CENTRE FOR
CYBER SECURITY

Threat assessment 2020

The cyber threat against Denmark

Indhold

CENTRE FOR
CYBER SECURITY

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

The cyber threat against Denmark

The purpose of this assessment is to inform public authority and private company decision-makers as well as citizens of the cyber threat against Denmark. Threat awareness may be used as a tool in prioritizing cyber security measures in individual public authorities and private companies and in Denmark as a whole.

Key assessment

- The cyber threat pose a serious threat to Denmark. Cyber attacks mainly carry economic and political consequences.

- Hackers have tried to take advantage of the COVID-19 pandemic. This constitutes a new element in the general threat landscape.

- The threat from cyber crime is **VERY HIGH**. No one is exempt from the threat. There is a growing threat from targeted ransomware attacks against Danish public authorities and private companies.

- The threat from cyber espionage is **VERY HIGH**. The threat is especially directed against public authorities dealing with foreign and security policy issues as well as private companies whose knowledge is of interest to foreign states.

- 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.

- The technological development, including the development of artificial intelligence and quantum computing, creates new cyber security possibilities and challenges.

Analysis

The Danish Defence Intelligence Service's Centre for Cyber Security (CFCS) now releases its fifth annual assessment of the cyber threat against Denmark. Cyber attacks are used by different actors to serve different purposes.

As in previous years, the assessment is divided into threats of cyber attacks that facilitate crime, espionage, activism and terrorism, as well as destructive cyber attacks. This year, the threat from destructive cyber attacks has for the first time been assigned a threat level in the recognition that destructive cyber attacks are not only an attack method; they can also serve a purpose in themselves.

The threat levels of cyber espionage and cyber crime continue to be **VERY HIGH**. The cyber threat to Denmark is still serious and will remain so in the future due to the continued digitalization and dependence on digital services.

Since our last assessment, the CFCS has adjusted two of the threat levels, downgrading cyber activism to **LOW** from **MIDDLE** and cyber terrorism to **NONE** from **LOW**. This adjustment is in response to a decrease in the threat from both types of cyber attacks as outlined below.

In the 2020s, new technologies such as quantum computing and artificial intelligence may work as drivers to push the cyber threat and cyber security in new directions – both positive and negative. Both technologies are dealt with in this year's trend analysis that concludes the assessment.

The cyber threat during the COVID-19 pandemic

Digitalization has helped mitigate the consequences of the health care crisis during the COVID-19 pandemic. The need for physical distancing has been underpinned by new routines such as increasing use of telecommuting, online meetings, home schooling and social media as well as the application of new technologies and platforms.

However, such new routines have also laid bare our dependency on digitised solutions, including their integrity, confidentiality and accessibility, intensifying cyber security awareness among many authorities and companies.

Hackers are constantly poised to exploit current events, developments and conditions to their own advantage. This has also been the case during the COVID-19 pandemic with foreign states and cyber criminals alike using COVID-19 as a lure in phishing mails.

The exploitation of COVID-19 constitutes a new element in the general threat landscape, but the overall threat level has not been affected significantly. The COVID-19 pandemic has primarily changed the threat landscape as regards the type of attack vectors used by the hackers. Consequently, the main focus of this threat assessment is on factors impacting the cyber threat besides COVID-19.

Authorities and businesses may become increasingly vulnerable during a crisis such as the ongoing COVID-19 pandemic. The cyber security of many authorities and companies is under pressure due to the change in routines in the form of increased use of telecommuting and because the availability of the systems takes priority.

The new working conditions may act as gateways for hackers into corporate systems and could impede detection of hacker presence. As a result, even though the overall threat landscape is unchanged, Danish authorities and companies may be facing changes in their risk landscape.

Hackers abuse COVID 19 as a theme

The CFCS has registered an increase in phishing emails sent to Danish authorities and companies during the COVID-19 pandemic. Several IT security companies also report an increase in phishing attempts in other countries since March.

Many of these phishing emails use COVID-19 as a lure in order to increase the likelihood that the receiver opens the email and clicks on links or attached files. The hackers thus try to exploit the Danes eagerness to stay updated on COVID-19 and the current health crisis.

The CFCS assesses that criminals will also try to take advantage of public compensation schemes as a theme in their phishing emails.

The COVID-19-pandemic has also seen the creation of quite a few new fake domains that are used by criminals to trick Danish citizens into disclosing their NemID information – NemID is Denmark's common secure login solution – or other login information. Some of the fake domains are hard to distinguish from legitimate health authority websites and names. The CFCS collaborates with our partners to take down known fake domains.

Furthermore, fake applications and malware for mobile devices have been created using COVID-19 as a theme. The false apps may, for example, steal information from the mobile device.

The CFCS assesses that hackers are exploiting the increased need for remote access, VPN solutions, online collaboration and communication platforms.

The cyber threat on the threshold to a new decade

The cyber threat is not only impacted by current events such as COVID-19, it also reflects the long-term development in how cyber attacks are used by state as well as non-state actors. As we stand on the threshold to a new decade, it is only natural to take stock of the cyber threat development in recent years.

Cyber attacks still mainly carry economic and political consequences. Unlike the threat from, for instance, war and terrorism, cyber attacks do not as yet pose a general threat to life and health. However, isolated cyber attack incidents resulting in physical damage and consequences of for instance ransomware attacks against hospitals, are proof that cyber attacks do pose a potential threat to life and health. Due to the continued digitalization of critical functions in society, cyber attacks may increasingly carry serious consequences in the physical world.

