Claims of State-Sponsored Cyberattack in the Maritime Industry

A Oruc* M.Sc. MIET MIMarEST

** Norwegian University of Science and Technology, Norway*
* Corresponding Author. Email: aybars.oruc@ntnu.no

Synopsis

Developments in technology bring inherent risks along with convenience. Undoubtedly, cyberattacks constitute one potentially serious risk. While a stereotypical scenario involves a curious teenager sitting in front of his computer at home, a much more critical threat comes from experienced professionals, supported by states, who are specially trained and who have the necessary technological equipment to do great harm. These cyberattacks exert a negative impact on the maritime industry due to the wide usage area of both information technology (IT) and operational technology (OT) systems. On a related note, opponents of autonomous ship projects can effectively cite the weaknesses detected in navigation systems onboard ships. Examination of cyberattacks in the maritime industry as reflected in the press or in academic studies reveals claims that some of these attacks are state-sponsored. However, no country has to date accepted responsibility for such cyberattacks. Although those targeted by such accusations have neither confirmed nor rejected responsibility, the nature of the attacks – sophisticated or requiring high-cost equipment – raises the possibility that behind the attacks are countries that may have conducted research studies for defensive or offensive purposes. China, Iran, North Korea, Russia and Turkey have been named among the countries carrying out cyberattacks on the maritime industry. It is envisaged that these attacks are based on motivations such as information theft, defence research or sabotage of exploration for underground sources. Among the cyberattacks on vessels that have been assessed as state-sponsored, the most common have involved GPS jamming, rendering GPS useless, and GPS spoofing that causes the GPS to report an incorrect position for a ship at sea. This study examines the cyberattacks on the maritime industry that are asserted as state-sponsored as well as the parties involved in these attacks and the possible objectives of those parties.

Keywords: Maritime; ship; cybersecurity; state-sponsored cyberattack

1. Introduction

Cybersecurity concerns are growing along with the advancement of technologies, the extensive use of digital and cyber-physical networks on ships, and autonomous ship initiatives such as the Maritime Unmanned Navigation through Intelligence in Networks (MUNIN), Autosea and Yara Birkeland (Brekke *et al.* 2019; MUNIN 2012; Yara International 2018). Furthermore, cybersecurity has led other maritime-related organisations to become involved due to cyber incidents both at sea and on shore.

Non-profit organisations such as the Oil Companies International Marine Forum (OCIMF) and Chemical Distribution Institute (CDI) have begun to pressure tanker operators to take action against cyber threats by offering vetting services for the commercial operations of tanker operators. The Tanker Management and Self-Assessment (TMSA) and Ship Inspection Report Program (SIRE) questionnaires developed by OCIMF have been enhanced with queries relevant to cybersecurity. Specific cybersecurity questions have been incorporated into CDI's Ship Inspection Report (SIR) questionnaire. RightShip, which offers vetting services for dry cargo ships, has introduced cybersecurity questions into its questionnaire as well (Oruc 2019).

The maritime sector has also seen initiatives for examining cybersecurity problems, such as 'Cyber-MAR' (Cyber-MAR 2019), 'Maritime Cyber Resilience' (MarCy) (CRISTIN 2020), 'Cyber Security of Maritime ICT-Based Systems' (University of Rijeka 2019) and the project of 'Centre for Maritime Cyber Security' at Tallinn University of Technology (CORDIS 2020). Countries have also started developing their own research facilities. The Danish Maritime Cybersecurity Unit was established by the Danish Maritime Authority in June 2018 (Danish Maritime Cybersecurity Unit 2019). The Maritime Cybersecurity Operations Centre was opened in 2019 by the Maritime and Port Authority of Singapore (Maritime and Port Authority of Singapore 2019). Lastly, the International Maritime Organization (IMO) has not been indifferent to developments. In accordance with International Safety Management (ISM) Code, all maritime companies are mandated to insert a 'Guidelines on Maritime Cyber Risk Management' into their safety management system, and this will be checked in the first annual verification of the company's Document of Compliance (DoC) as of 1 January 2021 (IMO 2017).

Individuals or teams may arrange cyberattacks for varied purposes. Additionally, governments are pursuing research not only on cybersecurity but also investigating purposes for cyberattack. Because of the technical facilities and qualified staff that states can offer, state-sponsored cyberattacks are highly sophisticated, yielding more serious results than attacks promoted by individuals or private groups. For instance, the Center for Advanced Defense (C4ADS) reported that the alleged attacks by Russia have affected 1,311 civilian vessels in about a 30-month period (C4ADS 2019). In other words, attacks are also harming merchant vessels.

Author's Biography
Aybars Oruc is a Marine Engineer. After he had worked as an engineer on different types of merchant vessels such as aframax tanker, LPG tanker and container vessel, he worked as HSEQ Coordinator, and then HSEQ Superintendent in a tanker management company for 4 years. He is a Ph.D. candidate at the NTNU. His research field is maritime cyber security.

https://doi.org/10.24868/issn.2515-818X.2020.021

Although researchers have investigated the subject of maritime cybersecurity, current academic studies to date are not sufficient. While considerable work has examined state-sponsored attacks, no studies have been identified that focus on these attacks within the maritime industry. Therefore, this paper intends to contribute to the development of the literature.

2. Cyberattacks in General Terms

The International Organization for Standardization (ISO) defines cyberattack as an attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset (ISO 2018). Cyberattacks may be carried out against companies or governments as well as individuals. Such attacks can be launched by computers, smartphones, tablets or electronic equipment developed for cyberattacks. The types of cyberattacks are divided into two categories: 'Targeted Attacks' and 'Untargeted Attacks'.

