CENTRE FOR CYBER SECURITY

Threat Assessment:

The cyber threat against Danish ports and logistics companies

First edition, April 2023

Table of Contents

CENTRE FOR CYBER SECURITY

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

1st edition, April 2023

The cyber threat against Danish ports and logistics companies

The purpose of this threat assessment is to describe the cyber threats against Danish commercial ports and logistics companies. This threat assessment can form part of the efforts by Danish port authorities and logistics companies in preparing cyber security risk assessments. The intended audiences of this threat assessment mainly include top management and IT employees in Danish ports and logistics companies.

Key assessment

- The threat of cyber espionage against Danish ports and logistics companies is **VERY HIGH**, regularly resulting in cyber attacks on Danish targets, including ports and logistics companies.

- The threat of cyber crime against Danish ports and logistics companies is **VERY HIGH**. Ransomware attacks are the most serious cyber crime threat, however, ports and logistics companies also fall victim to a high number of spear phishing and BEC scam attempts.

- The threat of cyber activism against Danish ports and logistics companies is **HIGH**. The threat mainly emanates from pro-Russian hackers, who have stepped up their level of activity following Russia's invasion of Ukraine, and regularly attack targets in the West, including in Denmark. Cyber activists, in particular, will likely focus on attacking targets in Denmark, including Danish ports and logistics companies.

- The threat of destructive cyber attacks against Danish ports and logistics companies is **LOW**. It is less likely that foreign states currently harbour intentions to launch destructive cyber attacks against ports and logistics companies in Denmark. However, CFCS assesses that hacker groups affiliated with foreign states are preparing the ability to carry out destructives cyber attacks against Danish targets at short notice.

- The threat of cyber terrorism against Danish ports and logistics companies is **NONE**.

Introduction

This threat assessment outlines the cyber threat against ports and logistics companies in Denmark. The threat assessment covers all commercial ports in Denmark regardless of ownership. Marinas and yacht harbours are not covered in this assessment. Logistics companies are companies whose core business is transport of goods and cargo for clients. Although the major part of freight transport in Denmark is by road or rail, some logistics companies transport goods by air. However, this assessment does not deal with the threat against concrete means of transportation i.e. airplanes, trains and truck. It only covers the threat against logistics companies and their systems. The maritime sector will not be dealt with in this threat assessment, as the Danish maritime sector is considered as a separate sector by the Danish authorities.

This assessment is based on the current threat landscape and operates with a warning horizon of up to two years. As cyber threats are dynamic, the threat landscape can quickly change. This assessment uses the DDIS threat level and probability level definitions, which are listed at the end of the assessment.

The assessment is based on analyses of Danish and international examples of cyber attack incidents against ports and logistics companies and on knowledge about the capability and intent of threat actors. The threat assessment has also been prepared on the basis of conversations with multiple port authorities and logistics companies in Denmark.

The greatest threats to ports and logistics companies in Denmark are cyber espionage and cyber crime. Cyber espionage, in particular, poses a serious threat as ports and logistics companies have access to critical information, not just vital to the functioning of society but also to the Danish military. As a result, foreign states may thus obtain unauthorized access to information of importance to the security of Denmark.

In addition, cyber crime poses a serious threat to ports and logistics companies in Denmark. Ransomware constitutes the most serious threat as ransomware attacks are among the most common types of cyber attack used against critical societal sectors. Also, a ransomware attack may have serious economic repercussions for Danish ports and logistics companies, and could in a worst-case scenario disrupt the delivery of critical services.

Ports and logistics companies are vital to the Danish supply chains
The COVID-19 pandemic illustrated that food shortage and lack of vital supplies such as medicine and technology are a real concern for the Danish population. At the outbreak of the pandemic, news outlets showed images from Danish supermarkets of Danes stocking up on food and supplies such as toilet paper, hand sanitizer and yeast, and several supermarkets quickly announced that ordinary household items were sold out. Also, the wait time for delivery of new cars and electronics was extensively

delayed, and it became apparent that supply chain resilience was vital to the functioning of the Danish society.