Some states, in particular Russia and China, use cyber espionage very actively, and there are no signs indicating a decrease in this threat. Recent years have seen an increase in the number of countries that use cyber espionage, in particular in Asia. With a few exceptions, destructive cyber attacks remain a regional phenomenon linked especially to the conflict in Ukraine and to the rivalry between Iran and Saudi Arabia. However, such attacks can spread and affect Denmark, as was the case in the 2017 NotPetya attack.

The increase in social media use and the challenges in assessing the veracity of information have provided states with new tools to influence populations. Hack and leaks in connection with the 2016 US presidential election was a new and serious application of cyber attacks in support of an influence operation attempting to influence public opinion in another country.

Criminals have continued the digitalization of traditional financially motivated crime. Technologies such as crypto currencies and anonymization services have provided a profitable foundation for a more evolved criminal environment with better options for cooperation between criminal. Some cyber criminals have expanded their operations to include criminal-to-criminal franchise models and customer support services.

In recent years, cyber activism has been on the retreat, except in places of social and political unrest. Militant extremist groups have been under strong pressure from the international anti-terrorism effort, and militant extremists have yet to succeed in launching serious cyber attacks with a terrorism perspective.

Infamous 2010s cyber attacks
Below are examples of known cyber attacks from the 2010s.

Stuxnet (2010) Iranian centrifuges for enrichment of uranium were the targets of a destructive cyber attack in 2010 involving the Stuxnet malware that resulted in physical destruction of the centrifuges.

Saudi Aramco (2012) The Saudi national oil and gas company, Saudi Aramco, became the target of a cyber attack in 2012 that resulted in the destruction of a large amount of data belonging to the company.

The Sony Hack (2014) Hackers attacked Sony Pictures Entertainment in 2014, destroying data and systems as well as leaking emails and copies of yet to be released films.

Power outages in Ukraine (2015) Several electricity companies in western Ukraine were hit by cyber attacks in 2015. The hackers gained access to the companies' control systems, shutting off power for up to six hours.

Democratic National Committee (2016)
The Democratic National Committee in the United States became the target of hack and leaks of information, including emails, in 2016 ahead of the presidential election that same year.

Mirai (2016) The Mirai malware was used to launch some of the until then largest Distributed Denial of Service (DDoS) attacks in 2016. One of the attacks rendered a number of major Internet services inaccessible.

WannaCry (2017) The WannaCry ransomware started to spread automatically to computers worldwide in May 2017. WannaCry facilitated encryption of files on victim computers and erasing of original files. Ransoms were then demanded for the decryption of the files. Victims included hospitals in Great Britain.

NotPetya (2017) The NotPetya malware hit many computers worldwide in June 2017. Despite posing as ransomware, NotPetya did in fact have a destructive function. NotPetya affected the Danish shipping company A. P. Moller-Maersk, that has assessed the loss to between DKK 1,6 and 1,9 billion.

OPCW (2018) Dutch authorities caught Russian intelligence agents red-handed trying to access the Organization for Prohibition of Chemical Weapons (OPCW's) Wi-Fi network in 2018.

Demant (2019) The Danish manufacturer of among others hearing aid, Demant, became the target of a ransomware attack in 2019, resulting in the shutdown of systems across the company. The financial losses from the attack were estimated to be as high as DKK 650 million.

Georgia (2019) On 28 October 2019, Georgia was hit by a widespread cyber attacks that took three TV stations offline and cut off more than 2,000 websites.

Cyber security is becoming institutionalized

Over the past decade, cyber security has also evolved. As a result of the increased attention and regulation as well as of major cyber incidents such as the 2017 NotPetya and WannaCry attacks, cyber security has moved from the IT departments and into the boardrooms of Danish public authorities and private companies. As mentioned above, the COVID-19 pandemic has also enhanced the focus on cyber security due to the almost overnight changes in the use of digital services and systems.

In Denmark, the CFCS was established in 2012, and other countries, including Great Britain, Australia and Canada have later also set up national cyber centres as part of their intelligence services. Critical sectors and companies have set up functions to heighten cyber security such as Decentral Cyber and Information Security units (DCIS), Computer Emergency Response Teams (CERT) and Security Operations Centers (SOC).

International formation of norms and attempts at condemning and deterring cyber attacks, for instance by publicly attributing cyber attacks to certain actors and issuing subpoenas for foreign hackers show a willingness from more countries to counter the threat. This is not only reflected in the establishment of strong cyber defence measures, but also in the pressure exerted on the countries constituting a cyber threat.

Some countries are willing to go to even greater lengths to counter the threat. One of the most far-reaching examples so far being Israel’s bombing in 2019 of a building claimed by Israel to house Hamas hackers.

Despite this trend, cyber threat awareness is still not sufficiently broad. As a result, hackers continue to exploit well-known vulnerabilities and even simple cyber attacks may hold serious repercussions. Another ramification is that many cyber incidents continue to go undetected or unreported to relevant public authorities.

Under-reporting thus continue to be a challenge when assessing the cyber threat against Denmark.

The CFCS recommends that public authorities and private companies regularly consult guidelines on how to increase cyber security. For guides, threat assessments and investigation reports see the CFCS website.

Cyber security – a distant concept until emergency strikes

“We do quite basic and simple things. We help accountants. We saw ourselves as quite distant from cybersecurity issues.”

