (2020). https://doi.org/10.1109/MCOM.001.1900632.
14. Cary, A.: Update: Hacker demands $200K ransom from Tri-Cities port to unlock computer data, https://www.tri-cityherald.com/news/local/crime/article247251569.html, last accessed 2021/04/25.
15. Cimpanu, C.: Ransomware Infection Cripples Shipping Giant COSCO's American Network, https://www.bleepingcomputer.com/news/security/ransomware-infection-cripples-shipping-giant-coscos-american-network/, last accessed 2021/04/25.
16. Cimpanu, C.: Shipping Firm Avoids Customer Data Dump in Last Year's Hack & Ransom Incident, https://www.bleepingcomputer.com/news/security/shipping-firm-avoids-customer-data-dump-in-last-years-hack-and-ransom-incident/, last accessed 2021/04/25.
17. Cimpanu, C.: US Coast Guard discloses Ryuk ransomware infection at maritime facility,

https://www.zdnet.com/article/us-coast-guard-discloses-ryuk-ransomware-infection-at-maritime-facility/, last accessed 2021/04/25.
18. Cimpean, D., Meire, J., Bouckaert, V., Casteele, S.V., Pelle, A., Hellebooge, L.: Analysis of Cyber Security Aspects in the Maritime Sector. (2011).
19. Coble, S.: Ransomware Attack on Shipping Giant, https://www.infosecurity-magazine.com:443/news/ransomware-attack-on-shipping-giant/, last accessed 2021/04/25.
20. CyberKeel: Maritime Cyber-Risks, https://maritimecyprus.files.wordpress.com/2015/06/maritime-cyber-risks.pdf, last accessed 2021/04/25.
21. Dragos, Inc.: Assessment of Ransomware Event at U.S. Pipeline Operator | Dragos, https://www.dragos.com/blog/industry-news/assessment-of-ransomware-event-at-u-s-pipeline-operator/, last accessed 2020/08/14.
22. Drougkas, A., Sarri, A., Kyranoudi, P., Zisi, A.: Port Cybersecurity: Good practices for cybersecurity in the maritime sector. (2019).
23. Dryad Global: Maritime Cyber Security & Threats March 2020 Week Three, https://dryadglobal.com/maritime-cyber-security-threats-2-2/, last accessed 2020/08/10.
24. ENISA: COVID19, https://www.enisa.europa.eu/topics/wfh-covid19, last accessed 2020/08/17.
25. Goud, N.: Cyber Attack on James Fisher and Sons, https://www.cybersecurity-insiders.com/cyber-attack-on-james-fisher-and-sons/, last accessed 2020/08/14.
26. Goud, N.: Ransomware attack on Norwegian Ship yard results in job loss to many, https://www.cybersecurity-insiders.com/ransomware-attack-on-norwegian-ship-yard-results-in-job-loss-to-many/, last accessed 2021/03/16.
27. GREAT: The Icefog APT: A Tale of Cloak and Three Daggers, https://securelist.com/the-icefog-apt-a-tale-of-cloak-and-three-daggers/57331/, last accessed 2020/08/10.
28. Greenberg, A.: The Untold Story of NotPetya, the Most Devastating Cyberattack in History, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, last accessed 2020/08/10.
29. Greenberg, M.D., Chalk, P., Willis, H.H., Khilko, I., Ortiz, D.S.: Maritime Terrorism. RAND Corporation (2006).
30. Grinter, M.: Maritime cyber-attacks up 900% in three years, http://www.hongkongmaritimehub.com/maritime-cyber-attacks-up-900-in-three-years/, last accessed 2020/08/10.
31. Hoo, K.J.S.: How Much Is Enough? A Risk-Management Approach to Computer Security. CISAC, Stanford University, UK (2000).
32. INTERPOL: Cybercrime: COVID-19 IMPACT, https://www.interpol.int/en/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf?inLanguage=eng-GB, last accessed 2021/03/16.
33. ISO/IEC 27000:2018: Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC (2018).
34. Jones, K.D., Tam, K., Papadaki, M.: Threats and Impacts in Maritime Cyber Security. Engineering & Technology Reference. 1, 1, (2016). https://doi.org/10.1049/etr.2015.0123.
35. Knox, J.: Coast Guard Commandant on Cyber in the maritime domain, https://mariners.coastguard.dodlive.mil/2015/06/15/6152015-coast-guard-commandant-on-cyber-in-the-maritime-domain/, last accessed 2020/08/11.
36. Kovacs, E.: UN Maritime Agency Hit by "Sophisticated Cyberattack," https://www.securityweek.com/un-maritime-agency-hit-sophisticated-cyberattack, last accessed 2021/04/25.