- Targeted Attacks: In such attacks, a company or a ship's systems and data are the intended targets (BIMCO 2018).
- Untargeted Attacks: In this kind of attack, the systems and data belonging to a company or ship are among many potential targets (BIMCO 2018).

The concept of 'Maritime Security' covers illegal and planned attacks against ships, port facilities and crew. The International Ship and Port Facility Security (ISPS) code was published to deter terror rampages against ships, ports and facilities after the 'September 11' attacks. 'Maritime Cybersecurity' is investigated by IMO under the Maritime Security category. The Maritime Safety Committee (MSC) and Facilitation Committee (FAL) publish regulations and guidance, which are then circulated to the maritime sector.

2.1. Typical Characteristics of Cyber Threats

As attack levels increase from level 1 to level 5, they become more sophisticated. Level advancement implies not only improved attack methods but also an increase in the qualification of aggressive groups. A level 1 attack can be carried out by a teenager sitting in front of a computer at home, even for entertainment purposes, while at level 5, the attackers appear to be more well-informed and experienced as well as supported by countries for political or military purposes. In other words, such high-level attacks are state-sponsored. Table 1 displays the five levels of cyber threats, dividing actors into five categories (Bodeau *et al.* 2010).

Table 1: Typical characteristics of cyber threats (Bodeau *et al.* 2010)

Level	Typical Threat Actors	Typical Intents of Threat Actors
1 Cyber Vandalism	Hackers, taggers, and 'script kiddies'; small disaffected groups of the above	Disrupt and/or embarrass the victimised organisation or type of organisation (e.g. a specific department or federal government as a whole)
2 Cyber Theft / Crime	Individuals or small, loosely affiliated groups; political or ideological activists; terrorists; domestic insiders; industrial espionage; spammers	Obtain critical information and/or usurp or disrupt the organisation's business or mission functions for profit or ideological cause
3 Cyber Incursion / Surveillance	Nation-state government entity; patriotic hacker group; sophisticated terrorist group; professional organised criminal enterprise	Increase knowledge of general infrastructure; plant seeds for future attacks; obtain or modify specific information and/or disrupt cyber resources, specifically resources associated with missions or even information types
4 Cyber Sabotage / Espionage	Professional intelligence organisation or military service operative	Obtain specific high-value information, undermine or impede critical aspects of a mission, programme or enterprise, or place itself in a position to do so in the future
5 Cyber Conflict / Warfare	Nation-state military, possibly supported by their intelligence service; very sophisticated and capable insurgent or terrorist group	Severely undermine or destroy an organisation's use of its mission, information and/or infrastructure

2.2. Implemented Cyberattack Methods for State-Sponsored Attacks

The current technological era has inaugurated an age of cyber threats as well. Cyberattacks are carried out by malicious individuals, groups or state-sponsored organisations using many different methods. This section explains the techniques employed in allegedly state-sponsored cyberattacks in the maritime industry.

2.2.1. GPS Jamming

According to the C4ADS, Global Positioning System (GPS) jamming is also called brute force jamming (C4ADS 2019). This type of attack involves GPS jamming where radio noise is broadcast on the GPS frequency, blocking the use of GPS and potentially disabling a vessel's ability to navigate safely (Vistiaho 2017). However, a GPS failure alert may notify an officer of the problem. Further countermeasures include anti-jamming devices to use against GPS jamming attacks. Because the applications of these devices are currently available only to land vehicles, no such implementation currently exists for ships.

2.2.2. GPS Spoofing

A GPS spoofing attack causes the targeted GPS to display the wrong location by receiving a false GPS signal (Lund *et al.* 2018). Because an officer on the bridge of a ship might not detect this type of attack, such an attack is more dangerous than a GPS jamming attack (Humphreys *et al.* 2008). An undetected attack of this nature endangers the safe navigation of a ship.

2.2.3. Spear Phishing

In this scenario, the attacker sends an e-mail to the victim's account. The target may be an individual, department or company. The malevolent e-mail, which appears to be sent from a reputable institution such as a bank, an e-mail provider or a university, often requests the recipient to click a link. The purpose of this attack is personal data theft by prompting the victim to enter the desired information on a pop-up page, which might include passwords, personal information and credit card numbers. Additionally, a customised e-mail may be sent that might contain the name, logo or personal details of the victim (Sophos 2013).

2.2.4. Malware

Harmful software, also known by the generic term malware, includes viruses, worms, trojans, spyware, etc. Malware is used to damage infected devices or files and to steal personal data, photos and videos (Sophos 2013). Malware usually attacks users through warez software and is easily accessed by attackers through files downloaded via torrent, USB (Universal Serial Bus) memory sticks or any visited websites. Connecting a mobile phone to a ship's computer to charge can cause the virus to infiltrate the ship's network and may lead to the crashing of some systems like the ship's Electronic Chart Display and Information System (ECDIS). Many types of malware are a current threat to users. Of these, the Petya virus, used for ransomware attacks, should be specifically examined, considering the damage it has caused to Maersk, making its name infamous in the maritime sector. Essentially, Petya renders all files on the victim's computer inaccessible, meaning these files cannot be accessed unless a ransom is paid to the Bitcoin account issued by the attacker (Trend Micro 2017). The Danish maritime company Maersk suffered about $300 million in damages from a Petya-based attack (Fadilpašić 2017). On a related note, another ransomware product, SamSam software, was used in a cyberattack on the Port of San Diego (Senzee 2019).

