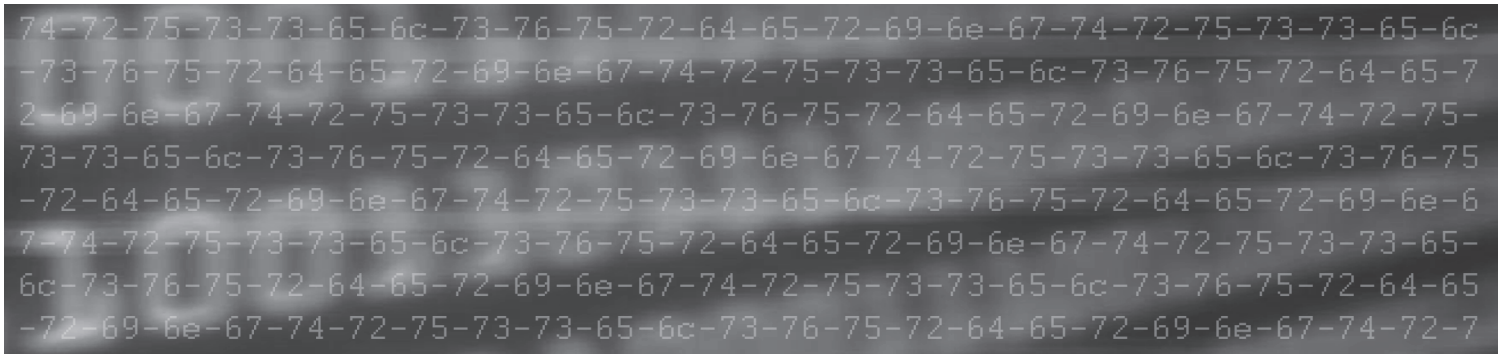
CENTRE FOR
CYBER SECURITY

Threat Assessment

The cyber threat against the Danish financial sector



Threat Assessment Branch under the Centre for Cyber Security

August 2018

CENTRE FOR CYBER SECURITY

Threat Assessment: The cyber threat against the Danish financial sector

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

Key Assessment

- The threat from cyber crime against the Danish financial sector is **VERY HIGH**. The threat from cyber crime is increasingly advanced and complex and cyber criminal attacks may cause disruptions in financial services provided by Danish financial companies.
- The threat from cyber espionage is **HIGH**. It is likely that foreign states have both political and economic interests in engaging cyber espionage against the Danish financial sector.
- The threat from cyber activism against the Danish financial sector is **MEDIUM**. The threat against individual financial companies can change suddenly, if attention of activists towards the company arises for political or ideological reasons.
- The threat from cyber terrorism is **LOW**. Even though militant extremists have expressed an intention to conduct cyber terrorism, they currently lack the capacities to do so.
- Foreign states are less likely to launch destructive cyber-attacks against critical infrastructure in Denmark, including the financial sector. However, it is possible that the Danish financial sector becomes a collateral victim of destructive cyberattacks against targets outside of Denmark.

Introduction

This threat assessment provides an overview of the general cyber threat against the Danish financial sector. The basis for the assessment is primarily Nordic and International examples of cyber-attacks against the financial sector, which are analysed with knowledge of the Danish financial sector and the threat actors' capacities and intentions.

The financial sector supports functions vital to the Danish society. Persistent and advanced cyber-attacks against critical segments of the Danish financial infrastructure may erode confidence in the financial sector and, at worst, threaten financial stability and, ultimately, the Danish national economy. Therefore, it is imperative that the companies, their infrastructure and financial services are available,

reliable and stable so that citizens and companies can rely on the integrity of the whole financial system to make payments, take out loans or trade securities for example.

In its systemic risk analysis for the first half of 2018, the Danish Financial Supervisory Authority (FSA) outlines the potentially serious impact of cyber-attacks against Denmark. The analysis finds that Danish financial companies regard cyber issues as the greatest threat to financial stability in Denmark over the next three years. Also, the report states that cyber security risks are the top challenges facing companies.