These words belong to Olesya Linnyk, head of the Linkos Group that was hacked and exploited to set off the as yet most extensive destructive cyber attack, the 2017 NotPetya attack. Hackers abused the Linkos Group’s software, M.E.doc, to transfer the NotPetya malware to Linkos Group clients, including Danish shipping company A.P. Moller-Maersk. The quote is from the book ’Sandworm’ by Andy Greenberg.

Cyber crime

The threat from cyber crime is **VERY HIGH**. As a result, it is highly likely that Danish private companies and public authorities will be the targets of attempted cyber crime within the next two years.

To the purposes of this assessment, the term cyber crime is used collectively to describe actions in which hackers use cyber attacks to commit crimes for financial gain.

Cyber crime constitutes a persistent and active threat to all Danish public authorities, private companies and citizens.

Cyber criminals most often carry out relatively simple attacks against multiple targets simultaneously, for instance through phishing attacks. However, networks also exist that have the capability to launch more complex and time-consuming cyber attacks, including targeted ransomware attacks.

Cyber attacks by criminal groups typically start without the actor having singled out a specific target. Most cyber attacks start off as attacks of opportunity. Attacks may include phishing emails being spread to thousands of victims, or IT systems and units with known vulnerabilities being abused by cyber criminals.

Cyber criminals also continuously exploit new vulnerabilities. When a new technical vulnerability emerges, it is often only a matter of a couple of weeks before it is exploited in hacking attempts against Danish targets.

The high frequency of attacks makes it vital for the IT departments of Danish public authorities and private companies to be timely in updating systems and software or in adopting mitigating measures in those instances when it is not possible to patch a vulnerability.

Citrix vulnerability left more than a thousand Danish units potentially vulnerable

An example of just how quickly and easily hackers are able to access thousands of servers played out in late 2019 and early 2020 following the public announcement of a vulnerability in Citrix equipment.

The affected Citrix units are used to control data traffic between the Internet and home workstations as well as communication between web servers and internal IT systems, etc. When the vulnerability was published, there were no security updates available to remedy the vulnerability. Citrix did, however, offer a guide on how to implement initial countermeasures.

Two weeks after the vulnerability became publicly known, the first descriptions of how to exploit the vulnerability started to be shared online, making it easy for hackers to use the descriptions as a formula for cyber attacks. The day after the guide was disseminated, an IT security company logged 290,000 attack attempts and scans from IP addresses in 42 countries against a single Citrix system.

In the days that followed, reports started circulating of how different hackers were fighting for access to the vulnerable systems. Some hackers even ousted the hackers that had been first to arrive, removing further attack possibilities as they wanted the system to themselves.

The hackers likely used public search engines such as Shodan to detect vulnerable Citrix units worldwide in their search for victims. At the time of the announcement of the vulnerability, a search in the Shodan database revealed more than a thousand potentially vulnerable units in Denmark.

CFCS knows of several Danish organizations that were the targeted during this period. CFCS has issued warnings to identified vulnerable public authorities and private companies, offering ongoing advice on countermeasures. Today, the number of vulnerable units in Denmark is less than a hundred.

The threat from targeted ransomware attacks is on the rise

There is a growing threat from targeted ransomware attacks against Danish public authorities and private companies.

In targeted ransomware attacks, criminals try to extort public authorities and private companies, demanding huge sums of money by using ransomware to encrypt key parts of the victim’s IT systems.

Since late 2019, hackers behind targeted ransomware attacks have occasionally also threatened to leak sensitive data from the affected systems if the victims did not pay the ransom.

A few Danish private companies have fallen victim to targeted ransomware attacks, and such attacks are now fairly common. In the autumn of 2019, Danish companies

Demant and GlobalConnect became targets of separate ransomware attacks. According to Demant's own estimates, the attack on the company resulted in losses running as high as DKK 650 million. In February 2020, the global service company ISS became the victim of a ransomware attack that also affected its Danish branch. In April 2020, the agricultural company Danish Agro and the pump solution company Desmi also fell victim to targeted ransomware attacks. In May 2020, GlobalConnect was compromised once again with the attack affecting systems belonging to many of its clients, including the pharmaceuticals procurement company Amgros.

Several countries have seen incidents in which targeted ransomware attacks have resulted in temporary shutdown of authority and company activities. Victims include local authorities, schools, manufacturers, hospitals, IT companies, ports and shipping companies.

Such targeted cyber attacks may have severe impact on critical functions as seen in connection with ransomware attacks against the healthcare sector in the United States and Great Britain, among others, where downtime in administrative systems resulted in the cancellation of appointments.

