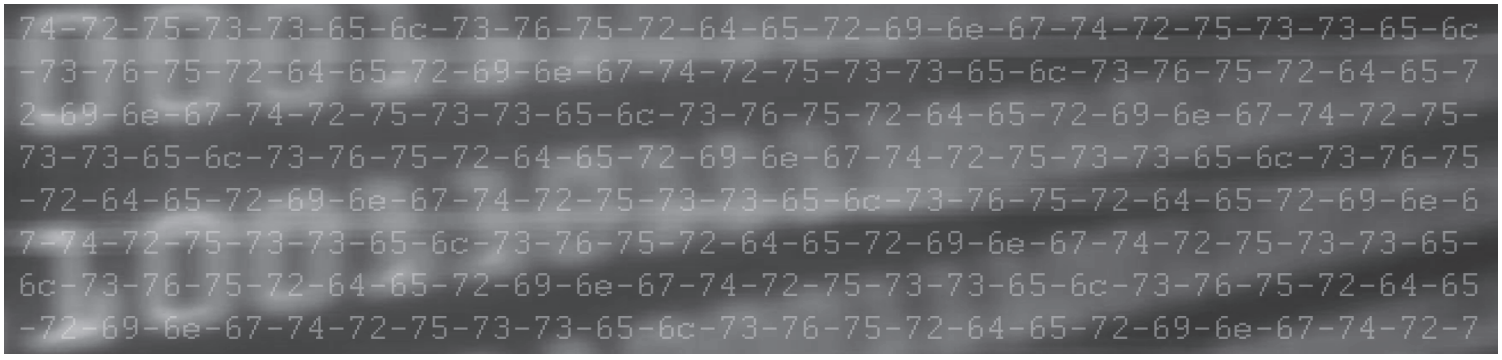
CENTRE FOR
CYBER SECURITY

Threat Assessment

The cyber threat against the Danish maritime sector



Threat Assessment Branch under the Centre for Cyber Security

January 2019

CENTRE FOR
CYBER SECURITY

Centre for Cyber Security
30 Kastellet
DK-2100 Copenhagen

Telephone: +45 3332 5580
Email: cfcs@cfcs.dk
www.cfcs.dk

1st version
09.01.2019

Threat assessment: The cyber threat against the Danish maritime sector

This threat assessment outlines the cyber threats facing the Danish maritime sector. The Danish maritime sector is of vital importance to the functioning, stability, and economy of the Danish society. The purpose of this assessment is to inform the maritime sector of threats in order to facilitate mitigation. This threat assessment could, for example, be included in the maritime sector's work related to the Danish cyber and information security strategy.

Key Assessment

- The threat from cyber espionage against the Danish maritime sector is **VERY HIGH**. The threat especially comes from foreign states that can have both financial as well as political interests in conducting cyber espionage against private companies and public authorities in the Danish maritime sector.
- The threat from cyber crime against the Danish maritime sector is **VERY HIGH.** Cyber criminals direct many different types of cyber attacks at private companies and public authorities in the maritime sector. In addition to the economic ramifications, cyber crime may, at worst, disrupt operations in the maritime sector.
- The threat from cyber activism is **LOW.** Cyber activists often pursue single-issue agendas, potentially causing the threat from cyber activism against the industry to increase suddenly, for instance, in the wake of global political discussions and incidents involving the maritime sector such as transport of controversial goods or major oil spills from ships.
- The threat from cyber terrorism is **LOW.** Even though militant extremists in a few instances have expressed an interest in conducting cyber terrorism, they currently lack the capabilities to do so.
- Foreign states are less likely to launch destructive cyber attacks against critical infrastructure in Denmark, including the maritime sector. However, the Danish maritime sector may become a collateral victim of destructive cyber attacks against targets outside of Denmark.

Introduction

This threat assessment provides an overview of the general cyber threat against the Danish maritime sector. Like most sectors in Denmark, the maritime sector is increasingly dependent on digital systems and units, potentially enabling cyber attacks to affect the operations and security of the sector. As the maritime sector is a part of the critical infrastructure in Denmark it is essential that public and private shipping companies are resilient against cyber attacks.

The maritime sector consists of several components of varying complexity and with different characteristics and vulnerabilities. This threat assessment analyses the cyber threat against the Danish maritime sector as a whole, making only limited distinctions between the different components of the sector. The cyber threat against ports will not be dealt with in this threat

assessment as Danish ports fall under the transport sector and are thus included in threat assessments pertaining to that sector. Shipping operations carried out by units under the Danish Armed Forces are also not included in this assessment.

Several shipping companies are present in different parts of the world, and the supply chain in the maritime sector can be long and complex. The transport of, for instance, a single container may involve an array of private companies and public authorities in several countries. Consequently, cyber attacks aimed at targets outside Denmark may affect operations in the Danish maritime sector or the integrity of the systems used by Danish shipping companies. Consequently, the cyber threats to the Danish and global maritime sector is therefore analysed in close coherence.