2.3. Cyber Incidents in the Maritime Industry

Cyberattacks in the maritime sector have been on the increase, particularly in recent years. The threats are targeting offices, ports and even ships. Attacks, especially when levied against ships, cause more concern because they can lead to injury of individuals and marine pollution. As an additional cautionary note, the possibility of cyberattacks is a critical question mark in autonomous ship projects, adding urgency to the necessity of a closer review of cyberattacks. The maritime sector is experiencing both targeted and untargeted attacks. In particular, the ransomware attack that caused Maersk to lose $300 million serves as a critical warning for untargeted attacks in the maritime industry. In the area of information theft, attacks can be carried out against the offices of maritime companies, and attackers can demand ransom. Furthermore, attacks may allegedly be supported by a state for both political and military purposes. It is possible to claim that attacks on the GPS systems of ships in particular are supported by governments because of being sophisticated of GPS attacks. In addition to the GPS attacks discussed here, the event of attackers taking complete possession of a massive container vessel in 2017 received extensive news coverage (Blake 2017). Ports represent another area in the maritime sector to be targeted. In general, port attacks are planned as part of carrying out smuggling activities. Table 2, corresponding to the years 2011-2019, reveals how cyberattacks reflected in the press have increased, especially in recent years. The table includes a total of 22 incidents, 17 of which were shore-based attacks, and five of which were targeted towards vessels. (A dash [-] in the table means 'particular information is unknown or does not apply').

Table 2: Cyberattacks in the maritime industry

Year	Impact Area	Organisation / Location	Affected System	Method	Impact	Reference	Accused State
2011	Shore	IRISL	Cargo tracking system	-	Operational interruption	(Torbati and Saul 2012) (Cyber Keel 2014)	-
2011	Shore	Ports of Belgium and the Netherlands	Container tracking system	Spear phishing	Smuggling	(Bateman 2013) (European Cybercrime Centre 2013)	-
2012	Shore	Australian Customs and Border Protection Service Agency	Container tracking system	-	Smuggling	(Kochetkova 2015)	-
2012	Shore	Danish Maritime Authority	Network	Spear phishing	Data theft	(Cyber Keel 2014) (The Local 2014)	China
2013	Vessel	Gulf of Mexico	Network	Malware	Operational interruption	(Shauk 2013)	-
2016	Vessel	Coast off South Korea	GPS	GPS jamming	Blocking GPS signal	(Saul 2017) (Graham 2017)	North Korea
2016	Shore	A Broker’s e-mail account	E-mail	-	$500,000 financial loss	(Belmont 2016)	-
2017	Shore	Clarksons	Network	-	Data theft	(Leyden 2018) (Esage 2018)	-
2017	Shore	Maersk	Network	Ransomware (Petya)	$250-300 million financial loss, data contamination	(Maersk 2017) (Tung 2018)	-
2017	Vessel	En route from Cyprus to Djibouti	Navigation system	-	Full control by attackers	(Blake 2017)	-
2017	Vessel	Coast off Russia	GPS	GPS spoofing	Wrong GPS location	(Goward 2017) (Humphreys 2017)	Russia
2017	Shore	BW Group	Network	-	Operational interruption	(Mohindru 2017) (Ngai 2017)	-
2018	Shore	Svitzer Australia	E-mail	E-Mail forwarding	Data theft	(WMN 2018b)	-
2018	Shore	COSCO Shipping	E-mail, phone, website, network	Ransomware	Operational interruption	(WMN 2018a)	-
2018	Shore	Austal	Network	-	Data theft	(Maritime Executive 2017)	-
2018	Shore	Port of Barcelona	-	-	-	(IMarEST 2018)	-
2018	Shore	Port of San Diego	Network	Ransomware (SamSam)	Data contamination	(Senzee 2019)	Iran
2018	Vessel	Coast off Cyprus	GPS	GPS Jamming	-	(2018 cited Denizcilik Bilgileri 2018)	Turkey
2019	Shore	James Fisher and Sons	Network	-	Data contamination	(Safety4Sea 2019)	-
2019	Shore	Princess & Holland America	E-mail	-	Data theft	(Coble 2020)	-
2019	Shore	Crew and Concierge	Network	-	Data theft	(Safety4Sea 2020)	-
2019	Shore	London Offshore Consultants	Network	Ransomware	Operational interruption	(Chambers 2020)	-

3. State-Sponsored Claims for Cyberattacks

Five countries are suspected of having carried out state-sponsored cyberattacks on the maritime industry. The suspects include China, Iran, North Korea, Russia and Turkey.

3.1. China

In April 2012, the Danish Maritime Authority was subjected to a critical cyberattack, though the cyberattack was not publicly announced until September 2014 (Cyber Keel 2014). The cybersecurity breach under discussion was discovered in 2014 after an American IT specialist reported it. Investigations revealed that when a Danish Maritime Authority employee opened a PDF file containing the virus that was sent as an e-mail attachment, the virus corrupted the employee's computer and infected the attached network. Investigation showed that the attackers wanted confidential information regarding Danish shipping companies and the merchant fleet. The entire network system was shut down for several days while new anti-virus programmes were installed. Danish Defence Intelligence Service announced that this attack was highly sophisticated, that it was state-sponsored and that evidence pointed to the attack being organized by China. The Chinese Embassy in Copenhagen refuted all accusations and announced that Chinese officials did not know about this attack (The Local 2014).

This targeted attack illustrates the spear-phishing method. Corporate or government staff must be mindful of the potential for this type of attack, taking precautions when reviewing e-mails received from unrecognised parties. Unfortunately, in this situation, if the American IT expert had not alerted the Danish Maritime Authority, the attackers might have been able to steal additional amounts of sensitive information for some time longer. Following this event and after the 2017 cyberattack that caused substantial damage to Maersk, one of the world's leading maritime firms, the Danish government took heed and took steps to create an official cybersecurity unit.