37. Kretschmann, L., Rødseth, Ø., Tjora, Å., Fuller, B.S., Noble, H., Horahan, J.: D9.2: Qualitative assessment. (2015).
38. Kristiansen, T.: DR: Kina hackede sig ind i Søfartsstyrelsen, https://shippingwatch.dk/Rederier/article7043149.ece, last accessed 2021/04/25.
39. Kristoffersen, P.B., Hartvigsen, T., Myrvang, P., Torjusen, A.: Digitale Sårbarheter Maritim Sektor. DNV-GL, Lysneutvalget (2015).
40. Lejon, J.: Kryptera.se Ransomware lista, https://kryptera.se/assets/uploads/2020/10/Ransomware-lista.pdf, last accessed 2021/03/23.
41. Lemos, R.: Coast Guard Warns Shipping Firms of Maritime Cyberattacks, https://www.darkreading.com/vulnerabilities---threats/coast-guard-warns-shipping-firms-of-maritime-cyberattacks/d/d-id/1335198, last accessed 2020/04/10.
42. Lloyd's List: Maritime Intelligence, https://lloydslist.maritimeintelligence.informa.com/, last accessed 2021/03/16.
43. Lubold, G., Volz, D.: Chinese Hackers Breach U.S. Navy Contractors - WSJ, https://www.wsj.com/articles/u-s-navy-is-struggling-to-fend-off-chinese-hackers-officials-say-11544783401, last accessed 2021/04/25.
44. Maritime Executive: Carnival Corporation Reports Ransomware Attack Accessed Data, https://www.maritime-executive.com/article/carnival-corporation-reports-ransomware-attack-accessed-data, last accessed 2021/04/25.
45. Maritime Executive: Hurtigruten Reports Passenger Data Exposed in Cyberattack, https://www.maritime-executive.com/article/hurtigruten-reports-passenger-data-exposed-in-cyberattack, last accessed 2021/04/25.
46. Maritime Executive: Naval Dome: Cyberattacks on OT Systems on the Rise, https://www.maritime-executive.com/article/naval-dome-cyberattacks-on-ot-systems-on-the-rise, last accessed 2021/04/25.
47. Maritime Executive: Ransomware Cripples IT Systems of Inland Port in Washington State, https://www.maritime-executive.com/article/ransomware-attack-cripples-systems-of-inland-port-in-washington-state, last accessed 2021/04/25.
48. Maritime Executive: Saipem's Servers Hit by Cyberattack, https://www.maritime-executive.com/article/saipem-s-servers-hit-by-cyberattack, last accessed 2021/03/16.
49. Matson: Matson Reports Cyber Attack, https://www.omnitrans.com/matson-reports-cyber-attack/, last accessed 2021/04/25.
50. Nesheim, D.A., Rødseth, Ø., Bernsmed, K., Frøystad, C., Meland, P.H.: D1.1 Risk Model and Analysis. (2017).
51. Nguyen, L.: Collaboration in the Shipping Industry: Innovation and Technology, https://informaconnect.com/epaper-collaboration-in-the-shipping-industry-innovation-and-technology/, last accessed 2021/04/25.
52. NSM: Helhetlig digitalt risikobilde 2019. (2019).
53. NSM: RISIKO 2020. (2020).
54. O'Dwyer, R.: IMO latest to fall victim to cyber attack, https://smartmaritimenetwork.com/2020/10/01/imo-latest-to-fall-victim-to-cyber-attack/, last accessed 2021/04/25.
55. Polychronis, K.: Cybersecurity at Sea. In: Otto, L. (ed.) Global Challenges in Maritime Security. p. 243 Springer International Publishing (2020).
56. PST: Nasjonal trusselvurdering 2020, https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/, last accessed 2021/04/25.
57. Redden, J.: Covid-19 has increased the chances of marine industry cyberassaults,

https://www.workboat.com/offshore/covid-19-has-increased-the-chances-of-marine-industry-cyberassaults, last accessed 2021/04/25.
58. Reynolds, Z.: Australian defence shipbuilder Austral victim of Iranian cyber attack, https://safetyatsea.net/news/news-safety/2018/australian-defence-shipbuilder-austral-victim-of-iranian-cyber-attack/.
59. Safety4Sea: 2018 Highlights: Major cyber attacks reported in maritime industry, https://safety4sea.com/cm-2018-highlights-major-cyber-attacks-reported-in-maritime-industry/, last accessed 2021/04/25.
60. Safety4Sea: Hurtigruten hit by cyber-attack, https://safety4sea.com/hurtigruten-hit-by-cyber-attack/, last accessed 2021/04/25.