This threat assessment is based on the Danish Defence Intelligence Service's Centre for Cyber Security's (CFCS) general knowledge of cyber threats and cyber incidents targeting the maritime sector. Compared to other critical sectors, CFCS' insights into issues specific to the maritime sector are still relatively limited.

This assessment is based on the current threat landscape and operates with a warning time frame of 0-2 years. Cyber threats are dynamic and can therefore quickly change, both on a general level and in relation to individual authorities and private companies. This assessment uses the threat and probability levels of the Danish Defence Intelligence Service (DDIS), defined at the end of the report.

The exact number of cyber attacks against public authorities and private companies in the maritime sector is difficult to determine as not all cyber attacks are reported to the relevant authorities – either because the organization wants to avoid drawing attention to the cyber attack or the attack has not been detected. CFCS recommends companies to use the CFCS' voluntary notification scheme if they are subject to cyber attacks.

What are cyber threats?
The CFCS defines cyber threats as threats from cyber attacks in which an actor tries to disrupt or gain unauthorized access to data, systems, digital networks or digital services. Use of the Internet for other purposes that may have a negative impact on society such as online sale of illegal goods and services is not included in this definition of cyber threats.

Cyber threats are multi-faceted. In this assessment the focus is on the end goal of different cyber attacks such as cyber espionage, cyber crime, cyber activism or cyber terrorism. Also, we will assess the potential threat from destructive cyber attacks.

The threat levels in this assessment are based on an analysis of the actors' intention and cyber capabilities. An actor's capabilities can be understood as its available human and material resources, ranging from skilled hackers, malware developers, information on targets that is useful in social engineering campaigns to IT infrastructure, time and funds. Thus, the scope of an actor's cyber capabilities depends on available resources as well as the actor's ability to exploit them.

Cyber espionage

The threat from cyber espionage against the Danish maritime sector is **VERY HIGH**.

CFCS assesses that the threat especially comes from foreign states. Cyber espionage against private companies and public authorities in the maritime sector can affect the targeted organizations' finances and integrity as well as pose a potential national security threat to Denmark.

Cyber espionage against the maritime sector may be motivated by financial interests. Foreign states can have an interest in stealing information on new maritime technology or information on large procurements or contract negotiations. By stealing information on valuable shipping contracts, foreign states may provide their own national companies a competitive edge.

Certain foreign states also conduct cyber espionage against private companies simply because they corporate with the foreign state's national companies or public authorities. The foreign states do this in an attempt to monitor cooperation partners and companies that may potentially influence national organizations.

Cyber espionage against the maritime sector may also be motivated by security-related interests, for instance, foreign states may have a special interest in the opening of new shipping routes as well as shipping in disputed territorial waters.

As the maritime sector is part of the critical infrastructure in Denmark, foreign states may have an interest in collecting information on capabilities and vulnerabilities in the maritime sector that may be of relevance in connection with a potential military conflict. Information collection on critical infrastructure may be exploited in the event of a future conflict to facilitate destructive cyber attacks or physical attacks against the maritime sector.

Foreign states can also be interested in information on companies or authorities in the maritime sector that provide support to the Danish Armed Forces or foreign military forces, for instance, in relation to transport of troops or equipment. Foreign civilian shipping companies commissioned with US army transports have been exposed to cyber espionage.

Cyber crime

The threat from cyber crime against the maritime sector is **VERY HIGH**.

In this assessment, cyber crime covers the uses cyber attacks in relation to financially motivated criminal activities.

Cyber criminals are resourceful in their attempts to make financial gain and employ many different types of cyber attacks, some of which are becoming increasingly sophisticated and complex. Some of these cyber attacks aim to extort money from private companies and public authorities and often take the shape of ransomware attacks in which cyber criminals demand a ransom to restore the victim's access to data and systems. Ransomware is particularly harmful as it may, at worst, disrupt operations in the maritime sector.

Spear phishing against the maritime sector

In October 2018, spear phishing mails were sent to several companies in different countries. Companies in the shipping sector abroad were amongst the targets. The emails used different levels of social engineering techniques in order to appear legitimate. For instance, a company in the Italian naval industry received an email requesting prices for maritime spare parts that contained a malware-infested attachment. Cyber criminals may be responsible for the attack, which has been referred to as the MartyMcFly campaign.

For example, operations may be disrupted if on-board operational systems are infected with ransomware. Maritime vessels are no longer isolated from external systems. Even when shipboard networks are segmented, over time they may be accidentally compromised by manual data transfers carried out by crew, technicians or suppliers, for instance, in connection with

maintenance. Open sources reported an incident abroad in which ransomware had infected a ship's systems, resulting in the shutdown of the ship's switchboard. A switchboard has a key function in relation to the management of the power supply on a ship. An IT security company has also described an incident abroad where a crucial navigation system was infected with malware via an USB stick.

Also, operations may be disrupted if a maritime company's administrative systems are infected with ransomware. According to media reports, Chinese shipping company China Ocean Shipping (Group) Company – often referred to as COSCO – was victim of a possible ransomware attack in July 2018. The cyber attack disabled the company's electronic communication channels in several branches in North- and South America, temporarily hampered the company's operations.