The Danish financial sector includes a diverse group of companies carrying out a wide range of tasks. In this assessment, the financial sector includes companies subject to financial regulation such as banks, mortgage credit institutions and insurance companies as well as financial infrastructure companies such as data centres, stock exchanges, etc. Authorities and public financial institutions such as the Danish FSA and the Danish National Bank are also part of the financial sector. The market for crypto currency is not included in this threat assessment as it is currently not subject to financial regulation. This threat assessment provides an overview of the cyber threats against the financial sector in Denmark as a whole, only making limited distinctions between the different components of the sector.

Danish financial institutions are highly interconnected through the digital infrastructure. The financial sector's overall resilience toward cyber-attacks to some degree depends on the cyber security capabilities of all financial organizations as those with vulnerable cyber security may be exploited by hackers and used as platforms to target organizations with better protection. The Danish financial sector may also be affected by cyber-attacks that are targeting foreign and international partners or counterparties, as Danish financial institutions are also connected to foreign financial institutions through the interbank market, which has repeatedly been exploited in cyber-attacks. Cyber-attacks against key software suppliers to the financial sector also pose a threat as hackers are able to use the suppliers as launching pads to gain access to their end target.

The interbank market
The interbank market is a market only for financial institutions and allows for trading in all securities including credit agreements, interest rate derivatives and currency trading.

SWIFT
SWIFT (the Society for Worldwide Interbank Financial Telecommunication) is an international financial data network that enables financial institutions to send and receive information about financial transactions.

What are cyber threats?
The Danish Defence Intelligence Service's Centre for Cyber Security (CFCS) defines cyber threats as threats from cyber-attacks in which an actor tries to disrupt or gain unauthorized access to data, systems, digital networks or digital services. Use of the Internet for other purposes that may have

negative impact on society such as facilitation of money laundering is not included in thid definition of cyber threats.

Cyber threats are multi-faceted. In this assessment, CFCS will focus on the purpose for the actor to carrying out a cyber-attack. CFCS describes and assesses activities which have the purpose of conducting cyber espionage, cyber crime, cyber activism or cyber terrorism. Besides this, the CFCS assesses the potential threat from destructive cyber-attacks.

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

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

The exact number of cyber-attacks against authorities and private companies is subject to some uncertainty as not all cyber-attacks are reported to the relevant authorities – either because the organization wants to avoid drawing attention to the cyber-attack or because the attack has not been detected. In May 2018, by law, the Danish government introduced a new incident reporting system which is expected to give a better insight of cyber-attacks against critical sectors.

Cyber crime

The threat from cyber crime against the Danish financial sector is **VERY HIGH.** In this assessment, cyber crime covers financially motivated criminal activities.

The threat from cyber crime against the Danish financial sector is directed at financial companies and clients alike. Advanced and targeted cyber-attacks happen with relatively low frequency. Such attacks can have serious consequences for financial companies in terms of loss of liquidity and reputation. Cyber criminals also try to steal data from financial companies.

Cyber attacks against the financial sector's clients are less advanced and less profitable, but attackers target many clients in one attack and often attack again and again. The increased use of eBanking and mobile banking services by Danes and Danish companies have increased the basis for hackers to launch cyber-attacks.

While cyber crime attacks against financial sector companies may have significant consequences that reach far beyond the companies, at worst, threatening financial stability in Denmark, cyber crime against clients may undermine confidence in the financial sector.

The threat from cyber crime is increasingly complex

Cyber criminals targeting the financial sector may range from individuals launching unsophisticated bulk attacks to skilled actors with sophisticated cyber capabilities specifically targeting financial companies or authorities. Some of the sophisticated cyber criminal groups are well organized, operating like companies with management structures and units tasked with developing and testing malware and carrying out money laundering. The threat picture facing the financial sector is further complicated by the fact that state-sponsored hackers likely launch financially motivated cyber-attacks against the financial sector. Attack types and actors which the financial sector has to defend itself from have become more advanced.

CFCS assesses that parts of the cyber crimes affecting the sector are growing in complexity and that advanced cyber criminals are launching increasingly targeted attacks. Hackers are becoming increasingly focused with regards to which regions, countries, companies and client segments they attack.

Cyber criminals are resourceful and quick to deploy new techniques, vulnerabilities and attack methods; for instance, some hackers are capable of quickly developing new versions of malware aimed at avoiding antivirus solutions. At times, there are only a few days between an initial attack is propelled until the hackers strike back with a slightly modified version of the same malware. During 2017, some actors have been able to introduce new malware versions on a daily basis. The financial sector is therefore facing a cyber-threat which is continuously evolving and adapting.