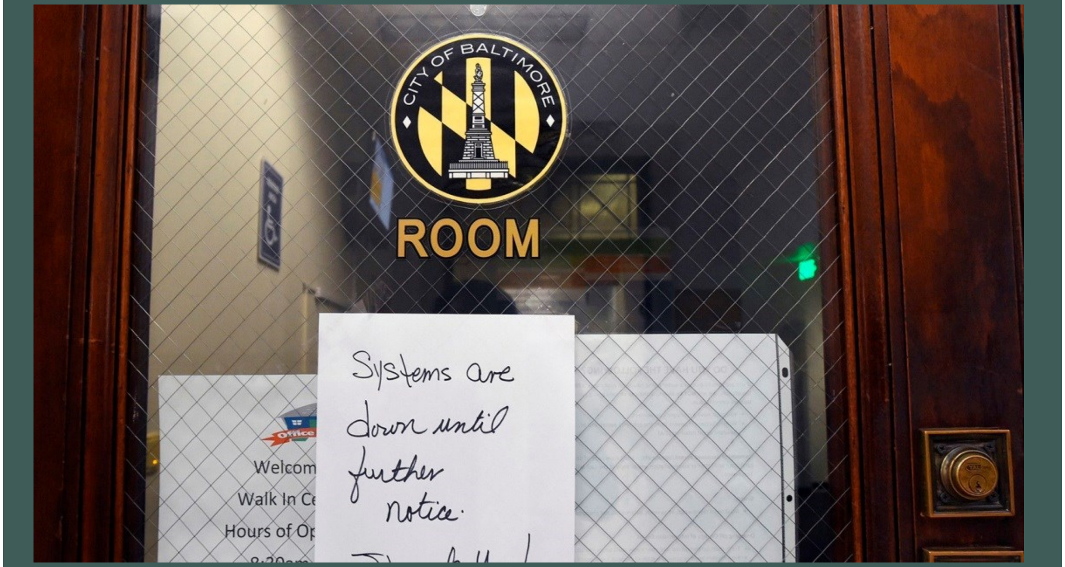
A successful ransomware attack against suppliers of critical services during a crisis, including against the Danish health sector during the COVID-19 pandemic, could add to the pressure that the sector is already under as a result of the crisis.

The attack against Amgros, which also supplies Danish hospital pharmacies, is among the ransomware attacks against the Danish health sector during the crisis. For a couple of days, the attack rendered Amgros unable to use its business system Naviline to buy and sell pharmaceuticals. The attack did not, however, cause a shortage in pharmaceuticals in the public hospitals.

Local authorities abroad have been attacked multiple times
Local authorities, in particular in the United States, have in recent years been frequent targets of targeted ransomware attacks, as have schools and school districts. As an example from august 2019 a targeted attack against an IT supplier paralyzed IT systems at 22 local authorities in Texas.

Some authorities have also been the targets of extortion in connection with ransomware attacks, where hackers have threatened to leak documents stolen from the affected systems. One such extortion was made against the city of Pensacola, where the extortionists at the end leaked data online in November 2019.

Attacks against local authorities have not been limited to the United States. The autumn of 2019 also saw a wave of attacks against local authorities in Spain.



The city of Baltimore in the United States became victim to ransomware in 2019.

Digital bank robberies have moved closer to Denmark

Targeted cyber attacks against financial institutions, so-called digital bank robberies, has moved into Europe in 2019, increasing the likelihood that Danish financial institutions may also become targets of such attacks.

In February 2019, the Maltese Bank of Valletta became victim of an digital bank robbery in which hackers tried to steal EUR 13 million. However, the bank subsequently succeeded in retrieving most of the money. During the same period, other European banks were the likely also targets of digital bank robberies.

CFCS is aware that hackers who likely hold sufficient capabilities for digital bank robberies specifically targeted Danish financial institutions in 2019, though without succeeding. Hackers have also sent phishing emails to banks outside Denmark, posing as staff from the Danish Financial Supervisory Authority. The hackers even used the names of real Authority staff.

The fact that it is common for financial institutions to receive inquiries from public authorities that require immediate response has likely motivated this type of abuse. This may increase the likelihood that whoever receives the phishing email reacts, for instance by clicking on links or opening files.

Simple attacks are a threat against everyone

Cyber criminals usually carry out relatively simple attacks against many potential victims simultaneously in the hope to reap from as many victims as possible. Such attacks are a continuous threat to Danish private companies, public authorities and citizens.

These attacks are often carried out as phishing attacks against thousands of recipients. However, alternative methods exist, including infection of websites as a way to spread malware to the sites visitors or in order to steal information entered by victims visiting the websites.

The distributed malware have different purposes that support financially motivated cyber crime. Trojans are for instance used for theft of personal and financial information. Crypto miners exploit the processing power and energy supply of infected computers to generate crypto currency. Ransomware holds data and systems on computers hostage by encrypting data and making them inaccessible to the victim.

The spread of malware through phishing is carried out by criminal groups and networks that cooperate and exchange services and capabilities, including malware and infrastructure.

Criminals sell network access used in targeted attacks

Cooperation takes place between criminals who launch more targeted attacks and criminals who target thousands of victims, for instance through phishing. Targeted ransomware attacks are for instance often opportunistic and launched following an initial compromise of the victim computer via malware distributed through phishing. Sharing and sale of such initial compromises are called ”access-as-a-service”.

Consequently, mass compromises through phishing are not only a threat in themselves; they also facilitate the increasing threat from targeted cyber attacks launched by criminals.

As the earning potential from, for instance, targeted ransomware attacks increases, so does the earning scope of the criminals who resell and facilitate network access to be used in the targeted attacks.

The broadened earning potential may be the reason that one of the most widespread types of malware globally, Emotet, has since 2017 not any longer been used by criminals to steal financial information as a direct source of gain. Emotet is now mainly used as a tool that other criminals can purchase access to.

State actors may also exploit the criminals' access and services to conduct, for instance, cyber espionage through purchase of access or extortion of domestic criminal networks. As an example, US authorities in 2019 officially accused Russian authorities of cooperating with cyber criminals.

In addition, several state actors use malware and techniques favoured by criminals. This may impede identification of cyber espionage incidents in the pool of the more frequent criminal cyber attacks.

US sanctions against network in Russia
In December 2019, US authorities, acting in coordination with British authorities, introduced economic sanctions against several named individuals and companies in Russia suspected of colluding with a cyber criminal network called Evil Corp.

The US authorities also accuse the Russian federal security service, FSB, of cooperating with the network for espionage purposes.