Cyber criminals also extort their victims by other means, for instance by launching DDoS attacks or by threatening to leak stolen data. In November 2018, it was revealed that Australian shipbuilding company Austal had been hacked and that the hackers had attempted to extort the company as well as sell the stolen data via the Internet. Similarly, in 2017, British company Clarkson PLC was exposed to extortion attempts following a compromise of a company user account, granting the hackers access to sensitive data. Theft of personal and financial data may undermine client confidence in compromised companies.

Fraud such as so-called Business Email Compromise scams (BEC-scams) continues to pose a threat across sectors. The aim of BEC scams is to trick money from private companies and public authorities via fraudulent emails instructing the victim to transfer money to the perpetrator. The fraudulent emails are often sent from external email accounts, but criminals have also been known to exploit compromised email accounts belonging to in-house employees. For instance, criminals may hack an executive's or a client's email account to make the fraudulent emails appear credible and legitimate. Some cyber criminals have targeted shipping companies and their clients with BEC scams, possibly because shipping companies often operate in different time zones and thus are often reliant on email for conducting business transactions. BEC scams may result in financial losses for the targeted victim.

Cyber criminals have also been known to spread malware exploiting the victim's IT capabilities to generate cryptocurrency. Malware that generate cryptocurrency may affect IT networks, disrupt operations, prolong response times and, at worst, cause system breakdowns.

In addition, cyber attacks may facilitate other forms of crimes against the maritime sector. Cyber criminals may engage in smuggling, piracy or theft of goods in ports by hacking into company systems, stealing and manipulating freight and vessel information. In addition to causing financial losses to shipping companies, it may affect the safety of transport of goods and people at sea.

Cyber activism

The threat from cyber activism against the maritime sector is **LOW**.

Cyber activism is typically motivated by ideological or political beliefs, and cyber activists often target individuals or organizations they perceive as opponents to their cause. Some hacker groups and individuals involved in cyber activism have significant capabilities and resources to conduct cyber attacks. Although we do not counter many cases of cyber activism in Denmark, the threat may suddenly increase. Hackers can mobilize quickly in the wake of political discussions and incidents involving the maritime sector, such as transport of controversial goods or oil spills from ships.

Cyber activists also attack public authorities and private companies which they perceive as symbolic targets, even though the organizations have not been directly involved in the issue that caught the hackers' attention. The attacks may also be random as hackers often attack easy and vulnerable targets.

Cyber terrorism

The threat from cyber terrorism against the maritime sector is **LOW**.

Even though militant extremists in a few instances have expressed an interest in launching cyber terrorism, CFCS assesses that they currently lack the capabilities to do so.

Consequently, the threat from cyber attacks against the Danish maritime sector aimed at causing the same effect as conventional terrorism such as physical harm to individuals or equipment or extensive infrastructural disruptions in the maritime sector is low.

Destructive cyber attacks

A number of countries have access to destructive cyber capabilities that could potentially be used against critical infrastructure such as the maritime sector. CFCS defines a destructive cyber attack as an attack that could result in death, personal harm, considerable damage to physical objects or destruction or manipulation of information, data or software, making them useless unless large-scale recovery efforts are made.

CFCS assesses it is less likely that foreign states have the intent to launch destructive cyber attacks against critical infrastructure in Denmark, including the maritime sector. However, the threat can increase in the event of a deepening political or military conflict in which Denmark is involved.

At present, Danish public authorities and private companies may be affected by destructive cyber attacks against targets outside Denmark. This is particular relevant for Danish maritime companies operating in conflict areas where foreign states or organized hacker groups with destructive cyber

capabilities have vested interests to defend, for instance, in parts of Eastern Europe, the Middle East and Southeast Asia.

A.P. Moller-Maersk was one of several companies worldwide that was affected by the June 2017 NotPetya attack, which was likely a destructive cyber attack disguised as a ransomware attack. As a result, A.P. Moller-Maersk suffered substantial financial losses, and the attack also hampered Maersk's ability to handle cargo in ports, demonstrating how a cyber attack against the maritime sector may potentially affect other sectors.

Definition of threat levels

The DDIS uses the following threat levels, ranging from **NONE** to **VERY HIGH**.

NONE	No indications of a threat. No acknowledged capacity or intent to carry out attacks. Attacks/harmful activities are unlikely.
LOW	A potential threat exists. Limited capacity and/or intent to carry out attacks. Attacks/harmful activities are not likely.
MEDIUM	A general threat exists. Capacity and/or intent to attack and possible planning. Attacks/harmful activities are possible.
HIGH	An acknowledged threat exists. Capacity and intent to carry out attacks and planning. Attacks/harmful activities are likely.
VERY HIGH	A specific threat exists. Capacity, intent to attack, planning and possible execution. Attacks/harmful activities are very likely.

Below is the scale of probability the DDIS applies