Cyber criminals also sell their services and tools, allowing less skilled criminals to pose a more serious threat. Hackers sell and share sophisticated tools and their knowledge of software vulnerabilities on the Internet. Consequently, tools and vulnerabilities that were previously mainly available to states are now to some degree being used by non-state cyber criminal hackers.

Globally, cyber criminals have directed various types of cyber-attacks at financial companies and authorities. A number of these cyber-attacks are outlined in the following pages. Even though some of these types of attacks have not yet been targeting the Danish financial sector, CFCS assesses that they are part of the overall threat picture facing the financial sector.

Hackers steal money in advanced digital bank robberies

In recent years foreign banks have been hit by a series of advanced cyber-attacks where actors have stolen considerable amounts of money. In some instances, the attacks have also disrupted the availability of financial services afforded by the affected banks. In several of the digital bank robberies, the hackers have exploited the interbank market's infrastructure. Illustrative of this is the February 2018 cyber-attack against City Union Bank in India, where hackers tried to steal USD two million by compromising the banks systems and thereby conducting unauthorized money transfers through the SWIFT-network. The attack, however, was only partially successful as some of the fraudulent transactions were detected and blocked. In several cases, cooperation between banks has prevented cyber criminals from carrying out unauthorized money transfers, thereby partially or fully mitigating attacks. However, in 2016 and 2017, hackers managed to compromise a number of local banks and siphon money corresponding to DKK 500 million by exploiting the SWIFT network. In some cases, the

banks had apparently been compromised through spear phishing mails sent to employees. Several security companies have attributed a share of these digital bank robberies to hacker groups, which CFCS assesses to be affiliated with North Korea.

SWIFT is not the only financial data network that facilitates financial transactions. Other financial data networks can also be exploited in digital bank robberies. In the spring of 2018, Mexico's financial data network SPEI was exploited in an attempt to steal money from local Mexican banks. In May 2018, Mexico's Central Bank stated that five unnamed banks had been hacked and that the hackers had siphoned an amount corresponding to nearly DKK 100 million.

Hackers have highly likely conducted reconnaissance ahead of the advanced digital bank robberies, by gaining unauthorized access to information on the bank's systems and processes. Banks that have been exposed to cyber-attacks allowing hackers access to confidential information or vital systems are thus more vulnerable to digital bank robberies.

In early 2017, the website of the Polish financial supervision authority was exploited in a watering hole attack to spread malware. The attack was possibly part of a reconnaissance ahead of subsequent attacks. CFCS is currently not aware of whether victims affected by the attack have suffered any economic losses so far. The watering hole infected a number of specified organizations visiting the website with malware. Among the targeted were three Danish financial companies. The watering hole attack was extensive, affecting more than 100 financial institutions in over 30 countries. Security companies assess that the watering hole attack in Poland was carried out by the same nation state actor responsible for the 2016 digital bank robbery against the Bangladesh Central Bank.

Watering hole attack
A watering hole attack is a malware attack in which the attacker seeks to compromise a specific group of end users by infecting a legitimate website with malware. The hackers may attempt to compromise all or targeted users.

This actor has also been identified by IT security companies as the one responsible for the 2018 cyber-attack against Turkish financial institutions aimed at collecting data for subsequent attacks. The financial institutions in Turkey were targeted through spear phishing emails containing files with a malware called Bankshot.

Hackers demonstrate willingness to destroy or encrypt data in digital bank robberies
In a few attacks carried out in recent years, hackers have demonstrated a willingness to destroy or encrypt financial company data in connection with digital bank robberies, probably in an attempt to cover their tracks or prevent companies from responding to the theft. CFCS assesses that these activities could also be carried out in connection with a digital bank robbery against a Danish financial company.

Although data destruction or encryption in digital bank robberies is as yet a relatively rare phenomenon, it could potentially have serious impact on the affected financial institutions. If hackers successfully encrypt or destroy critical data, the services afforded by the affected institutions may be disrupted or rendered unavailable. Illustrative of this is the May 2018 attack in which hackers , according to open sources, deleted the hard disk drives of the Bank of Chile (Banco De Chile), disrupting some of the bank's services. The aim of the attack was seemingly to steal assets, and the hackers probably deleted data to obstruct subsequent investigations.