Thus, in June 2018, the Danish Maritime Authority established the Danish Maritime Cybersecurity Unit. This unit, which serves players in the Danish maritime sector, also organises professional workshops and conferences especially for the maritime sector regarding cybersecurity. Not only do they develop strategy, but they play an essential role in implementing the formulated plans. An example of this unit's efforts is the document 'Cyber and Information Strategy for the Maritime Sector', covering 2019-2022 (Danish Maritime Cybersecurity Unit 2019).

3.2. Iran

The Port of San Diego in the USA was subjected to cyberattack on 25 September 2018 (IMarEST 2018). This incident, identified as a ransomware attack named SamSam, affected over 200 victims including hospitals, municipalities and public agencies as well as the port itself, inflicting $30 million in economic damage (U.S. Department of Justice 2018). Two Iranians orchestrated the attack, which demanded ransom over Bitcoin. The investigators of Federal Bureau of Investigation (FBI) consider such attacks to be highly sophisticated as well as supported by Iran as a state-sponsored cyberattack (ABS 2020; Senzee 2019).

3.3. North Korea

In April 2016, South Korea announced that around 280 vessels were under a GPS jamming attack that forced the affected vessels to return to port (Graham 2017). South Korea claimed that this attack was organised by North Korea. However, North Korea denied this claim (Saul 2017). Even if it cannot be verified with certainty that North Korea carried out this attack, investigations that revealed the complexity of the attack showed it to be highly sophisticated. Moreover, GPS jamming attacks cannot be carried out using a single computer but require specific technical equipment. For this reason, this incident was likely to be a state-sponsored attack. eLoran has been developed against GPS jamming and spoofing attacks by South Korea (Cozzens 2020).

3.4. Russia

On 22 June 2017, a ship off the Novorossiysk-Russia shore notified the U.S. Coast Guard Navigation Center about a problem with GPS. According to the report, the ship's GPS showed the wrong position, a problem that also affected more than 20 other vessels in the area. Figure 1 illustrates the spoofed vessel location and actual vessel location in this incident. The ship's GPS gave a position inland (near the Gelendyhik Airport), but the vessel was drifting more than 25 NM (nautical mile) from the given coordinates. Various investigations revealed that this was a GPS spoofing cyberattack. Experts claimed that Russia had organised the attack to test the defence system against American missiles (Humphreys 2017; Goward 2017).

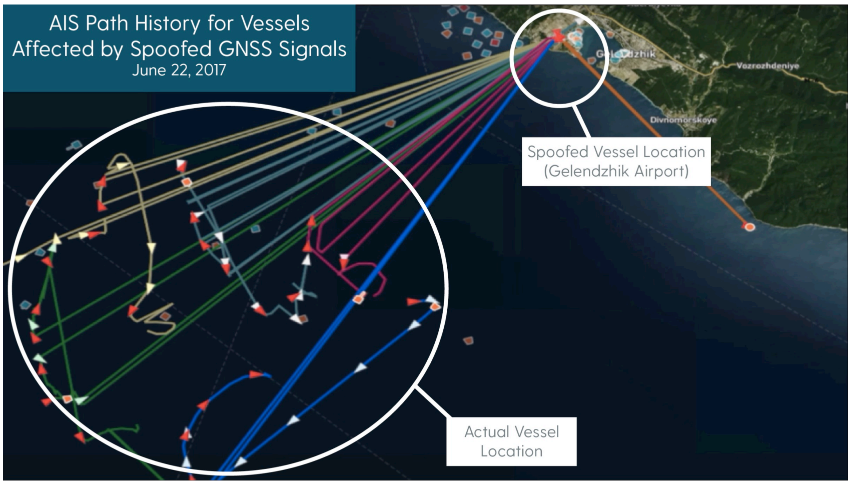

Figure 1: Actual and Spoofed Vessel Locations (C4ADS 2019)

GPS attacks, by their nature, cannot be carried out only with computers but require additional technical equipment as mentioned above. Although the attack was not confirmed by the Russian government, it could be inferred that the attack was state-sponsored, given the scope of the attack and the number of ships affected.

This case that Russia supposedly created and that the press has reported is not an isolated one in terms of such allegations. In 2019, the U.S.-based non-profit Center for Advanced Defence Studies (C4ADS) released a comprehensive report entitled ‘Above Us Only Stars’. This report estimated that a total of 1,311 civilian vessels were damaged by Global Navigation Satellite System (GNSS) spoofing attacks conducted by Russia between February 2016 and November 2018. As per C4ADS, such GNSS spoofing activities are potentially carried out for defensive reasons concerning strategic locations in Russia or for checking that country’s ability to attack (C4ADS 2019).

3.5. Turkey

As per the researches, numerous hydrocarbon reserves may be located in the Mediterranean around the island of Cyprus (Faustmann *et al.* 2012). In this sense, on 26 January 2007, the Greek Cypriot Southern Cyprus Administration (GCASC) separated the region identified as its own exclusive economic zone (EEZ) into 13 zones and began licensing those zones to oil exploration firms (Arıdemir and Allı 2019). These firms thus obtained the privilege to explore for hydrocarbons in the areas where they were licensed. However, several of the identified areas overlap with the Turkish continental shelf and the EEZ of the Turkish Republic of Northern Cyprus (TRNC). Figure 2 illustrates the EEZ claimed by the GCASC, the Turkish continental shelf alleged by Turkey, the EEZ claimed by the TRNC and the disputed zones (Yilmaz 2019).

