

Threat assessment

# The cyber threat against the Danish financial sector

November 2024

---

## Table of contents

The cyber threat against the Danish financial sector.....	3
Key Assessment .....	3
Introduction.....	4
Cyber crime .....	5
The threat of ransomware attacks remains a serious concern .....	5
Access to financial sector systems and data is of high value to cyber criminals .....	6
Criminals defraud organizations via email .....	7
Cyber crime against bank customers remains an issue of concern .....	8
Digital bank robberies and other types of attack .....	8
Cyber activism .....	11
DDoS – the activists’ weapon of choice .....	12
Cyber activism is more than DDoS attacks .....	13
Cyber activist communication could muddle the picture of the threat landscape.....	13
Cyber espionage.....	14
The financial sector could fall victim to opportunistic cyber espionage .....	14
The financial sector holds valuable data that is often also available in other sectors	14
The threat will likely increase in the event of a conflict .....	15
The cyber domain – an arena for state competition .....	16
Destructive cyber attacks .....	17
The purpose of destructive cyber attacks is likely to sway the population.....	17
Destructive cyber attacks can have serious consequences.....	18
Cyber terrorism.....	19
Threat levels.....	20
Definition of threat levels.....	20

Kastellet 30  
2100 København Ø  
Telefon: + 45 3332 5580  
E-mail: [cfcs@cfcs.dk](mailto:cfcs@cfcs.dk)  
November 2024

Cover photo: The central bank of Denmark (Danmarks Nationalbank)

# The cyber threat against the Danish financial sector

The purpose of this threat assessment is to raise awareness of the cyber threat against the Danish financial sector. The assessment can help strengthen risk owners' understanding of the cyber threat landscape and can be used as part of the basis for improving cyber resilience in the financial sector. This assessment replaces the "Cyber threat against the Danish financial sector", which was published in 2020 and has regularly been updated.

## Key Assessment

- The threat of cyber crime against the Danish financial sector is **VERY HIGH**. Cyber criminals launching ransomware attacks and other types of extortion attacks pose a particularly serious threat.
- The threat of cyber activism against the Danish financial sector is **HIGH**, with DDoS attacks on websites being the most prevalent threat. However, cyber activists are also able to launch other types of cyber attacks, including hack and leak attacks.
- The threat of cyber espionage against the Danish financial sector is **MEDIUM**. The threat level has been lowered from **HIGH** to **MEDIUM**, as the Centre for Cyber Security (CFCS) assesses that the sector is currently not a high-priority cyber espionage target. The CFCS assesses that the Danish financial sector could be targeted by foreign states if the way is paved for opportunistic attacks that require relatively few resources arises.
- The threat of destructive cyber attacks against the Danish financial sector is **MEDIUM**. The threat level is **MEDIUM** because of Russia's increased willingness to use destructive hybrid tactics against European NATO member states. The CFCS assesses that Russia's increased risk appetite also includes destructive cyber attacks. Like other critical sectors, the financial sector could constitute a target for destructive cyber attacks.
- The threat of cyber terrorism against the Danish financial sector is **NONE**. Cyber terrorism requires capabilities that militant extremists currently lack. At the same time, their intent is extremely limited.

# Introduction

For decades, the financial sector and Danish society as a whole has benefitted from the numerous opportunities brought by technological advancements. However, this technological progress has also made the financial sector and society at large highly dependent on digital systems' reliability and integrity.

Knowledge of the threats against these systems, including the cyber threat, is essential in ensuring the continued availability of the services provided by the sector. The vast cyber threat landscape presents significant challenges to public authorities and private companies, including the financial sector, which plays a critical role in Denmark. Persistent or advanced cyber attacks against financial sector companies or infrastructure can threaten the financial stability and the Danish economy.

Many different threat actors are trying to leverage cyber attacks in support of their end goals. Over the last few decades, crime for financial gain, the ongoing inter-state competition and activism have increasingly moved into the cyber domain.