Hackers steal information from financial companies

CFCS assesses that cyber criminals also have the intent and capacity to steal information from Danish financial companies.

Financial companies are highly data-driven and dependent. A large share of their data may be valuable to hackers, and data theft is particularly critical to a financial company's business operations and corporate reputation. Sensitive data ranges from simple customer credit card and account information to more complex data such as private customer data, creditworthiness and other financial affairs, business strategies, IPO's, etc., including information on the financial company's own business affairs such as financial reports, business strategies, acquisitions, software, liquidation and restoration plans.

Cyber criminals may try to steal information from the financial sector and sell it to other parties for profit. A group known as Carbanak managed to compromise a number of foreign financial institutions and steal sensitive information. After having gained access, the group searched for company systems that could access the financial data of interest such as specific programmes and processes relating to credit card data. The group had monitored employee screen displays to learn how to use company systems, and once it had identified the data of interest and a method to access the information, it was able to extract the data.

Hackers may also steal data from financial institutions for extortion purposes. CFCS has no knowledge of any incidents in the Danish financial sector where hackers have extorted victims by threatening to leak or sell stolen information. Foreign financial institutions and companies in other sectors in Denmark have been victims of such criminal activity. For instance, in May 2018, hackers successfully stole approx. 40 GB data from a Brazilian bank, subsequently demanding a ransom in Bitcoins. There is a risk that cyber criminals may try to exploit the new General Data Protection Regulation in order to extort public authorities and private companies, threatening to hack the organization unless ransom is paid. In case the organisation already is compromised, hackers may demand ransom in exchange for not leaking stolen data or publicly disclosing that the company has been compromised.

Cyber criminals may also steal information which can be used for insider trading. In March 2018, hackers tried to gain access to the Danish insurance company TRYG's systems, possibly to steal sensitive information which could be used for insider trading. The hackers sent spear phishing emails containing malicious files attachments to four key employees. However, the attack was detected in time to prevent the hackers from compromising the system.

DDoS attacks disrupt financial online services

Over the past years, DDoS attacks have threatened the availability of financial services. Globally, there are numerous examples of DDoS attacks against the financial sector. In 2017, Lloyds Bank in Great Britain was the victim of a massive DDoS attack disrupting its online banking services for two days. The actor demanded a GBP 75,000 Bitcoin ransom to stop the attack. The British authorities managed to identify and prosecute the actor responsible for the attack. One of the most known examples of the potentially disrupting impact of a DDoS attack dates back to 2007 when an extensive DDoS attack paralyzed multiple sectors critical to the Estonian society, including the financial sector. The attack periodically disrupted the services of two of the country's largest banks.

One reason for the high number of DDoS attacks is that these attacks can easily be carried out with tools that are available online. In September 2017, a Dutch online bank was made unavailable by a DDoS attack carried out by a teenager, who, according to open sources, had downloaded a DDoS tool online. By the end January 2018, the teenager was arrested shortly after several other Dutch online banking services were compromised by a DDoS attack. It remains uncertain whether the teenager was responsible for these subsequent attacks.

DDoS attacks

Distributed Denial of Service (DDoS) is a cyber attack in which the attacker exploits compromised devices to generate an overwhelming amount of data traffic against a website (web server) or network, rendering it unusable.

Fewer but more targeted ransomware attacks in future

So far, ransomware attacks have been a common type of attack which continues to pose a threat to the financial sector. By encrypting data, ransomware renders the victim's data and systems unavailable, allowing the perpetrators to demand a ransom to decrypt in order to make the data available again. Following a few years of increasing ransomware attacks, IT security companies report that the number of attacks is decreasing. However, ransomware attacks may become more targeted and sophisticated, potentially posing a threat to corporate infrastructure or production lines.

Ransomware attacks may also be launched in parallel with other attacks against the financial sector. Open sources report that in 2017, when hackers stole money from Far Eastern International Bank in Taiwan, they also directed a ransomware attack against the bank's systems to divert attention or cover their tracks.