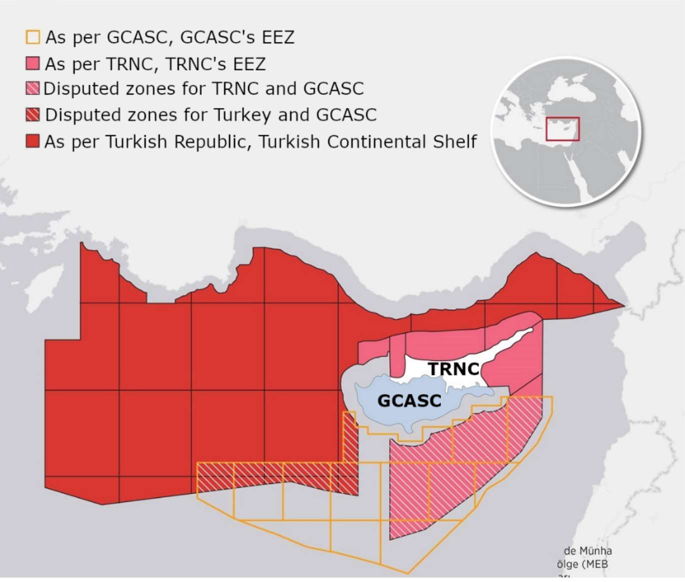
□ As per GCASC, GCASC's EEZ
■ As per TRNC, TRNC's EEZ
▨ Disputed zones for TRNC and GCASC
▨ Disputed zones for Turkey and GCASC
■ As per Turkish Republic, Turkish Continental Shelf
TRNC
GCASC
de Münha
ölge (MEB

Figure 2: Disputed Zones and EEZs of the TRNC and the GCASC (Yilmaz 2019)

The Republic of Turkey never considered it acceptable to perform reserve research in the disputed regions. First, on 17 March 2002, the Turkish Navy banned the 'Northern Access' research vessel from carrying out seismic studies on the Turkish continental shelf, and the Turkish Navy imposed similar limitations in 2016 and 2018 (Ozkaya 2018). Ships of the Republic of Turkey, the 'Yavuz', 'Fatih' and 'Barbaros Hayrettin Pasha', are continuing to conduct hydrocarbon exploration operations within the disputed areas around the island of Cyprus.

During 2018, multiple incidents involving GPS interference took place across the island of Cyprus. The NATO Shipping Centre and U.S. Maritime Administration (MARAD) confirm these interruptions (U.S. Maritime Administration 2018; NATO Shipping Center 2018). Figure 3 shows the GPS interference that has occurred off Cyprus. (NATO Shipping Center 2018)

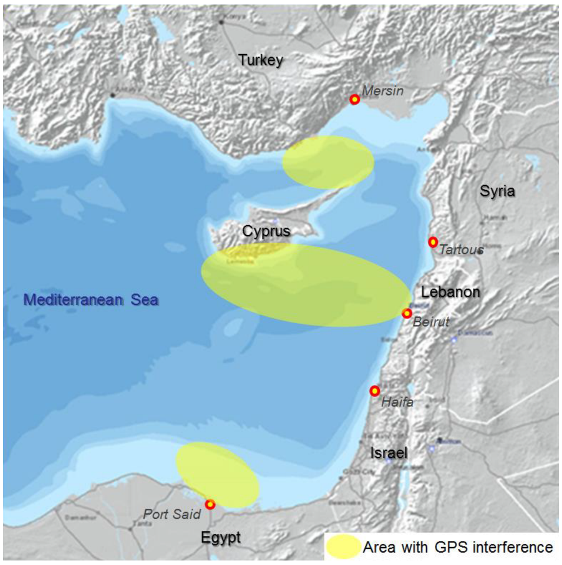

Figure 3: Area with GPS Interference (NATO Shipping Center 2018)

Additionally, on the organisation's website, the U.S. Coast Guard Navigation Center (USCG NAVCEN) posts numerous GPS interference problems received in reports. Around 2018 and 2019, three GPS problems were recorded from the Cyprus region. No reason for two of these was identified, and they were reported as 'Unknown Interference' in the (USCG NAVCEN 2020) records.

The Norwegian Shipowner's Mutual War Risks Insurance report focuses on the probability of GPS interference occurring around the island of Cyprus caused by Turkey (2018 cited Denizcilik Bilgileri 2018). Considering together the records of USCG NAVCEN, MARAD and the NATO Shipping Centre from the year 2018, the absence of any clarification of the origin of most of the GPS problems encountered, the frequency of GPS interference that generally occurred in the disputed area and the Turkish Navy's interference towards the research vessels, it is probable that the goal was to prevent the research vessels from performing hydrocarbon research in the controversial region by disrupting GPS signals using a GPS jamming attack by the Republic of Turkey. This possibility, though, remains to be admitted by the Republic of Turkey.

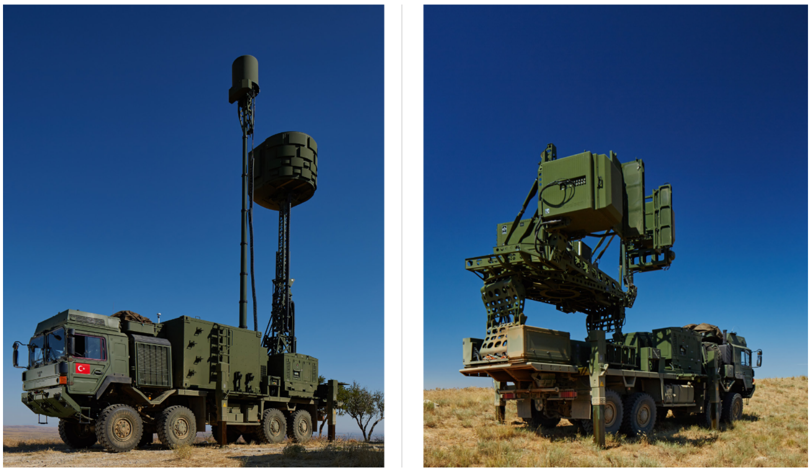

Figure 4: KORAL - Turkish Electronic Warfare Vehicle (Aselsan 2017)

'KORAL', developed by Aselsan, has been used by the Turkish army for electronic warfare since 2016 (Sabah 2016). Figure 4 shows photos of 'KORAL'. This system has various capabilities, including launching a GPS jamming attack. If the claim in 2018 was correct, KORAL must have been used in the attacks against the research vessels in the vicinity of Cyprus. In 2019, another electronic warfare vehicle developed by Aselsan, called 'REDET-II', was delivered to the Turkish army (C4Defence 2019).