The CFCS classifies cyber threats into five different categories: cyber crime, cyber activism, cyber espionage, destructive cyber attacks and cyber terrorism. Each category is based on the aim of a specific type of attack. The reason for this division is not to simplify the threat but rather to emphasize that the cyber threat is a complex issue that cannot be described from a single perspective. The CFCS uses the Danish Defence Intelligence Service's threat levels and probability degrees, which are explained at the end of this threat assessment.

## **The Danish financial sector**

Denmark's financial sector is made up of companies that provide a wide range of financial services. For the purpose of this assessment, the financial sector covers services such as banks, mortgage institutes, insurance and pension companies, data centres, payment infrastructure, payment institutions, etc. as well as relevant financial public authorities and institutions.

Financial sector companies differ considerably from each other with respect to type of company, the services provided, customer segment, etc. Consequently, the companies in the sector have different approaches to and standards for cyber security. The different nuances of the sector will not be further addressed in this threat assessment but should factor into the individual organization's risk assessment.

This assessment will not deal with threats associated with various crypto assets.

# Cyber crime

The CFCS assesses that the threat of cyber crime against the Danish financial sector is **VERY HIGH**. It is highly likely that Danish financial sector organizations will fall victim to cyber crime attempts within the next two years.

Cyber criminals employ different tactics for financial gain. Cyber criminals will typically try to extort victims, sell victim data or system access or lure victims into transferring money to fraudulent accounts. Though they are incredibly rare, so-called digital bank robberies also pose a potential threat.

## **The threat of ransomware attacks remains a serious concern**

Ransomware attacks pose a significant threat, including to the Danish financial sector. Numerous ransomware attacks are being launched across the world, including in Denmark, and the threat is further amplified by the existence of an extensive underground community of cyber criminals. Certain elements of the cyber criminal community have advanced capabilities and are thus also capable of compromising companies with strong security measures in place.

There have been several examples of successful ransomware attacks on the financial sector across the globe. The CFCS has no knowledge of any organizations in the Danish financial sector having fallen victim to successful ransomware attacks since our latest threat assessment for the financial sector. However, attempts of ransomware attacks have been observed. In addition, ransomware attacks have been launched against suppliers used by Danish financial sector companies.

Ransomware attacks can have serious consequences for the financial sector and for society at large. Ransomware attacks could potentially interrupt operations or disrupt critical services delivered by the financial sector. In addition, publicized ransomware attacks can erode trust in the affected organizations or the financial system at large.

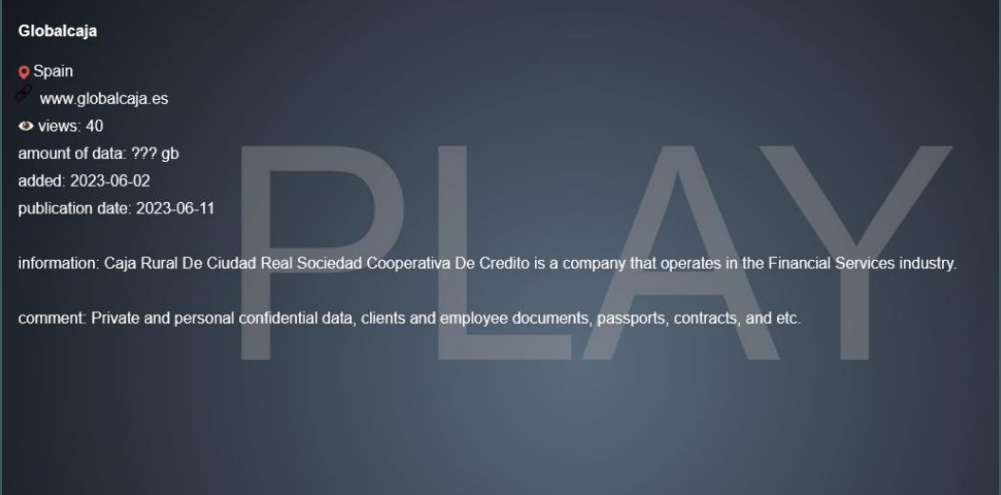
### **Insurance giant paid USD 40 million to criminals**

According to open sources, US insurance giant CNA Financial paid USD 400 million in ransom to criminals following a ransomware attack. The hackers gained a foothold on the company's network through a fake browser update delivered via a legitimate website. Once in, the hackers were able to move across the network, extract data, destroy backups and deploy ransomware.