Business Email Compromise (BEC) poses challenge

Business Email Compromise scams, so-called BEC scams, continue to pose a threat to all sectors including the financial sector. BEC scams typically target companies and authorities with fraudulent emails, containing instructions to wire funds to the actor's account. In order to exploit the loyalties of employees cyber criminals impersonate an in-house executive (often the CEO) who is authorized to do wire transfers, which is why this type of scam is frequently also referred to as CEO fraud. Every day, the financial sector settles thousands of transactions – many for which time is crucial aspect –

rendering the financial sector vulnerable to BEC scams as it can be difficult for the employees to verify the legitimacy of requests due to time pressure.

The fraudulent emails are often sent from external email accounts mimicking legitimate email addresses, but the actor can also exploit compromised email accounts of in-house employees. If an actor compromises an employee account this increase the hackers' chance of succeeding in fraud attempts, as the hackers hereby have gained access to information which is not publicly available.

Cryptocurrency mining malware can slow down systems

Cryptocurrency mining malware has become popular among cyber criminals, who use the malware to tap into the computing power of victim devices to mine cryptocurrencies such as Bitcoins. The increase in value of cryptocurrencies has likely contributed to the popularity of cryptocurrency mining attacks. It is likely that rapid declines in the value of cryptocurrencies may dissuade cyber criminals from launching this type of attack. In addition, IT security companies report that a rise in cryptocurrency mining malware may correlate with a decline in the use of ransomware. Consequently, a decline in the value of cryptocurrencies may potentially spark a rise in the use of ransomware.

Cryptocurrency mining is a resource-intensive undertaking that typically requires a massive amount of computing power from the infected devices, potentially affecting servers and causing operational disruptions, longer response times and, at worst, breakdowns. Financial systems and software which have been infected by malware exploiting their processing power may impair the availability of financial services. In addition, malware designed to mine cryptocurrency may disrupt some of the time-depend services offered by the financial sector, such as refinancing auctions, IPOs or securities trading in secondary markets. Trading servers must be able to handle a vast amount of data fast, since securities trading is exclusive electronically. If the processing power of a trading server is abused by cryptocurrency mining malware, it may decrease the speed at which markets and traders can trade and exchange information on securities, at worst preventing them from trading securities or causing serious information delays.

Even in the event that cryptocurrency mining malware attacks against the financial sector do not cause operational disruptions, such attacks still pose a problem, as cyber criminals may later exploit access to the targeted system for other purposes or cause unintentional damage. In addition, the malware may consume so many computational resources that it warrants a major investigation by the IT department, and the process of removing the malware may be so time consuming and arduous that it renders the infected systems temporarily unavailable.

Cyber-attacks against ATMs primarily target foreign financial companies

Malware targeting ATMs is another technique, used by cyber criminals to steal cash. CFCS has no knowledge of this type of attack being widespread in Denmark, although it did occur in 2017. According to IT security firms, attacks against ATMs outside of Europe are on the rise. Cyber criminals fraudulently posing as ATM technicians gain physical access to the cash machine using a phone or laptop to install malware and take control of the machine. Once taken over, the machine can be programmed to dispense cash at specific times with money mules standing by to retrieve the money. In some cyber-attacks against ATMs outside Denmark, the malware has also been used to steal credit

card information from unsuspecting ATM customers. CFCS has knowledge of a group called Cobalt Gang which is active in the Nordic countries and that the group has attempted to gain access to Nordic banks' systems. The group has launched cyber-attacks outside Denmark against ATMs by compromising the IT systems of the banks.

Credit card information stolen in cyber attacks against targets outside the financial sector
For years, cyber criminals have targeted customer credit card information with the purpose of exploiting the information or selling it to third parties. Hackers often steal credit card information by compromising a non-financial sector company or system. An example of this is online retailers with a vulnerability in its payment system which is exploited by cyber criminals. Even though these companies are not part of the financial sector, attacks against them still affect the sector, as it has to use resources to handle the credit card information theft.