The premise of the sanctions is that the network is responsible for the spreading of the Dridex malware. Since 2012, Dridex, whose earlier versions were known as Bugat and Cridex, has been spread through massive spam campaigns, raking in yield equivalent of more than DKK half a billion. Dridex has also been used to spread ransomware.

Russian authorities have officially rejected the accusations as propaganda. However, US court documents show that Russian authorities have helped identify the leader of the network, Maksim Yakubets.

The allegations were presented at a press conference at the US Ministry of Justice.

Cyber espionage

The threat from cyber espionage is **VERY HIGH**, meaning that Danish public authorities and private companies will highly likely become targets of attempted cyber espionage over the next two years.

Denmark is the target of both politically and commercially motivated cyber espionage by foreign states.

The threat from cyber espionage is persistent. It is particularly directed at Danish public authorities involved in foreign and security policy, and Danish private companies whose knowledge is of interest to foreign states.

Suppliers and partners working with these public authorities and private companies may also become victims of attempted cyber espionage because the hackers will try to use them as entry points for access to the authorities' and companies' systems.

Cyber espionage may result in pressure on Danish decision-makers

The cyber espionage threat against public authorities generally reflects current foreign and security policy conditions.

In the words of the Danish Defence Intelligence Service in its 2019 Intelligence Risk Assessment: The world order that for decades has provided the overall framework for how we address Denmark's and Europe's geopolitical and security interests is being redefined. Among other things the dominant position of the United States in international politics is being challenged.

Cyber espionage is actively being used by several countries, including Russia and China, to broaden national options and to avoid strategic surprises in a volatile foreign policy environment. Several publicly known cyber attacks against European foreign ministries serve to emphasize that the threat is very present and that insight into foreign policy decisions and dispositions is a priority to several countries' cyber spies.

CFCS regularly register attempts at cyber espionage against Danish public authorities. The threat is focused on public authorities and individuals working in the field of security and foreign policy, including the Ministry of Foreign Affairs and the Danish Defence.

Denmark participates in international forums that have proved persistent objects of interest to foreign states in the context of cyber espionage. NATO, the EU and the OSCE have thus all been targets of attempted cyber espionage.

Foreign states likely try to use cyber espionage as a means to gain insight into Danish interests, deliberations and decisions on major international issues or foreign policy negotiations. The states may exploit this knowledge as leverage against Danish interests or to put Danish negotiators and decision-makers under pressure.

Russia and China in particular have access to substantial cyber capabilities, which both countries use actively on a global scale. It is likely that some countries, including Iran, also conduct cyber espionage and other types of cyber attacks against targets in their immediate vicinity and beyond.

Other states that hold cyber capabilities mainly use them in their immediate vicinity. Such states pose a potential cyber threat to Denmark as they may try to conduct cyber espionage against Danish diplomatic representations, partly in an attempt to gain access to information related to Danish security and foreign policy in the particular region, and partly to gain access to knowledge about the country or region in which the representation is located.

Attacks against several foreign ministries in Europe

Shortly after the turn of the new year, Austrian authorities announced that the country's foreign ministry had been hit by a severe cyber attack. The Austrian authorities do not exclude the possibility that the attack was orchestrated by a state actor.

A couple of months earlier, the Czech intelligence service, BIS, had accused Russia's federal security service, FSB, of being behind repeated compromise attempts against the Czech Foreign Ministry and Ministry of Defence in 2018. In addition, Czech authorities have stated that China was likely behind an extensive attack against a ”strategically important government institution” in 2018.

These examples are merely two in a long series of cyber attacks against European ministries of foreign affairs. Over the past few years, countries such as Italy, Croatia, Belgium and Germany have all claimed that their foreign ministries have been targets of cyber attacks.

CFCS has described in two investigation reports on how the Danish Ministry of Foreign Affairs became the target of compromise attempts in 2014 and 2015 respectively. The reports are available in Danish and can be found on the CFCS website.

Cyber espionage may jeopardize Danish competitiveness and economy

States also resort to cyber espionage to strengthen their own national development and competitiveness. This particular breed of cyber espionage specifically targets private companies and institutions whose niche knowledge is attractive to foreign states.

The states may use the stolen information to promote the development of their own national sectors, as it allows them to skip several steps in their innovation and development process. It is for instance likely that the development of the engine in the Chinese C919 airliner was based on targeted state-sponsored cyber espionage against foreign aircraft manufacturers and sub-suppliers in other countries.

Research related to the COVID-19 pandemic is also an example of knowledge that can be valuable to foreign states. Independently of the COVID-19 pandemic, the CFCS assesses that foreign states have an particular interest in the parts of the Danish healthcare sector that have access to research data or intellectual property. This includes companies, universities and hospitals involved in the development of biochemistry, biotechnology and pharmaceuticals.

Cyber espionage may thus damage the competitiveness of Danish private companies and, by extension, the Danish economy, in particular if the espionage targets businesses that hold a competitive edge.

The boundaries between commercially motivated and security policy motivated cyber espionage may overlap. There are several examples of cyber espionage against technologies that can be used dually, for both civilian and military purposes, for instance within aerospace. In 2019, NASA thus announced that they were compromised for 10 months from 2017 to 2018. According to NASA, the actors succeeded in stealing arms export controlled information.

Suppliers and partners are being used as launch pads

Foreign states may also try to target suppliers and partners to the above-mentioned types of public authorities and private companies, using them as entry points for access to the public authorities and private companies that are the ultimate targets.

Under this technique, hackers attack an organization to use it as an entry point to compromise specific clients and partners of that organization that are of interest to the foreign state.