61. Safety4Sea: Vard shipbuilder experiences ransomware attack, https://safety4sea.com/vard-shipbuilder-experiences-ransomware-attack/, last accessed 2021/04/25.
62. Schnelle, S.: Kartlegging av maritime hybride trusler. Kan bruk av stordata og sosial nettverksanalyse bidra til økt maritim situasjonsbevissthet? Forsvarets Høgskole (2018).
63. Secureworks: GOLD GALLEON: How a Nigerian Cyber Crew Plunders the Shipping Industry, https://www.secureworks.com/research/gold-galleon-how-a-nigerian-cyber-crew-plunders-the-shipping-industry, last accessed 2020/08/11.
64. Security: Maritime Industry Sees 400% Increase in Attempted Cyberattacks Since February 2020, https://www.securitymagazine.com/articles/92541-maritime-industry-sees-400-increase-in-attempted-cyberattacks-since-february-2020?v=preview, last accessed 2020/08/10.
65. Sfakianakis, A., Drougkas, A., Douligeris, C., Marinos, L., Lourenço, M., Raghimi, O.: ENISA threat landscape report 2018 - 15 top cyberthreats and trends. (2019).
66. Shauk, Z.: Malware on the offshore rig: Danger lurks where the chips fail, https://www.houstonchronicle.com/business/energy/article/Malware-on-the-offshore-rig-Danger-lurks-where-4470723.php, last accessed 2021/04/25.
67. Shen, C., Baker, J.: CMA CGM confirms ransomware attack, https://lloydslist.maritimeintelligence.informa.com/LL1134044/CMA-CGM-confirms-ransomware-attack, last accessed 2021/03/16.
68. Singh, H.: Cyber Security in Maritime Industry. University of Oslo (2019).
69. Taleb, N.N.N.: The Black Swan: The Impact of the Highly Improbable. Random House Publishing Group, New York (2010).
70. Tam, K., Jones, K.: Cyber-Risk Assessment for Autonomous Ships. In: 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). pp. 1–8 (2018). https://doi.org/10.1109/CyberSecPODS.2018.8560690.
71. Tam, K., Moara-Nkwe, K., Jones, K.: A Conceptual Cyber-Risk Assessment of Port Infastructure. Presented at the 2021 World of Shipping Portugal. An International Research Conference on Maritime Affairs , Parede, Portugal January 29 (2021).
72. Toogood, D.: Red Funnel siffers "malicious attack" on IT systems causing major disruption, https://www.islandecho.co.uk/red-funnel-suffers-malicious-attack-on-it-systems-causing-major-disruption/, last accessed 2021/04/25.
73. Torbati, J., Saul, Y.: Iran's top cargo shipping line says sanctions damage mounting, https://www.reuters.com/article/us-iran-sanctions-shipping-idUSBRE89L10X20121022, (2012).
74. UNCTAD: Review of Maritime Transport 2020, https://unctad.org/webflyer/review-maritime-transport-2020, last accessed 2021/04/25.
75. Vold, L.B.: Den Norske Krigsforsikring for Skib, https://www.warrisk.no/, last accessed 2021/04/25.
76. Volz, D.: Chinese Hackers Target Universities in Pursuit of Maritime Military Secrets, https://www.wsj.com/articles/chinese-hackers-target-universities-in-pursuit-of-maritime-military-secrets-11551781800, (2019).
77. Walker, J.: AIDA Cruise Ships Under Cyber Attack - Are Costa Ships Also Affected?, https://www.cruiselawnews.com/2020/12/articles/cyber-attacks/aida-cruise-ships-under-cyber-attack-are-costa-ships-also-affected/, last accessed 2021/04/25.
78. Walker, J., Spencer, J.: Cyber Marine: Risks & Loss Scenarios, http://www.marineclaimsconference.com/imcc-docs/docs/Cyber%20workshop.pdf.
79. Wallace, T., Mesko, F.: The Odessa Network Mapping Facilitators of Russian and Ukrainian Arms Transfers, https://globalinitiative.net/analysis/the-odessa-network-mapping-facilitators-of-russian-and-ukrainian-arms-transfers/, last accessed 2021/04/25.
80. Warrick, J., Nakashima, E.: Officials: Israel linked to a disruptive cyberattack on Iranian port facility, https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html, (2020).
81. Weldemichael, A.T., Schneider, P., Winner, A.C.: Maritime Terrorism and Piracy in the Indian Ocean Region. Routledge (2017).
82. Windward: AIS Data on the High Seas: An Analysis of the Magnitude and Implications of Growing Data Manipulation at Sea. (2014).
83. Wohlin, C.: Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering. In: Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering. Association for Computing Machinery, New York, NY, USA (2014). https://doi.org/10.1145/2601248.2601268.