Over the last few years, it has become increasingly common that ransomware actors steal information from their victims and extort them further by threatening to leak or sell the stolen information. Some actors, who are otherwise known for launching ransomware attacks, sometimes choose to steal sensitive information without the encryption part. Banks abroad have occasionally been the victims of such attacks. The financial sector handles and manages large amounts of sensitive data, making it a prime target for this type of extortion.



Even though extortion without encryption does not cause direct operational disruptions, it may still be necessary to intentionally shut down all systems while the attack is mitigated. Operational disruptions or not, ransomware attacks and extortion without encryption can have serious consequences for the victim as they can e.g. erode customer trust, entail incident response costs, trigger GDPR fines and lead to loss of market value.



The screenshot shows a dark-themed interface with a large, semi-transparent 'PLAY' watermark in the center. On the left side, there is a list of details for 'Globalcaja': a location pin for 'Spain', the website 'www.globalcaja.es', 'views: 40', 'amount of data: ??? gb', 'added: 2023-06-02', and 'publication date: 2023-06-11'. Below this list, there is a line of 'information' stating that 'Caja Rural De Ciudad Real Sociedad Cooperativa De Credito is a company that operates in the Financial Services industry.' and a 'comment' stating 'Private and personal confidential data, clients and employee documents, passports, contracts, and etc.'

Screen dump from the hackers' Dedicated Leak Site (DLS) where Spanish bank Globalcaja was featured on the list of victims.

**Spanish bank hit by ransomware attackers threatening to leak data**

Spanish bank Globalcaja fell victim to a ransomware attack in June 2023. Globalcaja has close to 500,000 customers. The hackers threatened to leak confidential data on client and employee documents and contracts.

### **Access to financial sector systems and data is of high value to cyber criminals**

The CFCS assesses that information stolen from the financial sector and access to financial sector systems and networks are sought after data on cyber criminal marketplaces. Cyber criminals are highly likely well aware of the value of the sensitive information held by the sector..

Cyber criminals can make money by selling sensitive information stolen from the financial sector and its customers. Cyber criminal actors regularly claim to have stolen data from financial sector organizations abroad. For instance, in March 2023, an actor put 60GB data allegedly stolen from Deutsche Bank up for sale at a cyber criminal forum. As previously mentioned, it may cause reputational damage to organizations in the sector as well as financial losses to the affected organization and its customers.

In addition, criminal hackers can make money by establishing initial access to the information structure of financial sector systems and subsequently selling it to other criminals.

Hackers specializing in gaining unauthorized access to systems and selling it to other criminals are called Initial Access Brokers (IABs). IABs have a significant impact on the overall threat landscape for the financial sector. Initial access sale is part of a lucrative ecosystem on various underground forums.

Cyber criminals buy and sell access to compromised devices, malware and services on these forums via a form of platform economy, contributing to expanding the scale and profit of their attacks. The exchange of specialized services among hackers increases the potential for a successful cyber attack. In addition, collaboration and trade support the capabilities of cyber criminals, as hackers can specialize and hone their skills within the individual stages of the cyber kill chain.

It is highly likely that some foreign states turn to the cyber criminal community for malware, for instance by visiting online forums where hackers sell and exchange tools and services. The criminals are not necessarily aware that they are cooperating with or selling tools and services to a state actor. As a consequence, an initial compromise can be used to leverage several different types of attacks.

### **Agent Tesla**

Agent Tesla is one of several types of malware that cyber criminals use to perform cyber attacks, for instance against the financial sector. Agent Tesla is able to record keystrokes, capture screen shots and steal login credentials hidden in web browsers, for example.