Examples abound in which cyber criminals have breached foreign companies and gained access to customer credit card information, including cards issued in Denmark. In 2016, Danish payment processor company Nets advised local Danish banks to replace 100,000 potentially compromised credit cards pre-emptively, citing that the breach was probably linked to transactions with a foreign online retailer. This was one of the largest potential compromises of Danish credit cards. A more recent example of compromised credit card information is from late June 2018, when Ticketmaster UK announced that it had discovered malicious software on one of its customer support products hosted by a third party and that credit card information from its customers might have been compromised. As a security precaution, Danish Ticketmaster customers who had bought tickets during a specific time were advised to monitor their account statements for evidence of fraud. However, recent figures from Nets show a fall in reports of online shopping fraud, possibly as a result of the two-factor authentication which has gradually been introduced since May 2017.

Malware steal online banking login information
Malware still poses a significant threat to financial services customers, who may incur financial losses. The malware is often delivered to the victims by means of phishing mails from the hackers who use the malware to steal online banking credentials. Illustratively, the malware known as TrickBot redirects the customer to a fake web banking login page that looks exactly like the legitimate site. Once the login credentials have been entered, the malware will log in the customer to the legimate online bank while simultaneously sending the login credentials to the hackers. Trickbot has previously been targeting Danish banks, and it is highly likely that customers will be targets of malware with similar functions in the future.

Malware is also targeting mobile banking apps. The malware hides the original app screen behind a fake one. Users are asked to enter their credit card information, which is then stored by the malware. Layering of the fake app on top of the legitimate app makes detection more difficult. Security firms report that actors have started customizing their malware to specific customer segments such as private and institutional customers in a bid to optimize the effectiveness of the malware.

CFCS assesses that the threat from malware directed against Danish mobile banking apps is rising as the complexity and volume of malware have increased considerably. More customers use financial

services apps, increasingly enabling hackers to steal financial information and for larger criminal profits. Actors have developed malware specifically against apps developed by the Danish financial sector. Security experts have warned that the malware known as Red Alert has been developed specifically to also target the mobile banking apps provided by the five largest banks in Denmark.

IT security companies have recently discovered new versions of malware targeting banking apps with key-logger functions designed to monitor and log all keystrokes on the mobile device. Hackers have also expanded malware targeting banking apps allowing the hackers to use the malware to encrypt the victim phone or mine cryptocurrency.

Cyber espionage

The threat from cyber espionage against Danish financial institutions is **HIGH**.

CFCS assesses that the threat mainly emanates from foreign states, which likely have political as well as economic motives for committing cyber espionage against the Danish financial sector. In general, the threat from cyber espionage against Denmark is **VERY HIGH**, as foreign states are persistently making efforts to steal information from the government as well as from specific sectors. CFCS has no knowledge of an equally high level of activity against the financial sector but CFCS assesses that foreign states have the intent and capacity to commit cyber espionage against the financial sector with some financial institutions being more at risk than others.

Foreign states may conduct cyber espionage against the Danish financial sector to gain insight into investments or potential company acquisitions. Foreign states may also have an interest in spying against Danish companies in order to advance their own national companies. Consequently, foreign states may have a special interest in Danish financial companies with branch offices or subsidiaries with cross border businesses.

Cyber espionage might have serious consequences for Denmark, for example if a foreign state gains unwarranted access to valuable information on the Danish financial infrastructure or sensitive information from a large financial company. In addition to the socio-economic consequences of such an access, it might also damage the reputation of the Danish financial sector as well as affecting the confidence of the public, customers and partners in the sector.

Cyber espionage can also be used to underpin other types of cyber-attacks and threats. A company or public authority that has already been compromised is thus more vulnerable to destructive cyber attacks or hack and leak attacks.

Cyber espionage may be used to uncover weaknesses in the financial sector. Knowledge of such weaknesses may be exploited in the event of a future conflict to facilitate destructive cyber-attacks.

Cyber espionage may also enable an adversary to steal sensitive information and leak it in an attempt to sway public opinion. Hacked information may also be used in wide-ranging influence campaigns. For example, sensitive information concerning a politician’s personal financial situation or personal

investments from their banks may be leaked in a bid to damage their reputation. Information on the solvency of large financial companies or on an expected drop in market prices, such as stock market prices, may also be leaked in an attempt to affect the individual financial company's solvency and net worth and, ultimately, Denmark's national economy. However, CFCS is not aware of any examples of hack and leak attacks against the Danish financial sector.