Cyber espionage is thus not always used to harvest specific knowledge, but may also be used as a way to gain access to specific targets. Though some sub-suppliers or partners may not have knowledge of interest to foreign states, they may have access or credibility that can be exploited by hackers to compromise their intended targets.

IT suppliers, such as hosting and IT service providers, may have access to their clients' data or IT systems. Hackers may target these suppliers to access the clients' data or IT systems. Hackers may also exploit compromised software and equipment suppliers to spread malware used in cyber espionage to their clients, for instance through infected system updates.

Foreign states also compromise vulnerable IT systems broadly across society to build an IT infrastructure that can be used to launch cyber attacks against other targets. Even though they do not hold specific knowledge or accesses of interest to foreign states, Danish public authorities and private companies may thus become victims used as stepping-stones in cyber attacks by these states.

In 2015-2016, several Danish private companies and public authorities were systematically attacked as part of a campaign targeting vulnerable JBoss systems. The attacks hit a wide section of users with the only common denominator being their use of JBoss.

Cyber attack against Norwegian company Visma
In February 2019, Norwegian software company Visma reported that it had been compromised. According to open sources, the purpose was to gain access to Visma’s client data.

Visma is a large international supplier that delivers cloud-based business software solutions.

With branches in Denmark, Visma has delivered software solutions to the Danish Maritime Authority. We have no indications that the Danish Maritime Authority has been affected by the attack, but the incident illustrates how an attack on a supplier may pose a potential threat to other organizations.

Destructive cyber attacks

The CFCS assesses that the threat of destructive cyber attacks against Danish public authorities and private companies is **LOW**. This means that Danish private companies and public authorities 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.

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.

What is a destructive cyber attack?
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, ranging from data destruction to physical damage and death. 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. The CFCS assesses that the majority of known destructive cyber attacks have likely been state-sponsored. Nearly all of these attacks have been launched in connection with conflicts or geopolitical tensions between different countries. It is less likely that foreign states have the intention to attack Denmark.

However, 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, as was the case with the 2017 NotPetya attack in Ukraine, which hit the Danish shipping company A. P. Moller-Mærsk. 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 destruction 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.

States try to deter destructive cyber attacks

As a response to the 2017 NotPetya attack, NATO issued a joint statement that cyber attacks against any member country could lead to the invocation of the collective defence clause (Article 5) of NATO's founding treaty, the so-called musketeer clause.

So far, destructive cyber attacks have not triggered military responses. However, in May 2019, the Israeli Air Force launched an air strike against a building in Gaza that allegedly housed Hamas hackers. There are several examples of states reacting to destructive cyber attacks by introducing economic sanctions.

States may have different objectives of destructive cyber attacks

States may have different end results in mind when launching destructive cyber attacks. By launching a destructive cyber attack against critical sectors, a state may try to send a signal that the state under attack is unable to protect its population.

The aggressor state may also use the attacks to punish or deter other states from attacking its interests. Destructive cyber attacks against companies operating in a region fraught with geopolitical tensions may also be launched to dissuade foreign companies and investors from doing business in a specific country.

A destructive cyber attack that results in the destruction of critical infrastructure or military capacities may weaken potential adversaries in the event of a crisis or war. However, there are as yet no public examples of destructive cyber attacks having had consequences that far-reaching. The closest example is the 2010 attack on Iran's nuclear centrifuges, which is still the only known example of a destructive cyber attack causing large-scale physical damage.

In the decade that has passed since the attack on Iran's nuclear centrifuges, industrial systems and offensive cyber capabilities have developed immensely, suggesting that several countries now likely hold the capabilities required to launch a similar attack.

Few examples of destructive cyber attacks independent of conflicts

In a few cases, hackers have been known to launch simple destructive cyber attacks that have been unrelated to political and military conflicts.

There are a few examples of hackers deleting or encrypting financial companies' data in connection with digital bank robberies with the likely purpose of covering their tracks or preventing the companies from responding to the theft. Cyber crime may potentially also be accompanied by cyber attacks with a destructive effect. So far, deletion or encryption of data in connection with digital bank robberies is a relatively rare phenomenon, but it may nevertheless have serious consequences for the affected financial institution.

Errors may occur when hackers manipulate IT systems. Cyber attacks need not be destructive in scale to have a harmful effect, however unintentionally. Within the maritime sector, cyber attacks have affected ships’ power supply as well as their navigation and positioning systems. Though CFCS has no knowledge of any ensuing physical harm or accidents, it is possible that such attacks could have physical consequences.

Cyber activism

The threat from cyber activism is **LOW**, suggesting that the probability of Danish private companies and public authorities falling victim to cyber activism within the next two years is less likely.

On a global scale, 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 of cyber activism is most pronounced in connection with events or single issues that catch the attention of cyber activists.

Also, it is less likely that Denmark will become target of faketivism, which involves state-sponsored hackers launching cyber attacks while emulating cyber activists. The threat from faketivism would likely increase in connection with military or political conflicts with foreign states.

Football activist tackled Africa's richest woman
Since 2015, Portuguese hacker Rui Pinto has hacked and leaked information on the football world in what has become known as the Football Leaks campaign.

Open sources report that in 2018, when Pinto stole documents to support the Football Leaks campaign, he accidently came across confidential documents containing incriminating information on the richest woman in Africa, Isabel dos Santos.

Pinto gave the documents to an African whistle-blower organization, marking the start of the Luanda Leaks. The Luanda Leaks has made dos Santos the object of a criminal investigation in Angola, and Portugal has frozen her bank accounts in the country.