4. Findings

Twenty-two maritime cybersecurity incidents were detected between 2011 and 2019. Even though 17 of these were shore-based incidents, involving ports and shipping companies, five of them were attacks on vessels at sea. However, it is highly probable that the attacks on vessels have been even more widespread than those reported. Examination of USCG NAVCEN records found that between 4 February 2017 and 13 March 2020, 68 cases involving GPS interference were recorded for marine-type devices. Of those 68 records, 56 were reported as 'Unknown Interference' after investigation. In other words, no explanation was stated for these GPS-related troubles.

China, Iran, North Korea, Russia and Turkey are alleged to have carried out attacks affecting the maritime industry. Russia is believed to be capable of carrying out GPS spoofing attacks. Turkey and North Korea are suspected of GPS jamming attacks. China and Iran are asserted to have the capacity to carry out shore-based cyberattacks.

Turkey is allegedly accused of trying to blockade hydrocarbon exploration activities around the island of Cyprus, and Russia is alleged to be causing GPS interference for the intent of defence or researching electronic warfare technologies.

Any claims or state-sponsored allegations in incidents related to the maritime industry have not been accepted by the countries so accused.

The alleged state-sponsored ship attacks under consideration were limited to GPS.

In 2012, the attack on the Danish Maritime Authority, allegedly planned by the Chinese government, was the first to target a governmental organisation directly related to the maritime industry.

The GPS jamming attack, which was supposedly carried out by North Korea in 2016 and impacted more than 280 vessels, came to light as the incident that affected the most vessels at one time.

Between February 2016 and November 2018, a total of 1,311 civilian vessels' navigation systems were allegedly affected due to Russian-organised GNSS spoofing attacks. Taking into consideration the current statements, Russia appears to be the state behind most attacks on marine vessels.

The attacks influence not only state institutions but also private industry and individuals. Since GPS attacks threaten a region, they impact all vessels in the subject area. In comparison, attacks against land facilities aim at obtaining data or destroying a facility's computer infrastructure.

Cyber incident record for war ships are not available. It is likely that war ships are affected from cyber incidents, however, these incidents are not disclosed by navies suffering such attacks. Leaders are likely covering up the attacks to avoid further damage publicly.

5. Conclusion

Advances in technology have often influenced aggressor states' methods of attack. Organisations or governments can now hack information using cyberattacks without the requirement for a spy, or they can limit ships' ability to navigate safely by removing GPS capability in an area. State-sponsored attacks threaten to exert a detrimental effect on merchant shipping, an impact likely to worsen if various states' attack capabilities are strengthened over the coming years and more countries begin to participate in this activity. Added to the difficulty is the reality that states typically cover up such attacks. Throughout the research endeavour, attempts were made to collect information via e-mail and telephone from different organisations. The e-mails sent, however, received either no answer or feedback saying that no details could be provided. Further research could evaluate the efforts of states to counter possible cyberattacks impacting the maritime industry. An additional topic for investigation would be to examine how such attacks can affect merchant shipping and assess the detrimental impacts on the global supply chain.

Acknowledgements

This study was supported by the project 'Maritime Cyber Resilience' (MarCy) funded by the Research Council of Norway.

References

ABS, 2020. *IMO 2021 cyber risk management guidelines - What to know and how to comply [PowerPoint presentation]*.

Arıdemir, H., and Allı, C., 2019. An analysis of the exclusive economic zone debates in Eastern Mediterranean region. *Journal of Economics Business and Political Researches,* 4 (10), 188–202. Available from: https://dergipark.org.tr/en/download/article-file/829290 [Accessed 4 May 2020].

Aselsan, 2017. *KORAL mobil radar EH (elektronik harp) sistemi* [online]. Available from: https://www.aselsan.com.tr/1a8b7437-1ca0-4652-bd30-d71640c857b2.pdf [Accessed 22 July 2020].

Bateman, T., 2013. *Police warn over drugs cyber-attack* [online]. Available from: https://www.bbc.com/news/world-europe-24539417 [Accessed 25 March 2020].

Belmont, K.B., 2016. *Cyber Cases in the Maritime Environment*.

BIMCO, 2018. *The guidelines on cyber security onboard ships*. 3rd ed.

Blake, T., 2017. *Hackers took 'full control' of container ship's navigation systems for 10 hours - IHS Fairplay | RNTF* [online]. Available from: https://rntfnd.org/2017/11/25/hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-ihs-fairplay/ [Accessed 25 March 2020].

Bodeau, D.J., Graubart, R., and Fabius-Greene, J., 2010. Improving cyber security and mission assurance via cyber preparedness (Cyber Prep) levels*. International conference on social computing,* 20-22 August 2010 Minneapolis.

Brekke, E.F*., et al.,* 2019. The Autosea project: Developing closed-loop target tracking and collision avoidance systems. *Journal of Physics: Conference Series*.

C4ADS, 2019. *Above us only stars. Exposing GPS spoofing in Russia and Syria*.