Also, Denmark is the sixth largest shipping nation in the world measured by operated tonnage. Some 780 merchant vessels operate under Danish flag, and close to 2,000 vessels are operated from Denmark. With more than 100,000 annual ship calls, the commercial ports in Denmark ensure supplies to the whole country. 70 per cent of Danish imports are transported via ports. Consequently, it is vital that ports and logistics companies in Denmark are resilient against cyber attacks, which may, at worst, result in supply chain disruptions.

Finally, the war in Ukraine has demonstrated that a stable supply chain may become vital during a crisis, and that ports and logistics companies play a key role in ensuring the necessary supply of goods and equipment to the Danish armed forces.

Technology development may become vital to the sector

Many ports and logistics companies in Denmark were established at a time when digital solutions and IT operated systems were not an integral part of daily operations, and as a result, the implementation of technological development in companies has taken place gradually and within recent years. Consequently, several ports are still equipped to switch to manual operations in case of IT outages or hacker attacks.

Cyber attack surfaces are expanding as technological developments make ports and logistics companies increasingly dependent on digital solutions. Work processes and systems that were previously person-dependent and analogue are increasingly connected to or controlled by IT systems, which hackers may, at worst, exploit to launch attacks. Should such a scenario occur, it could potentially cause significant financial losses, reputational damage to the companies or disruption of infrastructure vital to the functioning of society.

Cyber espionage

The threat of cyber espionage against ports and logistics companies in Denmark is **VERY HIGH**, meaning that ports and logistics companies in Denmark are highly likely to become targets of cyber espionage attempts in the next two years. Cyber espionage poses a persistent threat and continuously results in cyber attacks against Danish targets, including ports and logistics companies.

The DDIS Centre for Cyber Security (CFCS) assesses that ports and logistics companies in Denmark and abroad have seen an increase in cyber espionage activity in recent years.

Ports and logistics companies are crucial in a military conflict
The serious threat of cyber espionage is rooted in the interest of foreign states, including in particular Russia and China, in gaining access to information on foreign, security and defence policy. The espionage threat against ports and logistics companies could thus be motivated by security policy interests, for example, information relating to NATO or Arctic issues.

In connection with military conflicts, the role that civil companies in the sector plays in maintaining supply chain security and supporting the Danish armed forces could change. Ports and logistics companies may become vital, not only to society but also to the Danish military. Foreign states may also show an interest in the parts of the Danish ports and logistics companies that are tasked with supporting Danish military and foreign states' military, providing transport of military personnel for missions abroad or allowing military use of civil traffic hubs.

Information collection on ports and logistics companies that are part of Danish critical infrastructure could also be used in preparation of destructive cyber attacks or physical attacks against the sector.

Ports and companies may suddenly become attractive espionage targets
Even though ports and logistics companies in Denmark have not yet fallen victim to cyber espionage attacks or do not consider themselves attractive cyber espionage targets, the situation may quickly change if a company enters into a major defence contract with a foreign country, holds a key physical location in connection with a military training exercise or becomes a key hub for new research and innovation.

For example, the United States has shown an interest in using the port of Esbjerg for deployment of allied forces to the Baltic Sea region and the Baltic states. Also, according to plan, Europe's largest Power-to-X production facility will be located in the Danish city of Esbjerg. The facility is designed to convert power from offshore wind turbines to CO2-free green ammonia to be used as fertilizer in the agricultural sector and as fuel in the shipping industry.

CFCS assesses that Russia's invasion of Ukraine has not warranted a change in the threat of cyber espionage against ports and logistics companies in Denmark. The majority of Danish ports and logistics companies report that they have not noticed an increase in the number of recorded cyber attacks. It is highly likely that Russia will remain just as intent on conducting cyber espionage against public authorities and private organizations in Denmark, including ports and logistics companies as it was before the invasion of Ukraine. Finally, Russia's cyber espionage attempts may intensify should the conflict between NATO and Russia worsens.

Ports and logistics companies may become entry points for attacks on other companies

Cyber espionage may also be directed at ports and logistics companies that may be used as initial entry points to compromise the intended targets.