### **Criminals defraud organizations via email**

Both Danish and foreign financial sector organizations are regularly exposed to BEC fraud (Business E-mail Compromise). Globally, BEC fraud is among the most lucrative forms of cyber crime. In BEC fraud, criminals try to defraud organizations of money by sending false payment requests. In some cases, the hackers compromise a legitimate email account with an organization or its business partners and subsequently manipulate employees into wiring funds to fraudulent accounts.

BEC fraud via a compromised email account can be difficult to detect as it involves the use of a legitimate email account. However, cyber criminals often do not need to compromise an email account for their attacks to succeed. Instead, they merely have to create emails that look legitimate on the surface, for instance by creating email addresses that closely resemble legitimate email addresses from the recipient's own company.

In addition, cyber criminals can use their knowledge of a company or authority and its employees to make their emails appear convincing. For instance, there have been examples abroad where hackers have used LinkedIn to target new company employees as they often lack the familiarity with company procedures and processes, potentially making them more susceptible to manipulation.

### **Cyber crime against bank customers remains an issue of concern**

Criminals still launch cyber attacks against bank customers in an attempt to gain access to their online banking systems, credit card information or to manipulate the customers into sending money to false accounts. For instance, cyber criminals use malware to steal login credentials, but not all attempts of online banking fraud are cyber-enabled. Online banking fraud, whether cyber-enabled or not, cause significant financial losses every year.

#### **Cyber-enabled criminally manipulated transfers**

The Italian financial sector has been the target of a years-long campaign leveraging a web inject toolkit known as drIBAN.

The goal of the campaign was to infect the systems in the banks' production environment. This allowed the hackers to alter legitimate bank transfers by changing the beneficiary and transferring money to illegitimate bank accounts belonging to either the hackers themselves or affiliates that helped launder the stolen funds.

The attack chain began with a spoofed phishing email containing a malicious executable file that acted as a downloader for the malware. Subsequently, the hackers were able to install a banking trojan that paved the way for drIBAN.

### **Digital bank robberies and other types of attack**

Cyber criminals are creative. Even though most cyber attacks involve ransomware, sale of information or BEC fraud, there is a potential threat that the financial sector could fall victim to other types of cyber crime.

Information stolen from the financial sector could for example be used for financial crime such as insider trading or insurance fraud.

Organizations abroad have previously fallen victim to so-called digital bank robberies. IT security companies and different national authorities have attributed many of these attacks to North Korea.

North Korea is under heavy sanctions, and North Korean state hackers are likely committing cyber crime to generate revenue for the state. Over the last few years, North Korea has been linked to cryptocurrency theft. However, cryptocurrencies are relatively volatile and it is thus possible that North Korea will also target traditional financial institutions.



### **A chain reaction of supply chain attacks**

According to open sources, software company 3CX was attacked by North Korean hackers in early 2023. 3CX's Voice over Internet Protocol (VoIP) software have more than 12 million daily users. An employee with 3CX downloaded an infected version of the X Trader application that installed a backdoor on the employee's workstation that allowed the hackers to move through 3CX's network and infect the main application for sound and video calls. The compromised application was subsequently downloaded by 3CX's unsuspecting customers. The victims also include financial sector customers.

In October 2023, US law enforcement agency FBI warned that North Korea had sent thousands of IT workers outside its borders as part of a scheme to generate revenue for the state. According to the FBI, some of the IT workers have exploited their employee access to infiltrate their workplace networks and steal information which, according to US authorities, can be exploited for extortion purposes, among others. This modus operandi is illustrative of North Korea's creative approach to conducting cyber crime.

# Common attack techniques

In the following section, we will list some of the different techniques that make up the hackers' toolkit. The list is far from exhaustive but includes some of the most common attack vectors. The techniques are employed by cyber criminals and state actors alike. Many of the techniques have been used against the financial sector abroad and in some cases also against the Danish financial sector.



## Phishing

The CFCS assesses that phishing is still the weapon of choice for many hackers. Hackers phish in an attempt to compromise private companies and public authorities in the Danish financial sector. Phishing does not require extensive resources and is a scalable act of deception. Once a phishing email has slipped past the anti-phishing filter, it is up to the individual employee to act as firewall. Phishing emails exploit human psychology to entice employees into clicking on a malicious link or attached file.