C4Defence, 2019. *KORAL'a REDET-II desteği* [online]. Available from: https://www.c4defence.com/Arsiv/korala-redetii-destegi/8940/1 [Accessed 22 July 2020].

Chambers, S., 2020. *London Offshore Consultants suffers ransomware attack* [online]. Available from: https://splash247.com/london-offshore-consultants-suffers-ransomware-attack/ [Accessed 25 March 2020].

Coble, S., 2020. *Carnival Cruise Lines hacked* [online]. Available from: https://www.infosecurity-magazine.com/news/carnival-cruise-lines-hacked/ [Accessed 25 March 2020].

CORDIS, 2020. *ERA Chair in Maritime Cyber Security at Tallinn University of Technology* [online]. Available from: https://cordis.europa.eu/project/id/952360 [Accessed 21 August 2020].

Cozzens, T., 2020. *UrsaNav installs eLoran testbed in South Korea* [online]. Available from: https://www.gpsworld.com/ursanav-installs-eloran-testbed-in-south-korea/ [Accessed 23 July 2020].

CRISTIN, 2020. *Maritime Cyber Resilience* [online]. Available from: https://app.cristin.no/projects/show.jsf?id=2057306 [Accessed 30 July 2020].

Cyber Keel, 2014. *Maritime cyber-risks*.

Cyber-MAR, 2019. *About* [online]. Available from: https://www.cyber-mar.eu/about/ [Accessed 25 April 2020].

Danish Maritime Cybersecurity Unit, 2019. *Cyber and information strategy for the maritime sector 2019 - 2022* [online]. Available from: https://www.dma.dk/Documents/Publikationer/Cyber%20and%20Information%20Security%20Strategy%20for%20the%20Maritime%20Sector.pdf [Accessed 4 January 2020].

Denizcilik Bilgileri, 2018. *Türkiye GPS jammer ile Yunan araştırma gemilerini engelliyor mu?* [online]. Available from: https://www.denizcilikbilgileri.com/turkiye-gps-jammer-ile-yunan-arastirma-gemilerini-engelliyor-mu/ [Accessed 4 February 2020].

Eastern Mediterranean Sea-GPS Interference, 2018 [online]. *U.S. Maritime Administration.* Available from: https://www.maritime.dot.gov/content/2018-014-eastern-mediterranean-sea-gps-interference [Accessed 8 April 2020].

Electronic interferences assesment, 2018 [online]. *NATO Shipping Center.* Available from: https://shipping.nato.int/nsc/page10303037.aspx [Accessed 8 April 2020].

Esage, A., 2018. *British shipping company Clarksons hacked* [online]. Available from: https://www.securitynewspaper.com/2018/08/02/british-shipping-company-clarksons-hacked/ [Accessed 26 March 2020].

European Cybercrime Centre, 2013. *Hackers deployed to facilitate drugs smuggling* [online]. *EC3.* Available from: https://www.europol.europa.eu/sites/default/files/documents/cyberbits_04_ocean13.pdf [Accessed 8 May 2020].

Fadilpašić, S., 2017. *Shipping giant Maersk reveals $300 million cyber-attack loss* [online]. Available from: https://www.itproportal.com/news/maersk-lost-300-million-due-to-notpetya/ [Accessed 25 April 2020].

Faustmann, H., Gurel, A., and Reichberg, G.M., eds., 2012. *Cyprus Offshore Hydrocarbons: Regional Politics and Wealth Distribution.* Peace Research Institute.

Goward, D., 2017. *Mass GPS Spoofing Attack in Black Sea?* [online]. Available from: https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea [Accessed 25 April 2020].

Graham, L., 2017. *Shipping industry vulnerable to cyber attacks and GPS jamming* [online]. Available from: https://www.cnbc.com/2017/02/01/shipping-industry-vulnerable-to-cyber-attacks-and-gps-jamming.html [Accessed 23 March 2020].

Humphreys, T., 2017. *Ships fooled in GPS spoofing attack suggest Russian cyberweapon* [online]. Available from: https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/ [Accessed 23 March 2020].

Humphreys, T.E*., et al.,* 2008. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *International technical meeting of the satellite division of the institute of navigation,* 16-19 September 2008 Savannah.

IMarEST, 2018. *Ports of Barcelona and San Diego hit by cyber attacks* [online]. Available from: https://www.imarest.org/themarineprofessional/item/4473-ports-of-barcelona-and-san-diego-hit-by-cyber-attacks [Accessed 13 April 2020].

IMO, 2017. *Resolution MSC.428(98).*

ISO, 2018. *ISO/IEC 27000:2018(en) Information technology - security techniques - information security management systems.*

Kochetkova, K., 2015. *Maritime industry is easy meat for cyber criminals* [online]. Available from: https://www.kaspersky.com/blog/maritime-cyber-security/8796/ [Accessed 25 March 2020].

Leyden, J., 2018. *Holy ship! UK shipping biz Clarksons blames megahack on single point of pwnage* [online]. Available from: https://www.theregister.co.uk/2018/08/01/clarksons_breach_update/ [Accessed 26 March 2020].

Lund, M.S*., et al.,* 2018. Integrity of integrated navigation systems*. Conference on communications and network security* (CNS), 30 May - 1 June 2018 Beijing.

Maersk, 2017. *Cyber attack update.*

Maritime and Port Authority of Singapore, 2019. *New 24/7 Maritime Cybersecurity Operations Centre to Boost Cyber Defence Readiness* [online]. Available from: https://www.mpa.gov.sg/web/portal/home/media-centre/news-releases/mpa-news-releases/detail/8a5114cf-8214-4b46-8999-2c6c42433b1e [Accessed 25 April 2020].