Ports and logistics companies may become attractive targets for hackers as they often interface with other organizations and have clients across many sectors. By compromising a single port or logistics company, a malicious actor may be able to gain access to the networks and data of multiple clients, ultimately gaining unauthorized access to the end target. Thus, foreign states are potentially able to use compromised logistics companies or ports as stepping stones to gain unlawful access to companies working with, for instance, new technology, medical research or other expensive research area.

In some instances, ports and logistics companies have access to information on cargo deliveries, passengers and travel patterns, which foreign intelligence services may use to monitor certain individuals.

One setup with many attack surfaces

As technology is constantly evolving, cyber security extends beyond IT. As the modern world is becoming increasingly digitalized, the digital domain is not only storing our personal data. Large parts of production and operations in modern societies are also connected to the Internet. In addition to the central IT systems that manage HR, economy and logistics planning, ports and logistics companies have a large OT system connected to physical operations such as surveillance cameras, access control systems, gates, cranes, communications and error detection systems that are often connected to Internet-facing surfaces. As a result, Danish ports and logistics companies have many potential cyber attack surfaces.

It has been strongly debated whether foreign surveillance cameras could be used for cyber espionage. Several media outlets have focused on Chinese tech company Hikvision, which is known for delivering cameras and technology, which, among other things, are used by China to monitor its citizens. Against this backdrop, the United States passed a bill in 2019 prohibiting federal agencies from using Hikvision technology.

Most surveillance systems have vulnerabilities that could potentially allow unauthorized access to the security equipment. Regardless of manufacturer, surveillance equipment may thus constitute a security threat.

IT, OT and IoT – a gateway to vulnerabilities
Below are the CFCS' overall definitions of IT, OT and IoT:

IT (Information Technology): IT systems include hardware and software and may operate independently or interconnected with other systems in a network.

OT (Operational Technology): Systems used for surveillance and control of mechanical devices, including industrial control systems (ICS).

IoT (Internet of Things): A term covering devices, including anything from thermostats to everyday objects such as refrigerators or cameras connected to the Internet. When internet-connected OT systems use IP networks, it is known as the Industrial Internet of Things (IIoT).

Cyber crime

The threat of cyber crime against ports and logistics companies in Denmark is **VERY HIGH**, indicating that ports and logistics companies in Denmark are highly likely to fall victim to cyber crime attacks within the next two years.

In this assessment, the term cyber crime is used collectively to describe actions in which criminal hackers use cyber attacks to commit crimes for financial gain. Ransomware attacks and BEC scams, in particular, pose a serious threat to ports and logistics companies as ransomware attacks and BEC scams remain a widely popular form of cyber attack against critical societal sectors. CFCS knows of a number of ransomware attacks and attempts of BEC scams perpetrated against Danish ports and logistics companies in recent years.

Russia's invasion of Ukraine has sparked several reactions internally in the cyber criminal community. In October 2022, a number of ransomware attacks targeted ports and logistics companies in Ukraine and Poland. However, CFCS assesses that the invasion of Ukraine has not had a significant impact on the cyber crime threat against Denmark, including Danish ports and logistics companies. The general feedback from ports and logistics companies in Denmark also indicate that the sector has not recorded any real increase in the number of cyber attack attempts.

Innocent phishing may lead to serious ransomware attacks

Ports and logistics companies are generally very dependent on email correspondence. A large share of the companies' orders and invoicing of clients and external business partners is conducted via email, and phishing and spear phishing attacks are a regular occurrence among the companies. For instance, a company reports that it sends more than 1.5 million emails weekly, exposing the company to the risk of phishing and spear phishing scams. The risk of an employer being tricked by a phishing email depends on how professional the email is designed and the employer's training and skills in recognizing phishing attempts.

Phishing and spear phishing may be used in the initial compromise in connection with a ransomware attack, and once the cyber criminals gain unauthorized access to some of the central systems, it could have major repercussions for the affected companies. The operating systems used by logistics companies, in particular, to manage all their logistics and traffic planning are in many instances vital to the company's day-to-day operations. CFCS knows of several ransomware attacks targeting logistics companies, including Danish ones. Cyber criminals likely rely on the assumption that companies hit by a ransomware attack are willing to pay ransom because of the criticality of the systems to their business operations.

