CENTRE FOR
CYBER SECURITY

Threat Assessment:

The cyber threat against marine aids to navigation

1st edition November 2022.

Table of Contents

CENTRE FOR
CYBER SECURITY

Kastellet 30
2100 København Ø
Phone: + 45 3332 5580
Email: cfcs@cfcs.dk

1st edition November 2022.

The cyber threat against marine aids to navigation

The purpose of this threat assessment is to inform Danish authorities and operators of marine aids to navigation of the cyber threat against marine aids to navigation. The assessment is to supplement the CFCS threat assessments: The cyber threat against the maritime industry and ports and The cyber threat against operational systems on ships.

Key assessment

- The threat from cyber attacks against marine aids to navigation is **HIGH**.
  For the purpose of this threat assessment, the term marine aids to navigation includes both special equipment and the authorities' underlying IT infrastructure.

- Criminal hackers attack private companies and public authorities across society. They can also attack organizations and IT systems that deliver marine aids to navigation.

- Foreign states may also pose a threat to the systems. Foreign states may for instance have an interest in information on sailing patterns of military vessels and shipment of military equipment and supplies.

- In a conflict situation, foreign states may have an interest in manipulating or destroying the systems to disrupt navigation in Danish waters.

- Suppliers of equipment used as marine aids to navigation may be used as stepping stones for attacks against these systems.

Introduction

Some 70,000 ships navigate the Danish straits every year, many of which are tankers going to and from the Baltic Sea, making Danish waters some of the busiest in the world.

A number of services, collectively known as marine aids to navigation, are designed to help navigators and ships maintain high navigation safety through the waters in consideration of safety and the environment.

Marine aids to navigation

"The International Association of Marine Aids to Navigation and Lighthouse Authorities" (IALA) is the international organisation covering aid to navigation. IALA describes "marine aid to navigation" (ATON) as "a device, system or service, external to a vessel, designed and operated to enhance safe and efficient navigation of individual vessels and/or vessel traffic".

The term covers both analogue aids such as lighthouses and marks (buoys), and more technical and digitized services such as navigation warnings and Vessel Traffic Service (VTS). The term may be broadened to include maritime surveillance, pilot service, positioning services, chart updates, meteorological services, notice to mariners, communication channels, etc.

Authorities use different operational equipment and special IT systems to generate and deliver these services. However, in order to maintain delivery of these services, authorities are also highly dependent on common administrative IT systems.

This threat assessment covers marine aids to navigation in the broad sense of the term, the special equipment used and the authorities' underlying IT infrastructure.

Marine aids to navigation provide key input for safe navigation in and through Danish waters but are also significant for the rest of Denmark's infrastructure.

At the Great Belt Bridge, the Øresund Bridge and at the Femern connection there are Vessel Traffic Service (VTS) centres that provide monitoring and navigational advice for vessels, ensuring the safety of vessels and bridge.

Cyber attacks against the organizations and systems that provide marine aids to navigation may potentially cause operational disruptions and theft of data. At worst, cyber attacks against the systems may affect maritime traffic and safety in Danish waters.

Additional information on maritime cyber threats
For information on the cyber threat against operational systems on ships see the CFCS Threat Assessment: The cyber threat against operational systems on ships. Information on the general threat against the maritime industry can be found in the CFCS Threat Assessment: The cyber threat against the maritime industry and ports. Both threat assessments are available on the CFCS website.

The cyber threat from criminals and foreign states

The CFCS assesses that the threat from cyber attacks against marine aids to navigation in Denmark is **HIGH**, making it likely that the special equipment used to produce these systems and the authorities' underlying IT infrastructure will be subject to cyber attack attempts within the next two years.

The threat mainly emanates from financially motivated criminal hackers and hackers spying for foreign states.

Criminal hackers may cause disruptions
The CFCS assesses that criminal hackers generally do not specifically target the organizations that manufacture and deliver marine aids to navigation. They do, however, attack private companies and public authorities across society. Criminal hackers can therefore also attack organizations and IT systems that deliver marine aids to navigation.

Cyber criminals use different attack techniques to make a profit, including ransomware attacks and theft of financial information. Common to all cyber attacks is that they may, intentionally or inadvertently, cause system disruptions.

Targeted ransomware attacks are one method in which the attack typically causes as much inconvenience as possible to the victims. In this type of attack, hackers invest significant time and effort encrypting vital parts of compromised victim networks. Once the systems have been encrypted, the hackers often demand millions in ransom to decrypt the systems. Over the past few years, targeted ransomware attacks have been on the rise in Denmark, making them a frequent occurrence.

The threat from cyber attacks is primarily directed at administrative IT systems. As mentioned in the introduction, Danish authorities rely on administrative IT systems in maintaining services such as navigation warnings.