Maritime Executive, 2017. *Ferry builder Austal hit by cyberattack* [online]. Available from: https://www.maritime-executive.com/article/ferry-builder-austal-hit-by-cyberattack [Accessed 25 March 2020].

Mohindru, S.C., 2017. *Shipping: BW Group's computer systems hacked; steps up cyber security* [online]. Available from: https://www.spglobal.com/platts/en/market-insights/latest-news/shipping/101317-shipping-bw-groups-computer-systems-hacked-steps-up-cyber-security [Accessed 25 March 2020].

MUNIN, 2012. *About MUNIN* [online]. Available from: http://www.unmanned-ship.org/munin/ [Accessed 24 April 2020].

Ngai, S., 2017. *BW Group steps up cyber security after IT infringement – IHS Markit Safety at Sea* [online]. Available from: https://safetyatsea.net/news/2017/bw-group-steps-up-cyber-security-after-it-infringement/ [Accessed 25 March 2020].

Oruc, A., 2019. Tanker industry is more ready against cyber threats*. International conference on marine engineering and technology,* 5-7 November 2019 Muscat.

Ozkaya, S., 2018. *Doğu Akdeniz'de ısınan sular ve Kıbrıs denklemi* [online]. *Anadolu Agency.* Available from: https://www.aa.com.tr/tr/analiz-haber/dogu-akdeniz-de-isinan-sular-ve-kibris-denklemi/1278755 [Accessed 8 May 2020].

Sabah, 2016. *KORAL TSK'ya teslim edildi* [online]. Available from: https://www.sabah.com.tr/galeri/turkiye/koral-tskya-teslim-edildi [Accessed 22 July 2020].

Safety4Sea, 2019. *UK marine services company hit by cyber attack* [online]. Available from: https://safety4sea.com/uk-marine-services-company-hit-by-cyber-attack/ [Accessed 22 March 2020].

Safety4Sea, 2020. *Data breach at UK yachting recruitment agency exposes 17,000 personal data* [online]. Available from: https://safety4sea.com/data-breach-at-uk-yachting-recruitment-agency-exposes-17000-personal-data/ [Accessed 22 March 2020].

Saul, J., 2017. *Cyber threats prompt return of radio for ship navigation* [online]. Available from: https://www.reuters.com/article/us-shipping-gps-cyber/cyber-threats-prompt-return-of-radio-for-ship-navigation-idUSKBN1AN0HT [Accessed 23 March 2020].

Senzee, T., 2019. *What happened in ransomware attack on Port of San Diego* [online]. Available from: https://www.sandiegoreader.com/news/2019/apr/10/city-lights-happened-ransomware-port-san-diego/ [Accessed 13 April 2020].

Shauk, Z., 2013. *Malware on oil rig computers raises security fears* [online]. Available from: https://www.houstonchronicle.com/business/energy/article/Malware-on-oil-rig-computers-raises-security-fears-4301773.php [Accessed 25 March 2020].

Sophos, 2013. *The A-Z of computer and data security threats*.

The Local, 2014. *State-sponsored hackers spied on Denmark* [online]. Available from: https://www.thelocal.dk/20140922/denmark-was-hacked-by-state-sponsored-spies [Accessed 23 March 2020].

Torbati, Y., and Saul, J., 2012. *Iran's top cargo shipping line says sanctions damage mounting* [online]. Available from: https://www.reuters.com/article/us-iran-sanctions-shipping-idUSBRE89L10X20121022 [Accessed 26 March 2020].

Trend Micro, 2017. *Ransomware* [online]. Available from: https://www.trendmicro.com/vinfo/us/security/definition/ransomware [Accessed 25 April 2020].

Tung, L., 2018. *Maersk took just 10 days to replace 45,000 PCs wiped by NotPetya attack* [online]. Available from: https://www.csoonline.com/article/3514914/maersk-took-just-10-days-to-replace-45-000-pcs-wiped-by-notpetya-attack.html [Accessed 26 March 2020].

U.S. Department of Justice, 2018. *Two Iranian men indicted for deploying ransomware to extort hospitals, municipalities, and public institutions, causing over $30 million in losses* [online]. Available from: https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public [Accessed 13 April 2020].

University of Rijeka, 2019. Cyber Security of Maritime ICT-Based Systems. Available from: https://www.pfri.uniri.hr/web/en/projekti/aktivni/10-2019/2019-Svilicic-eng.pdf [Accessed 30 July 2020].

USCG NAVCEN, 2020. *GPS problem reports status* [online]. Available from: https://navcen.uscg.gov/?Do=GPSReportStatus [Accessed 4 April 2020].

Vistiaho, P., 2017. *Maritime cyber security incident data reporting for autonomous ships.* Thesis (M.Sc.). Tampere University of Technology.

WMN, 2018a. *COSCO Shipping Lines falls victim to cyber attack* [online]. Available from: https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/ [Accessed 25 March 2020].

WMN, 2018b. *Data theft affects hundreds of Svitzer Australia's employees* [online]. Available from: https://worldmaritimenews.com/archives/247526/data-theft-affects-hundreds-of-svitzer-australias-employees/ [Accessed 25 March 2020].

Yara International, 2018. *Yara Birkeland* [online]. Available from: https://www.yara.com/knowledge-grows/game-changer-for-the-environment/ [Accessed 24 April 2020].

Yilmaz, T., 2019. *Doğu Akdeniz'de GKRY için en akılcı seçenek iş birliği* [online]. *Anadolu Agency.* Available from: https://www.aa.com.tr/tr/turkiye/dogu-akdenizde-gkry-icin-en-akilci-secenek-is-birligi-/1488040 [Accessed 4 May 2020].