There have been several ransomware attacks abroad and in Denmark, for instance, against ports and logistics companies, where cyber criminals have gained access via phishing. A case in point is the 2020 ransomware attack on Port of Kennewick, USA, where cyber criminals encrypted the port's servers. According to open sources,

malware injected via phishing enabled the criminals to breach the port systems, and it took more than a week before the systems were regained.

Many emails means a higher number of phishing, spear phishing and BEC scam attempts

Spear phishing resembles ordinary phishing attempts, but differs in the sense that the victims are not picked at random but rather handpicked. Often, hackers use social engineering to customize an attack to a specific victim. Emails are usually tailored to appear particularly relevant, legitimate and credible to the victim. This is done by including elements such as the victim's name, personal details or other information gathered during reconnaissance prior to the attack. Often, spear phishing is a precursor to different types of attacks such as BEC-scams. CFCS knows of several ports and logistics companies that are exposed to targeted spear phishing attempts on a regular basis. For example, Copenhagen-Malmö Port has experienced several targeted spear phishing attempts in which the attackers used employee names and personal information.

Fraud in the form of Business Email Compromise scams (BEC scams) remains a threat across sectors. BEC scams use fraudulent emails to trick private companies and public authorities into wiring funds. The criminals typically impersonate in-house executives in an attempt to exploit employee loyalty – a scam that is also often referred to as CEO fraud. BEC scams may result in significant financial losses for the affected private company or public authority.

CFCS is aware of several attempted BEC scams against ports and logistics companies in Denmark. For instance, a senior employer with Blue Water Shipping in Australia received a payment request from a colleague in Denmark via WhatsApp. The Australian employee reacted swiftly though, and the attack was prevented. In addition, Kalundborg Port reports that it was targeted in a sophisticated CEO fraud attempt which involved the name of the affected employee and vital information on the employee's work calendar. This attack was also prevented.

Criminals exploit the good name of logistics companies

Several logistics companies report that their names have been exploited in connection with a non-cyber related financial scam against private individuals.

The scam involved criminals contacting their victims in connection with sale and purchase of luxury items, like motorcycles, etc. Subsequently, the criminals directed their victims to a false website which looked identical to the company's legitimate website, tricking the victims into entering their payment information which the criminals then harvested to exploit the victims' data.

Logistics companies report that they continuously keep an eye on newly established domains that overlap with their company domains. They also report that the issue of overlapping domains is a major concern as it could ultimately inflict reputational damage. Even though this type of scams cannot be categorized as cyber attacks, they indicate that criminal hackers focus on ports and logistics companies in general.

Cyber activism

The threat of cyber activism against ports and logistics companies in Denmark is **HIGH**, meaning that ports and logistics companies in Denmark are likely to be hit by cyber activism within the next two years.

On 31 January 2023, CFCS raised the threat level of cyber activism from **MEDIUM** to **HIGH**. The threat level was raised in response to the high activity level of pro-Russian hacktivist groups against NATO countries, including Denmark, and also in response to their formalized attack modus and improved capability.

The threat level of cyber activism is **HIGH** because of concrete activities conducted by pro-Russian cyber activists in connection with the war in Ukraine, this means that the threat level may change again with little or no warning depending on the development of the war.

Cyber activists call for attacks against ports and logistics companies
Cyber activism is typically ideologically or politically motivated, and cyber activists often focus on individuals or organizations that are perceived as opponents to their cause or as symbolic targets.

The war in Ukraine has resulted in the emergence of activist communities which, on social media like the Russian-developed application Telegram, call for and coordinate cyber activist attacks against individuals and organizations that they perceive as opponents to their cause. For example, pro-Russian groups have identified Ukrainian and Western companies that they believe will be particularly relevant targets. In this connection, they have repeatedly called for attacks against ports and logistics companies. A case in point is the October 2022 incident, where a pro-Russian activist group called on other hackers to launch DDoS attacks against marine terminals and logistics companies in the United States.