Cyber activism

The threat from cyber activism against the Danish financial sector is **MEDIUM**.

Cyber activists typically launch attacks for ideological or political reasons, and they often target individuals or organizations that are perceived as opponents to their cause. Some hacker groups and cyber activist network members have significant capabilities and resources to launch cyber-attacks. Consequently, the threat level may suddenly increase, should Danish financial companies attract the attention of cyber activists. Financial companies should thus be particularly aware of the risk of cyber activism in situations where they may become embroiled in single issues that may be subject to public debate or in cases where cyber activists threaten to launch attacks.

For years, hackers claiming to belong to the activist groups Anonymous have called for cyber-attacks against large financial institutions worldwide. In 2010, members of Anonymous launched DDoS attacks against Visa, Mastercard and PayPal after these companies had blocked customer donations to WikiLeaks. In the subsequent court case against some of the hackers, PayPal stated that the attack had cost the company GBP 3.5 million.

Cyber activists also use other types of attacks besides DDoS attacks to draw attention to their cause. Cyber activists have been known to hack and leak sensitive information or launch so-called defacement attacks in which hacked websites have been defaced with political messages. In May 2018, an Italian group by the name of AnonPlus hacked the website of a smaller Danish bank using the Anonymous logo and lingo. The hackers replaced the bank's website with AnonPlus's political manifesto in which they declared that they were opponents of financial institutions. The hackers did not gain access to customer information, but the attack temporarily made the bank's website unavailable.

Financial authorities or companies in Denmark may become targets of cyber activism even though they might not be linked to the actual issue that has caught the activists' attention. The reason might be that hackers consider the authorities or companies symbolic targets. Authorities or companies with a strong public presence may also become targets as they can provide the hackers with a greater platform to promote their cause. At times, cyber activism is purely opportunistic and dependent on where actors can gain access and exploit vulnerabilities.

It is likely that Turkish cyber activists perceived the central bank of Denmark as a symbol of the Danish government when they launched a DDoS attack on the institution in September 2017. This was likely in response to a debate on the Muhammed cartoons, though the central bank was not directly involved in the issue.

Cyber terrorism

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

CFCS assesses that militant extremists have limited capabilities and resources to launch cyber terrorism attacks. Even though some militant extremists have expressed interest in launching cyber terror attacks, they do not currently possess the necessary capacity.

Consequently, there is a low threat from cyber-attacks against the Danish financial sector with the intent of causing the same effect as more conventional terrorist attacks, for example cyber-attacks resulting in personal injury or property damage or widespread disruption of the financial sector's infrastructure.

Destructive cyber attacks

A number of countries have access to destructive cyber capabilities that could potentially be used against critical infrastructure such as the financial sector.

CFCS assesses it less likely that foreign states have the intent to launch destructive cyber-attacks against critical infrastructure in Denmark, including the financial sector. The threat can increase, if a political or military conflict in which Denmark is involved escalates.

Destructive cyber attacks
CFCS define destructive cyber-attacks as attacks that could potentially result in death, personal injury, property damage, or destruction or manipulation of information, data or software, rendering it unfit for use unless extensive restoration is undertaken.

At present, destructive cyber-attacks against targets outside of Denmark could have negative spillover effects on Danish companies and public authorities. This is particularly relevant for Danish companies, including financial companies, operating in conflict areas where foreign states or organized hacker groups with strong cyber capabilities have vested interests to defend, for example in parts of Eastern Europe, the Middle East and Southeast Asia.

Foreign financial companies in Ukraine and South Korea have been the targets of destructive cyber-attacks adversely affecting the availability of financial services. In late 2016, Ukraine's Ministry of Finance and other financial authorities were infected by data-wiping malware. Bank transactions were delayed or cancelled, which also had consequences for citizens. In 2017, Ukrainian banks were also hit by the NotPetya attack, which was likely a destructive cyber-attack disguised as a ransomware attack. The Ukrainian bank Oschadbank was severely affected and the effect was very visible as a message demanding ransom could be seen on the monitors of the bank's ATM terminals in Kiev.

ATM in Kiev that was disabled by the NotPetya attack

Threat levels

The Danish Defence Intelligence Service (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.