Phishing emails are used to lure recipients into disclosing their login credentials or distributing malware. The propagation of generative AI can make it even harder to spot phishing emails as hackers are exploiting the technology to compose highly convincing emails – including in different languages that the hackers themselves do not master.



## Attacks via suppliers

Suppliers, especially software suppliers or cloud suppliers, are attractive targets for both state hackers and cyber criminals. Attacks on suppliers with access to customer IT systems or data are popular as they can give hackers access to multiple targets through a single breach.

Hackers can also launch targeted attacks against suppliers, exploiting them to gain access to organizations with strong security measures in place that would otherwise be hard to compromise directly.



## Exploitation of software and system vulnerabilities

Software vulnerabilities that have not been patched remain a popular exploit among cyber criminals and states. The CFCS assesses that both types of actors are generally quick to exploit their knowledge of vulnerabilities.

For quite some time, states have had the resources to purchase or develop exploits for zero-day vulnerabilities. In 2021, China adopted a law requiring individuals and companies to report all zero-day vulnerabilities to relevant authorities within two days of discovery. A zero day is a vulnerability that has yet to be discovered and addressed by the supplier, making zero-day attacks difficult to counter. The CFCS assesses that several criminal hackers are now also investing time and resources into detecting or acquiring zero-day exploits. As a case in point, in May 2023, the cyber criminal group CIOp exploited a zero-day vulnerability in the MOVEit application to attack and extort numerous victims across the world. The attack affected several banks and financial institutions in the West, including in the Nordic countries.



### **Exploitation of weak or reused passwords**

Simple attack techniques such as brute force attacks are still effective. Brute force attacks cover a wide range of different attacks in which hackers try to guess different combinations of usernames and passwords, for instance through exploitation of leaked passwords from previous data breaches or systematic guessing of combinations across different user accounts. Brute force attacks are directed against many different forms of systems, ranging from email accounts to remote access systems such as Remote Desktop Protocol (RDP).



### **Insider attacks**

The threat emanates from employees with access to IT systems, customer data or knowledge who unknowingly or intentionally facilitate or launch cyber attacks. There have been several examples abroad where cyber attacks on financial companies have been carried out by deliberate insiders and where cyber criminals have made attempts to recruit company employees for malicious acts.



### **Malvertising and watering hole attacks**

Malvertising is the use of online advertising by hackers to spread malware. Hackers inject malware-laden ads into legitimate websites. Downloading of applications such as anti-virus programs is a common technique to infect devices with malware.

Another attack technique that exploits websites is watering hole attacks. In these attacks, hackers compromise legitimate websites by injecting malware. The users who normally use the website risk getting infected with the malware. In watering hole attacks, the website has typically been targeted in an effort to affect a specific target group or because the website has numerous visitors. However, hackers can also infiltrate random websites if they are easy to compromise.

# Cyber activism

The threat of cyber activism against the Danish financial sector is **HIGH**. It is highly likely that Danish financial sector companies and authorities will fall victim to attempts of cyber activist attacks within the next two years.

Cyber activism is performed by individuals and groups that use cyber attacks to draw maximum attention to their cause. Cyber activists also target organizations that they feel do not align with their political views. Pro-Russian groups are a good example of how cyber activists can support state interests. However, that does not mean that they work directly for the state. However, the CFCS assesses that some pro-Russian cyber activist groups are linked to the Russian state.

Activists conduct different types of attacks. Some launch simple defacement attacks and DDoS attacks while others have the capabilities to launch the more demanding hack and leak type attacks.

## **DDoS – the activists' weapon of choice**

Pro-Russian hackers regularly launch DDoS attacks on websites belonging to Western authorities and companies. The financial sector along with the transport sector, abroad as well as in Denmark, has been a high-priority target for DDoS attacks launched by cyber activists. The CFCS assesses that the financial sector represents a symbolic target for cyber activists, but that it is also targeted because of its function as a critical sector as well as its daily interaction with the public that relies on its services. Financial service disruptions generate visibility due to the financial sector's significant exposure to and interaction with the population.

