CENTER FOR
CYBERSIKKERHED

Threat assessment: Cyber threat against the defence industry

The purpose of this assessment is to inform decision-makers in the defence industry in Denmark of the cyber threat. The assessment has been prepared in collaboration with the Danish Defence and Security Industries Association (FAD).

Date: August 2020

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Tlf.: 33 32 55 80
E-mail: cfcs@cfcs.dk
www.cfcs.dk

Key assessment

- The threat from cyber espionage is **VERY HIGH**. Several countries have conducted cyber espionage against the defence industry worldwide. Due to the overlap of technologies, the threat from cyber espionage overlaps with the threat against associated sectors, in particular within the maritime and aerospace industries.

- The threat from cyber crime is **VERY HIGH**. CFCS assesses that the overall threat posed by cyber criminal actors to Danish private companies and public authorities also applies to the defence industry. However, cyber criminals do not have a particular focus on the industry.

- The threat from destructive cyber attacks is **LOW**. It is less likely that foreign states will launch destructive cyber attacks against Denmark. Private companies and public authorities operating in conflict-ridden regions are at a greater risk from this threat.

- The threat from cyber activism is **LOW**. Globally, the number of cyber activism attacks has dropped in recent years, and cyber activists rarely focus on Danish public authorities and private companies.

- The threat from cyber terrorism is **NONE**. Serious cyber attacks aimed at creating effects similar to those of conventional terrorism presuppose a level of technical expertise and organizational resources that militant extremists, at present, do not possess. Also, the intention remains limited.

Analysis

This report assesses the cyber threat against the defence industry in Denmark. The assessment will examine the different types of cyber threat against the defence industry, including threats that facilitate espionage, crime, activism, terrorism, as well as destructive cyber attacks.

For the purpose of this assessment, the defence industry is defined as manufacturers of equipment and components for systems and platforms used for military purposes.

As many of the components and technologies used in these systems and platforms are dual use, applicable to both civilian and military usage, an overlap often exists between the defence industry and other industries and sectors.

Companies inside the defence industry thus have both civilian and military product ranges and clients. Organizationally, the overlap is also apparent in that some Danish equipment manufacturers, for instance within the maritime sector, are part of international corporations also involved in defence technology. Several foreign defence industry companies have branches in Denmark too.

The overlap means that the threat against the defence industry is connected to the threat against associated industries. Cyber espionage against, for instance, an international defence industry corporation may come to target its Danish subsidiary just as cyber espionage against dual-use technologies may be directed against civilian and military producers alike.

Cyber espionage

The threat from cyber espionage is **VERY HIGH**. As a result, it is highly likely that defence industry companies in Denmark will be the targets of attempted cyber espionage within the next two years.

Several states have performed cyber espionage against the defence industry worldwide.

These states use cyber espionage and other means to obtain industrial and business advantages and to strengthen their security policy position. Espionage against the defence industry is thus likely driven by economic as well as security policy motives.

The states behind the cyber espionage can exploit the stolen information commercially to promote domestic companies and to gain an insight into the military technologies and systems used by other countries.

The potential use of technologies that are applicable for both civilian and military purposes means that both commercial and security policy needs can be obtained in one go. Some countries with extensive cyber capabilities even have a special focus on dual-use technology at the defence policy level.

As part of the modernization of its armed forces, China thus has a declared goal of ”civilian and military fusion” (”junmin ronghe”) whose focus includes dual-use technologies. In Russia, the development of dual-use technologies is also a declared goal for the country’s military development organization, the Advanced Research Foundation (FPI).

Russia and China both hold significant cyber capabilities that they actively use globally.

Due to the overlaps in technologies and organization, the threat from cyber espionage is connected to the threat against associated sectors. Global incidents show a particular overlap with the threat against companies within the maritime and aerospace industries. The Centre for Cyber Security (CFCS) has in assessments for the maritime and aviation industries in Denmark, assessed that the threat from cyber espionage against these sectors is also **VERY HIGH**.

Companies and organizations inside the defence industry may also be used as platforms for attacks against other victims in and outside the sector.

Hacker groups abroad have thus set up fake websites and domains mimicking those belonging to defence industry companies, naval and aircraft exhibitions, and industry associations with the intent to compromise other companies or authorities.

Recent years have seen examples that known hacker groups have used fake job advertisements from defence industry companies, including companies in the United States and India, as lures in phishing attacks.

In another example, a hacker group used documents and military systems as lures in a phishing attacks targeting security-cleared employees in US defence industry companies.

Cyber espionage may also be used in combination with traditional espionage methods and attempts at acquisition of goods under export control.

Cyber crime

The threat from cyber crime is **VERY HIGH**. As a result, it is highly likely that defence industry companies in Denmark will be the targets of attempted cyber crime within the next two years.

For the purpose of this threat assessment, the term cyber crime is used collectively to describe activities in which hackers launch cyber attacks to commit criminal activity for financial gain.

CFCS assesses that the general threat of cyber crime against private companies and public authorities in Denmark also applies to the defence sector.