Though European football fields and Angolan government offices seem completely unrelated, there appears to be a common denominator between the two cases. Football Leaks and Luanda Leaks both contain accusations of corruption and abuse of power. The case illustrates how activist focus but also coincidence may both play a role in who becomes a target of cyber activism.

Rui Pinto was arrested in Hungary in 2019.

Events and coincidences may trigger cyber activism

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.

The most recent cyber activist attack in Denmark, which received a lot of media attention, was a DDoS attack launched in 2017 against the Danish Ministry of Immigration and Integration and the Danish Ministry of Foreign Affairs. The attack likely came in response to a debate on the Muhammad cartoons that had taken place shortly before the attack. The attack illustrates that the threat is dynamic with attacks launched by cyber activists often being spontaneous responses to specific events.

DDoS attacks are relatively easy to launch and thus typically presuppose only minimal planning and technical skills. The threat from such simple attacks may suddenly increase, should Danish public authorities or private companies land in the crosshairs of cyber activists, as was the case in 2017. In comparison, hacks and leaks of personal information, for instance, require longer planning and more advanced technical skills.

Cyber activism attacks cover a multitude of activities, ranging from attacks of opportunity to organized campaigns. However, a common denominator seems to be that while the attacks are often launched in response to specific events, there appears to be continuity in the topics pursued by the different activists.

States use cyber activism as a cover for influence

In some countries, cyber activism also accompanies traditional political activism. For instance, cyber activism attacks have accompanied the most recent wave of protests and civil unrest in South America and Catalonia. This type of activism is typically sparked by local conflicts and unrest.

Foreign states may have an interest in magnifying these local conflicts and unrest by launching cyber attacks disguised as cyber activism. This type of attack is popularly coined as faketivism.

Faketivism is typically an attempt at derailing or diverting public debate and cultivating societal polarization. It may prove difficult to attribute faketivism to specific countries, giving the states plausible deniability for influence campaigns in other countries.

It is less likely that Denmark will fall victim to faketivism. However, the threat may increase in cases involving political, strategic or economic issues which foreign states may have an interest in influencing. It is likely that the threat will rise should Denmark find itself engulfed in deepening political or military conflicts with other foreign states.

Hackers planted fake news in Lithuania
On 19 June 2019, fake news circulated on several Lithuanian online media claiming that NATO had accidently polluted a river in Lithuania with radioactive substances during the ”Iron Wolf” training exercise. However, it later turned out that the Internet pages had been compromised and the story planted by hackers.

A few months later, in October 2019, the pattern repeated itself. A Lithuanian online paper reported that the United States had plans to move nuclear arms to Lithuania, but, once again, the story turned out to be fake and planted by hackers.

In November 2019, the Lithuanian Armed Forces stated that they suspected the incidents to be part of a major Russian influence campaign aimed at sowing doubt as to NATO’s presence in the country.

In April 2020, a fake email posing as NATO’s secretary general was sent to a number of recipients, including Lithuanian media outlets, falsely claiming that NATO was planning to withdraw from the country.

Cyber terrorism

The threat from cyber terrorism is NONE, meaning that it is unlikely that Denmark, including Danish private companies and public authorities, will be exposed 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, 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.

So far, no terrorist groups have conducted cyber attacks against Danish or foreign targets that fall under the CFCS definition of cyber terrorism. Similarly, there have been no incidents in which terrorist groups have claimed responsibility for any cyber terrorism attacks.

Lack of capabilities accompanied by very limited intent

So far, there have only been a few examples of militant extremists calling for cyber terrorism attacks. Militant extremists have not claimed responsibility for any of the destructive cyber attacks that the world has seen so far. Even though terrorist groups do not always claim responsibility for their terrorist acts, the CFCS assesses that a successful serious cyber attack would have been followed up by propaganda to emphasize the new threat.

The absence of intent is likely rooted in the fact that the established terrorist groups do not consider cyber attacks a realistic and effective way to create the same kind of fear and chaos that a conventional terrorist attack would cause.

Militant extremists behind cyber activism

Cyber attacks launched by militant extremist groups have primarily manifested themselves as cyber activism as evidenced by the calls for cyber attacks and the cyber attack instructions posted by militant extremists. Attacks and ambitions for attacks have typically revolved around website defacement and DDoS attacks as well as hacks and leaks of personal information accompanied by calls for killings in the form of so-called kill lists.

The hackers behind such cyber attacks have typically shown support for Islamic State. In 2016, four hacker groups joined forces, forming the United Cyber Caliphate (UCC), likely to strengthen their capacity. As a result of the military pressure on Islamic State, the hacker groups have not been able to establish themselves as a physical group, but have been forced to operate as a loosely affiliated group of individuals.

Radicalization and recruitment may heighten the threat

The threat from cyber terrorism may increase should militant extremists succeed in radicalizing and recruiting resourceful hackers or insiders with access to critical IT systems. There have been examples abroad where insiders have offered their IT expertise to militant extremists.

In the medium term, the increased fusion between the physical and digital domain may entail an increasing risk of damage to property or people, potentially increasing the threat from cyber terrorism as well.

The absence of cyber terrorism attacks does not mean that the Internet has no impact on the terrorist threat. Militant extremists have been known to use encrypted chat services and closed Internet forums to recruit and radicalize new extremists across borders, sharing calls and manuals for conventional terrorist attacks on closed forums as well as advice on how mobile phone and Internet communication can be concealed from the authorities.