DDoS attacks on Danish banks launched by pro-Russian hacktivists have in some cases briefly prevented bank customers from accessing their online banking systems.

*"They continue to supply arms to Ukraine.  
So we have to teach the two 🇺🇦 countries  
a lesson"*



## **DDoS attacks triggered by Denmark's support for Ukraine**

The quote above is a translation of a pro-Russian activist group's reason for launching a DDoS attack against a Danish bank in late February 2024. During the course of 2023, the group repeatedly targeted their DDoS attacks against the websites of different Danish banks.

Organizations in the Danish financial sector could also become collateral victims of DDoS attacks when the attacks target financial sector suppliers. For instance, Microsoft's cloud service Azure and email client Outlook fell victim to a layer 7 DDoS attack in June 2023. Layer 7 is also known as the application layer and manages the protocols and services necessary for an application to work. The layer is thus the foundation of the software application that the user interacts with. The attack affected the availability of Microsoft's services.

DDoS attacks are, however, often technically simple and do not in themselves have destructive effects. However, the attacks can affect the availability of services and erode trust in the targeted organization.

### **Cyber activism is more than DDoS attacks**

Even though DDoS attacks have generated wide media coverage, the financial sector could also fall victim to other types of cyber activist attacks, such as hack and leak attacks. There have been several examples abroad where hackers have leaked data stolen from bank customers. The data, which included credit card information and personal information, was leaked on hacking forums.

The CFCS assesses that some cyber activist groups are intent on launching destructive cyber attacks but that their capacity is limited.

If cyber activists attempt to launch destructive cyber attacks, weak security measures pose the biggest risk as they could allow for unauthorized system access. Weak security measures enable even low-skilled cyber activists to compromise systems.

Some cyber activist groups have claimed responsibility for destructive cyber attacks in connection with conflicts, for example the conflict between Israel and Hamas and Russia's invasion of Ukraine in 2022. However, most of the attacks have not had any real verifiable impact.

### **Cyber activist communication could muddle the picture of the threat landscape**

The primary goal of cyber activists is to draw attention to their cause. Consequently, the mere mentioning of their attacks is almost as important as the attacks themselves. Often, activists issue misleading and exaggerated details of their attacks. The misleading information is a tool that cyber activists use to strengthen their political narrative and the psychological effect of their cyber attacks.

Cyber activists use their social media platforms, among others, to exaggerate the impact of their attacks. Here, they describe simple DDoS attacks on user-facing websites as incidents generating disruption in critical infrastructure even though this has no basis in reality.

# Cyber espionage

The threat of cyber espionage against the Danish financial sector is **MEDIUM**. It is possible that the Danish financial sector will fall victim to cyber espionage attempts within the next two years.

Compared to the previous CFCS threat assessment for the financial sector, the threat level has been lowered from **HIGH** to **MEDIUM**. The threat level has been changed due to a new analysis of the threat of cyber espionage against the financial sector. The CFCS assesses that even though foreign states have the intent and capacity to conduct cyber espionage against the financial sector, it is less likely that the Danish financial sector is a high-priority target in the short term, i.e. a two-year perspective. Consequently, it is less likely that foreign states will dedicate the necessary resources to target the Danish financial sector in the short term.

## **Espionage is committed under the cover of darkness**

Cyber espionage is typically less visible than other types of cyber attacks. Highly capable hackers try to move undetected in the victims' IT systems in order to gain access to valuable knowledge. Consequently, there is likely a dark figure of cyber espionage.

## **The financial sector could fall victim to opportunistic cyber espionage**

The CFCS assesses that foreign states will attempt to conduct cyber espionage against the Danish financial sector if the opportunity to launch attacks using relatively simple means presents itself. Such opportunities include widespread vulnerabilities that are easily exploitable or extensive supply chain attacks that provide access to numerous victims through a single breach.

The Danish financial sector will thus likely be exposed to reconnaissance by foreign states in the form of vulnerability scans, for example.