There have been several publicly known examples of cyber attacks conducted by criminals against the defence sector across the world. However, CFCS assesses that in general cyber criminals do not have a special focus on the sector.

Cyber crime poses an ongoing and active threat to all Danish public authorities, private companies and citizens. Cyber criminals often launch relatively simple attacks against multiple potential victims at once, for instance through phishing attacks. However, networks exist that have the capability to launch more sophisticated and time-consuming cyber attacks, including targeted ransomware attacks.

Rather than singling out a specific target, cyber criminals are typically opportunistic looking to exploit situations to their advantage. Initially, the majority of cyber attacks are opportunistic involving, for instance, phishing emails sent to thousands of victims or criminals exploiting IT systems and devices with known vulnerabilities.

However, there is a growing threat from targeted ransomware attacks against Danish public authorities and private companies. In this type of attack, criminals encrypt vital parts of the victims' IT systems by deploying ransomware, holding the systems hostage for a large ransom fee.

Danish companies have fallen victim to targeted ransomware attacks, which now happen relatively frequent. Danish pump manufacturer Desmi, which is also a supplier to the Danish Armed Forces, suffered a ransomware attack in 2020.

Abroad, aircraft component maker ASCO was hit by ransomware in 2019. The attack disrupted production significantly. ASCO manufactures aircraft parts to military aircraft, including F-35. Earlier that same year, Mitsubishi Heavy Industries Canada Aerospace, another aircraft component maker, suffered a similar attack.

Cyber criminals may also threaten to leak stolen information or sell it. For example, in Australia criminal hackers tried to extort money from Austal, a shipbuilder with both civilian and military customers, by threatening to leak stolen information. The hackers attempted to sell the information online, claiming that the information was related to military vessels.

Since late 2019, hackers behind targeted ransomware attacks have occasionally threatened to leak sensitive data stolen from the infected system unless ransom was paid.

Destructive cyber attacks

The threat from destructive cyber attacks is **LOW**. This means that defence industry companies in Denmark are less likely to fall victim to attempts at destructive cyber attacks within the next two years.

At present, it is less likely that foreign states are intent on conducting destructive cyber attacks against Denmark.

The CFCS defines destructive cyber attacks as cyber attacks that could potentially result in death or personal injury, significant physical damage, destruction or manipulation of information, data or software, rendering them unfit for use unless extensive restoration is undertaken.

It is important to note that the CFCS's definition of destructive cyber attacks cover cyber attacks with very different consequences. The majority of the destructive cyber attacks launched so far have destroyed data by deleting or encrypting it without the option of recreating the data. Even within this broad definition, destructive cyber attacks are relatively rare.

However, several foreign states have the capabilities to launch destructive cyber attacks, which are continuously improved. The threat may increase in connection with intensified political or military conflicts with countries that hold the capability for destructive cyber attacks .

It is possible that Danish private companies and public authorities operating in regions fraught with conflicts may become collateral victims of a destructive cyber attack. So far, most destructive cyber attacks have taken place in Ukraine and Saudi Arabia.

Danish private companies operating in Ukraine and Saudi Arabia, in particular, may in a few cases risk becoming direct targets of destructive cyber attacks. A case in point is the 2018 data wiper attack on Italian company Saipem, a sub-contractor of the Saudi oil company Saudi Aramco. Saudi Aramco itself fell victim to destructive cyber attacks in 2012, 2016 and 2017.

Cyber activism

The threat from cyber activism is **LOW**, suggesting that the probability of companies in the defence industry in Denmark will be exposed to cyber activism within the next two years is less likely.

Globally, the number of cyber activism attacks has fallen over the past few years. Cyber activists rarely focus on Danish public authorities and private companies. The treat from cyber activism is most pronounced in connection with events or single issues that catch the attention of cyber activists.

The purpose of cyber activism is to draw the largest possible attention to a specific cause. To this end, cyber activists use different means and attack techniques that differ in complexity, ranging from relatively simple DDoS attacks to resource-heavy hacks and leaks of sensitive information from public authorities and private companies.

Cyber terrorism

The threat from cyber terrorism is **NONE**, meaning that it is unlikely that Denmark, including companies in the defence industry in Denmark, will be exposed to cyber terrorism attempts within the next two years.

CFCS defines cyber terrorism as cyber attacks aimed at creating effects similar to those of conventional terrorism, including cyber attacks causing personal injury or major disruptions of critical infrastructure.

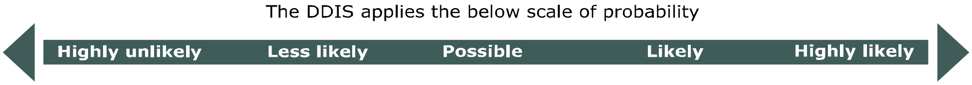
Cyber attacks of such serious magnitude presuppose technical skills and organizational resources that militant extremists currently do not possess. At the same time, the intent to conduct cyber terrorism is extremely limited.

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.