CFCS knows of no examples of pro-Russian cyber hacktivists calling on other hackers to attack specific ports or logistics companies in Denmark. However, given the fact that activist groups call for attacks on ports and logistics companies in other NATO countries, ports and logistics companies in Denmark are likely also at risk of becoming targets of cyber activist attacks.

Client-facing surfaces may be relevant DDoS targets
Cyber hacktivists often use DDoS attacks. DDoS attacks refer to cyber attacks in which the attacker exploits compromised computers to flood the targeted website or network with massive amounts of data traffic, rendering the website or network unavailable for legitimate traffic for as long as the attack is in progress. DDoS attacks may have serious consequences if directed at client-facing surfaces, at worst costing the ports and logistic companies potential clients and preventing their customers from placing orders via the compromised website.

Also, this form of attack may inflict reputational damage to ports and logistics companies due to the unavailability of the affected systems, ultimately affecting the revenue of the targeted company.

Destructive cyber attacks

The threat of destructive cyber attacks against ports and logistics companies in Denmark is **LOW**, making it less likely that ports and logistics companies in Denmark will fall victim to attempted destructive cyber attacks within the next two years.

Even though CFCS assesses that it is less likely that foreign states currently have the intention to carry our destructive cyber attacks against Denmark, it is likely that state-sponsored hacker groups are preparing to launch destructive cyber attacks against critical infrastructure in Denmark. The threat to Denmark could increase with little or no warning if, for instance, the political situation were to escalate in the direction of a military confrontation between Russia and NATO.

A number of countries have cyber capabilities to carry out destructive cyber attacks that can be used against critical infrastructure such as ports and logistics companies. CFCS defines destructive cyber attacks as attacks where the expected result is death, personal injury, significant physical damage or destruction or manipulation of information, data or software, rendering it unfit for use unless extensive restoration is undertaken.

Destructive attacks are used in conflicts

Since the onset of Russia's invasion of Ukraine in February 2022, Russian cyber attacks against Denmark have become a major issue of concern in the public debate. The September 2022 pipeline sabotage against Nord Stream 1 and 2 in the Baltic Sea has raised concern that critical Danish infrastructure may become part of the conflict.

In 2022, Ukraine was hit by different types of destructive cyber attacks. According to several IT security companies, Russia launched a host of so-called wiper attacks against Ukrainian public authorities and private companies, causing permanent data destruction. In October 2022, several logistics companies in Poland and Ukraine were hit by a ransomware-like attack, which, according to Microsoft, was carried out by Russian state-sponsored hacker group Sandworm, which has previously carried out destructive cyber attacks in and outside of Ukraine. The malware known as Prestige targeted several different logistics companies across the two countries within the span of a few hours. The attacks indicate that hacker groups focus on European logistics companies responsible for transport of humanitarian and military aid to Ukraine.

It is less likely that foreign states, including Russia, have intention of carrying out destructive cyber attacks against Denmark and Danish ports and logistics companies. However, Danish public authorities and private companies may become collateral victims of destructive cyber attacks directed at targets outside of Denmark, especially Danish logistics companies operating in conflict areas such as Ukraine or the Middle East where foreign states with capabilities to launch destructive cyber attacks have interests at stake. A case in point is the 2020 hacker attack against the Iranian port of Sharid Rajai, which led to the disruption of IT systems controlling all the logistics of trucks, goods and containers.

Destructive cyber attacks can spread

CFCS assesses that in connection with conflicts, there is an increased risk of destructive cyber attacks spreading to affect victims outside the actual conflict zone. It is possible that Danish private companies and public authorities operating in Ukraine or the Middle East in particular will fall victim to destructive cyber attacks or to the results of such attacks in the form of power outages and the lack of Internet access. The majority of the destructive cyber attacks that hit Ukraine in 2022 were limited in scope and did not spread beyond the Ukrainian border. This was, however, not the case with the cyber attack against the American satellite communication provider Viasat.