## **The financial sector holds valuable data that is often also available in other sectors**

Confirmed examples of cyber espionage overseas indicate that the financial sector is an attractive target. The objective of cyber espionage against foreign financial sectors could have been to harvest data sets, including sensitive personal information, and gain access to confidential information on financial plans, investments and business-critical matters.

In general, the financial sector has access to large quantities of data. In Denmark, the financial sector has extensive information on private and business customers. The financial sector also provides services to independent institutions as well as local and public authorities. The information comprises personal information, strategic investments by customers, financial dispositions and government and public sector borrowing.



The CFCS assesses that much of this information can be collected easier from other sectors. For instance, there have been several examples abroad of cyber espionage attacks targeting lawyers, accountants and consultancy firms.

Lawyers, accountants and consultancy firms also handle sensitive data and information on mergers and acquisitions, financial dispositions, patents, trade secrets, etc. Finally, state hackers can also choose to directly target a specific customer, thereby circumventing the financial sector.

Hackers are more than happy to pursue quick wins. If similar data is available in other sectors that are easier to compromise, they will likely target their attacks against these sectors.

### **The threat will likely increase in the event of a conflict**

The CFCS assesses that the threat of cyber espionage against the Danish financial sector will increase if Denmark becomes embroiled in a heightened conflict, including if the security situation brought about by the Russia-Ukraine conflict escalates towards a military confrontation between Russia and NATO.

In the event of a heightened conflict, the financial sector will likely become a higher prioritized cyber espionage target.

States employ cyber espionage, among others, in preparation for destructive cyber attacks. Destructive cyber attacks against the financial sector could potentially have a serious impact on the population and the economy. Consequently, the financial sector could become an attractive target for destructive cyber attacks in connection with a conflict. The threat of destructive cyber attacks will be touched upon later in this threat assessment.

Known cyber espionage incidents against the financial sectors in Ukraine, Taiwan and Israel indicate that financial sectors are likely deemed prioritized targets for cyber espionage in connection with conflicts. These three countries are all embroiled in intensified political or armed conflict with Russia, China or Iran, respectively.

### **Taiwan's financial sector was exposed to long-term cyber espionage**

The tensions in the Taiwan Strait have heightened over the past few years. Several sectors in Taiwan are being targeted with cyber attacks, and the country's financial sector is not immune to the threat. According to open sources, Chinese hackers conducted cyber espionage against Taiwan's financial sector from 2021 to 2022, exploiting a software vulnerability. The software was widely used by the country's financial sector companies. As a result of the compromise, the hackers gained a foothold in individual networks for several months.

**The cyber domain – an arena for state competition**

Foreign states, including Russia and China in particular, have considerable capabilities to conduct cyber espionage. The CFCS assesses that Russia and China employ cyber espionage for strategic purposes and that cyber espionage constitutes a prioritized tool in their foreign and security policy.

States conduct espionage for a number of reasons, for instance for political ends, to gain comparative advantages within research and development of advanced technology and to shape the battlefield in case of future conflicts. If foreign states steal confidential information from the financial sector it could harm Danish national interests, undermine trust in the sector and adversely affect the competitiveness and market shares of the individual victims.

# Destructive cyber attacks

The CFCS assesses that the threat of destructive cyber attacks against the Danish financial sector is **MEDIUM**. The threat of destructive cyber attacks on Denmark in general was raised in June 2024 from **LOW** to **MEDIUM**, and the CFCS assesses that the threat level also applies to the financial sector. The threat level is **MEDIUM** because of Russia's increased willingness to use destructive hybrid tactics against European NATO member states. The CFCS assesses that Russia's increased risk appetite also includes destructive cyber attacks.

## CFCS' definition of destructive cyber attacks

The CFCS defines destructive cyber attacks as attacks that could result in:

- Death or personal injury
- Significant property damage
- Destruction or manipulation of information, data or software, rendering them unfit for use unless extensive restoration is undertaken.