Artificial intelligence and quantum computing are changing cyber security

Over the past few years, a number of technological breakthroughs have provided an abundance of digital opportunities. In-home digital personal assistants are becoming increasingly popular, facial recognition can be used for authentication, and self-driving cars are already being tested in many big cities.

However, fast progress brings new challenges that will shape the digital security landscape in the years to come. Breakthroughs, in particular within artificial intelligence and quantum computing, have brought new opportunities and challenges.

Artificial intelligence: defence and attack automation

The development within artificial intelligence has improved detection of cyber attacks. Today, machine learning algorithms form the core business of many private cyber security companies' IT solutions. Several companies even offer active monitoring of network traffic that regularly trains algorithms to identify and stop malicious activity in real time. Progress has especially been made within the identification of phishing emails. Today, most phishing emails are detected and automatically filtered out by machine learning algorithms.

Artificial intelligence
Technologies that mimic human intelligence, including language, eyesight, learning and the ability to generalize.

Machine Learning
IT systems that process new data based on machine analysis of previous data sets (learning) rather than through explicit programming (instructions).

On the other hand, artificial intelligence has also created several challenges. For example, hackers have started exploiting the same algorithms to automatically generate far more credible phishing emails to trick these advanced machine learning algorithms. To this end, the algorithms are increasingly actively incorporating information about their targets from social media in a bid to appear more credible.

Artificial intelligence also provides new opportunities to launch increasingly targeted hacker attacks. During the 2018 Black Hat IT security conference, IBM demonstrated how it is possible to embed machine learning algorithms in malware that will only activate when the target is identified through indicators such as facial and voice recognition. This opens up for the possibility of launching targeted cyber attacks against singled-out individuals or groups. In other words, artificial intelligence has made it possible to exploit our biometric data against ourselves. As artificial intelligence is becoming increasingly integrated in modern life, including in critical infrastructure systems, it is vital that cyber security is incorporated into the development and application phases.

Cyber security following the quantum leap

The development of quantum computing will also affect cyber security in the years to come. Researchers and companies are trying to transfer quantum physics to the digital realm, including to develop universal quantum computers and quantum-secure communication channels.

Quantum computers use so-called ”qubits” that are capable of performing calculations that exceed the limitations of conventional computers. In fact, each additional qubit doubles the processing power of a quantum computer. In other words, the processing power of a quantum computer expands at a double exponential rate, while that of conventional computers only expands exponentially. This is a very big difference, whose future impact will likely be significant.

The development of quantum computers poses a potential threat to the cyber security in Denmark as the increased processing power of quantum computers may be exploited in cyber attacks. The development of quantum computers challenges online data security, in particular. At the moment, Internet communication is encrypted using very complex calculations that protect our data in a way that would take a conventional computer thousands of years to crack. In the future, quantum computers may be able to break encryption systems in a matter of seconds, and encrypted information sent over the Internet today could potentially become readable again.

One of the most widespread encryption techniques today is called RSA. According to the US National Institute of Standards and Technology (NIST), quantum computers will likely be able to break RSA encryption in ten years’ time. Consequently, in 2017, NIST launched an international competition for the development of a new encryption technique to replace RSA. The challenge now lies in choosing a replacement and implementing it before quantum computers become able to break RSA encryption.

Even though the technology is still in its infancy, the first two quantum computer prototypes have already started delivering results. For example, in 2019, Google built a quantum computer that was able to solve a mathematical problem in three minutes that would take a conventional computer approx. 10,000 years to solve. There are still significant challenges connected to quantum computers, but some compare Google’s breakthrough to the Wright brothers’ first plane flight, which, despite its limited performance, opened the door to a new future.

However, the development of quantum-secure communication presents a potential solution to some of these challenges. The idea behind quantum-secure communication is based on the sharing of ’keys’ which are already used legitimately to decode messages in a new and secure way based on quantum physics. What is special is that the exchange of key happens in a way in which data security is no longer dependent on limited processing power and that sender and recipient will always be able to detect any attempts at interception of the key exchange during the transmission.

At present, the development of quantum-secure communication is ahead of the development of quantum computers. For example, China has on a trial basis opened a 2,000 km long fibre-optic quantum communication line connecting the cities of Beijing, Jinan, Hefei and Shanghai. In 2016, China launched the "Micius" satellite designed to facilitate quantum communication across national borders.

Large-scale implementation of quantum communication online would require a massive restructuring of the current Internet structure.

Employee inspecting IBM's quantum computer 'Q'.

Commercial interests are drivers for development

The development of artificial intelligence and quantum technology in the Western world is primarily driven by large tech companies in the private sector.

For these companies, the technologies support significant commercial interests, such as first-mover advantages in the development of self-driving cars, development of digital assistants, and additional optimization of machine learning algorithms.

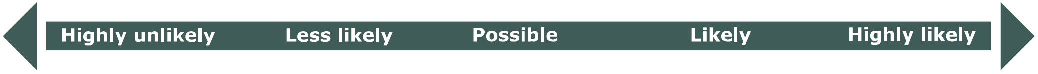
There is a risk that commercial interests will be allowed to eclipse the need to address the security challenges of the future outlined in this assessment.

Definition of threat levels

The Danish Defence Intelligence Service 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



Highly unlikely **Less likely** **Possible** **Likely** **Highly likely**

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

References

Center for Cybersikkerhed and Digitaliseringsstyrelsen (2016): *Cyberforsvar der virker*

Centre for Cyber Security (2020): *Password Security*