The very high cyber threat against such systems in Denmark also poses a threat to the administrative systems that are used for such tasks. However, the actual attack surface is limited as only a small group of government units provide marine aids to navigation, lowering the likelihood of them being exposed to more or less random attacks.

Attacks against administrative IT systems may spread and at worst upset the operation of administrative as well as operational systems. A case in point is the ransomware attack against a US port facility described below.

Systems in US port facility disabled by ransomware

In December 2019, the US coast guard informed that a port facility had been encrypted by the Ryuk ransomware. The hackers attacked the port through a phishing email sent to a port employee who clicked on the embedded malicious link.

Besides encrypting the administrative IT systems, the attack also impacted critical industrial control systems and caused disruption of security cameras, physical access control systems, and critical process control monitoring systems.

The port facility was forced to shut down for more than 30 hours until its critical systems had been restored.

So-called DDoS attacks are another attack technique used by cyber criminals. This type of attack is aimed at overloading victim systems with traffic, rendering them inaccessible. Some cyber criminals carry out DDoS attacks and follow up with a ransom demand to stop the attacks. This extortion method is called RDDoS or RDoS.

Other methods used by cyber criminals are not intended to disrupt victim systems. For instance, when hackers compromise IT systems and digital units in order to exploit their capacity. Cyber criminals may exploit the computing power of devices to distribute spam, generate cryptocurrency or launch attacks on other victims. However, these attacks sometimes inadvertently disrupt the victim’s IT systems, for example in connection with technical errors by the hacker or system overloads.

Foreign states may also pose a threat against the systems

Cyber espionage poses a persistent threat against civilian and military authorities in Denmark, including the authorities that deliver marine aids to navigation such as the Danish Defence and the Danish Maritime Authority.

Foreign states motives for spying against Danish authorities, include gaining access to information that is relevant in a security policy context. It is possible that foreign states have an interest in the units and systems that provide navigation support. For instance, VTS handles information on dangerous goods and military maritime traffic, which some foreign states might find interesting.

Information on civilian maritime traffic is typically publicly available via AIS services and thus less interesting in a cyber espionage context.

Aids to navigation could be targeted by destructive cyber attacks during a conflict
Foreign states may also have an interest in gaining access to and information on marine aids to navigation in preparation of future destructive cyber attacks.

Destructive cyber attacks are attacks that are expected to result in death, personal injury, significant physical damage, or destruction or manipulation of information, data or software, rendering them unfit for use unless extensive restoration is undertaken.

At present, the threat from destructive cyber attacks against Denmark is low. However, the threat may increase in case the security situation escalates towards a military confrontation.

In preparation for a potential future conflict, foreign states may have an interest in exploring the possibility of gaining access to and information on marine aids to navigation.

In a conflict situation foreign states could for instance have an interest in manipulating or destroying marine aids to navigation to disrupt navigation in Danish waters as well as access to the Baltic Sea through the Danish straits.

Suppliers as stepping stones for cyber attacks

Cyber criminals and state-sponsored hackers alike use compromised companies as stepping stones for attacks against the companies customers. The cyber threat against marine aids to navigation and the cyber threat against the suppliers of these systems are thus interrelated.

Special equipment for marine aids to navigation is often supplied by international defence equipment suppliers. It is possible that the persistent cyber threat against the defence industry globally and in Denmark may impact on the cyber threat against marine aids to navigation, as suppliers may be used as stepping stones for cyber attacks against the operators of marine aids to navigation.

Attacks may take place by sending infected software updates from a supplier that are subsequently downloaded by customers. This method was for instance used in the 2020 SolarWinds attacks.

Some suppliers also have remote access directly to customer equipment. If hackers manage to compromise a supplier and secure remote access, they may exploit this access to attack the supplier’s customers to steal data, launch destructive cyber attacks or install ransomware.

Perspective: Digitalization enhances the importance of cyber security

Like the rest of society, the maritime industry is becoming increasingly digitalized, making functions on ships more automatic or autonomous. Ships are becoming more reliant on technology, and the aid provided by maritime authorities to support more digitalized ships are also under development, a concept known as e-Navigation.

In 2020-2021, the Danish Maritime Authority tested the use of virtual buoys in selected areas in Danish waters. Similarly, in Denmark and other places of the world there are areas for remote-controlled and even autonomous ship testing.

The increased reliance on maritime technology may render ships more vulnerable if the navigation does not work, or if the data is manipulated. This reliance can make aid to navigation an attractive target for both cyber criminals and state-affiliated hackers.

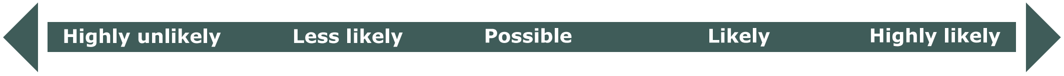
Threat levels

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.

The DDIS applies the below scale of probability



”We assess” corresponds to ”likely” unless a different probability level is indicated.