## The purpose of destructive cyber attacks is likely to sway the population

The CFCS assesses that many types of organizations in critical sectors, including the financial sector, could become targets of destructive cyber attacks. The financial sector has high visibility in the population and plays a central role in facilitating the exchange of goods and services across society, making it a potentially attractive target for destructive cyber attacks. However, the selection of targets will likely be influenced by factors such as established entry points and ease of accessibility.

Russian hacker groups have previously been linked to several destructive cyber attacks against Ukraine, including attacks against the Ukrainian financial sector. IT security companies and different national authorities have attributed many of these attacks to Russia.

The CFCS assesses that the objective of destructive cyber attacks is likely to influence the population and decision-makers. As influencing is likely the primary objective, it is likely that the physical impact of potential destructive cyber attacks on Denmark will be secondary for the hackers as their main objective is to generate attention.

### **Wiper attacks**

The most common type of destructive cyber attacks are wiper attacks. Wiper attacks are designed to delete, overwrite or encrypt data beyond recoverability. Such an attack could be a serious threat to the affected organization and, depending on the target, to society as a whole. By destroying critical information and systems, attackers can hamper or bring business operations to a standstill and potentially disrupt essential services.

### **Destructive cyber attacks can have serious consequences**

In the current situation, it is less likely that Russia is intent on launching destructive cyber attacks on Denmark with serious and far-reaching consequences for critical societal functions, including the financial sector. Even though these attacks are less likely, the CFCS assesses that hacker groups affiliated with Russia are continually preparing the capability to launch destructive cyber attacks against Denmark with this objective. The likelihood of these attacks occurring could thus increase at short notice or without any warning – especially if the conflict between Russia and the West escalates or changes in nature.

However, small-scale cyber attacks could still have a serious impact on the victim and on society as a whole. Such attacks could include attacks that have limited impact on critical societal functions. Even if destructive cyber attacks do not have any impact on critical societal functions, they could cause uncertainty and thereby influence society.

Russia's increased risk appetite could also be reflected in widespread DDoS attacks against critical systems in the financial sector, for instance. DDoS attacks do not in themselves have destructive implications but widespread DDoS attacks against key systems could potentially cripple or incapacitate critical functions for shorter or longer periods of time and thus influence the population and decision-makers in the same way as destructive cyber attacks.

# Cyber terrorism

The threat of cyber terrorism against the financial sector in Denmark is **NONE**. It is highly unlikely that the Danish financial sector will fall victim to cyber terrorism attempts within the next two years.

The CFCS defines cyber terrorism as cyber attacks aimed at creating effects similar to those of conventional terrorism. This could be cyber attacks causing physical harm to human beings or significant disruption of critical infrastructure.

Such serious cyber attacks require technical skills and organizational resources that militant extremists currently lack. At the same time, the intent is limited.

The CFCS has monitored developments in the threat of cyber terrorism since 2016 with focus on militant extremists. The Centre for Terror Analysis under the Danish Security Defence Service (PET) currently assesses that the threat of conventional terrorism against Denmark is at the level of significant. Consequently, the CFCS monitors developments despite the fact that the threat of cyber terrorism has been assessed to be **NONE** for several years.

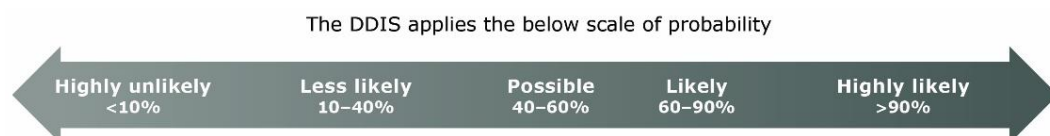
# Threat levels

## Definition of threat levels

The DDIS uses the following threat levels.

<b>NONE</b>	There are no signs of a threat. There are no actors with both the capacity and intention for attacks/harmful activity.
<b>LOW</b>	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.
<b>MEDIUM</b>	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.
<b>HIGH</b>	There are one or 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.
<b>VERY HIGH</b>	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 probabilities are estimates, not calculated statistical probabilities.  
"We assess" corresponds to "likely" unless a different probability level is indicated.