On the same day Russia invaded Ukraine, Viasat was hit by a wiper malware dubbed AcidRain disabling thousands of satellite modems in Europe in particular. Alongside the EU and a number of allies, Denmark has publicly stated that Russia was behind the attack and that Russia was aware that the consequences would extend beyond Ukraine. The attack was likely meant to cripple the communication of Ukrainian military. The attack against Viasat demonstrates that destructive cyber attacks may have consequences far beyond the direct victim.

Several ports and logistics companies have fallen victim to destructive cyber attacks that were directed at other victims. In June 2017, several transport companies were hit by the NotPetya attack – a destructive cyber attack disguised as a ransomware attack. As a result, logistics companies FedEx and Deutsche Post DHL Group and DAMCO suffered major financial losses.

In Denmark, the NotPetya attack against Aarhus Port also caused some challenges. However, the port authorities managed to avoid long lorry tail-backs as they were able to quickly inform the truck operators not to show up at the port for the planned transports.

Foreign states continue to develop destructive cyber attack capabilities

CFCS assesses that foreign states continue to develop the capabilities to launch destructive cyber attacks with little warning. The states use tools like cyber espionage to prepare the ability to carry out destructive cyber attacks, that could be launched in in the event of an escalating crisis or war.

Cyber espionage can give access to critical infrastructure, which states may try to destroy or disrupt in the event of serious crisis or war.

The preparation of destructive cyber attacks will often involve mapping of organizations, systems and network units. Through data collection on organizations and systems, hackers are able to customize malware. Also, hackers are capable of installing so-called backdoors into compromised systems, that could be used in subsequent destructive attacks.

Cyber terrorism

The threat of cyber terrorism against ports and logistics companies in Denmark is **NONE**, indicating that Danish ports and logistics companies are unlikely to fall victim to cyber terrorism attempts in the next two years.

CFCS defines cyber terrorism as a cyber attack aimed at creating effects similar to those of conventional terrorism, including cyber attacks causing bodily harm or major disruption of critical infrastructure.

CFCS assesses that militant extremists have limited intention to launch cyber attacks aimed at creating effects similar to those of conventional terrorism, and that they lack the necessary capabilities for doing so.

Conventional terrorism is more effective than cyber terrorism
Despite the serious threat from conventional terrorism and the fact that militant extremists have used the Internet for years to support their activities, plan conventional terrorist attacks and launch simple cyber activist attacks such as DDoS attacks and website defacement, there has, as of yet, not been any incident in which terrorists have launched cyber attacks creating the same effects as conventional terrorist attacks.

Danish ports focus more on the threat from conventional terrorism than they do on the threat from cyber terrorism, and most port authorities refer to the ISPS Code (the international Maritime Organization's port facility security code) as a central part of their security measures.

Threat levels

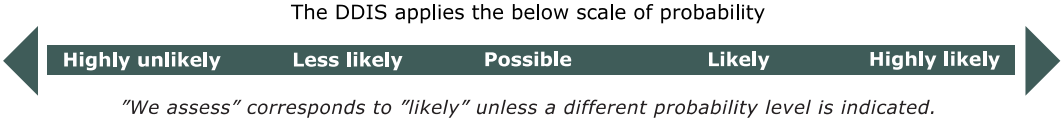
Definition of threat levels

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

NONE	There are no signs of a threat. There are no actors with both the capacity and intention for attacks/harmful activities.
LOW	There are one or more actors with the capacity and intention for attacks/harmful activity. However, either the capacity or the intention or both are limited.
MEDIUM	There are one or more actors with the capacity and intention for attacks/harmful activity. However, there are no indications of specific planning of attacks/harmful activity.
HIGH	There are one of more actors that have the capacity for and are specifically planning attacks/harmful activity or that have already carried out or attempted attacks/harmful activity.
VERY HIGH	There is either information that one or more actors are initiating attacks/harmful activity, including information about time and target, or that one or more actors are continuously initiating attacks /harmful activity.

An applied threat level reflects the DDIS's assessment of the intention, capacity and activity of one or more actors based on the available information.

The DDIS applies the below scale of probability



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