CENTRE FOR CYBER SECURITY

Threat assessment

The cyber threat against Denmark 2021

1st edition June 2021

Table of contents

CENTRE FOR CYBER SECURITY

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

1st edition June 2021

The cyber threat against Denmark 2021

The purpose of this threat assessment is to inform Danish decision-makers, public authorities and private companies of the cyber threat against Denmark. It is vital that organizations actively pursue initiatives to address the cyber threat in order to counter it. Knowledge of the threat will help the individual public authorities and private companies to prioritize cyber security measures.

Key Assessment

- The threat from cyber crime is **VERY HIGH**. Cyber crime poses a real and persistent threat to all Danish public authorities, private companies and citizens. The ability of cyber criminals to develop and adapt their tactics to new realities and the specialized cooperation that takes place on closed Internet forums increases the threat.

- The threat from cyber espionage is **VERY HIGH**. Centre for Cyber Security (CFCS) assesses that foreign states can and will try to steal valuable information from Denmark. Time after time, specific incidents and attack attempts have given credence to this assessment.

- CFCS assesses that the threat from destructive cyber attacks against Danish public authorities and private companies is **LOW**. Though several foreign states have the capabilities to launch destructive cyber attacks, they are currently less likely intent on conducting destructive cyber attacks against Danish targets.

- The threat from cyber activism is **LOW**. The numerous protests seen in 2020 have not been reflected in more cyber activism attacks worldwide. The number of attacks has thus remained at the same level as in previous years.

- The threat from cyber terrorism is **NONE**. Serious cyber attacks aimed at creating effects similar to those of conventional terrorism presuppose technical skills and organizational resources that militant extremists do not possess at this point. At the same time, their intent to conduct cyber terrorism is limited.

Introduction

Centre for Cyber Security (CFCS) under the Danish Defence Intelligence Service is releasing its sixth annual assessment of the cyber threat against Denmark. Like in previous years, the assessment is divided into sections addressing different types of cyber threats, including cyber crime, cyber espionage, destructive cyber attacks, cyber activism, and cyber terrorism. The analysis has not prompted CFCS to adjust its threat levels compared to the 2020 levels.

Consequently, CFCS assesses that the threat levels from cyber crime and cyber espionage remain **VERY HIGH**. When a threat level is **VERY HIGH**, it indicates that actors are able, willing and continuously trying to attack Denmark. Both cyber criminals and states systematically and persistently target victims in Denmark

Even if a threat level has not changed, the threat may be reflected differently from year to year, suggesting that knowing the threat level is not enough to understanding the threat.

Theat levels are designed to provide a broad overview of different threats and may be indicative of which threat requires the most attention. At the same time, threat levels may provide an indication of how a threat may evolve over time. But if a private company, public authority or organization is to build an effective cyber defence, they need to see beyond the threat level alone and adopt a nuanced approach that reflects the nature of the different threats.

Even though a threat level has not changed, threat actors, techniques and the extent of consequences may have.

This year's chapter on cyber crime provides a good example of the relationship between threat level and threat. Like in previous years, the threat level for cyber crime is placed at the highest level possible due to, among other things, the targeted ransomware attacks that have affected Danish companies in recent years. In order to step up pressure on their victims, several hacker groups started threatening to leak data that was stolen in connection with ransowmare attacks. IT security vernacular refers to this extortion technique as double extortion.

The double extortion tactic has increased the potential consequences of targeted ransomware attacks. The victims not only risk losing access to vital IT systems, they also risk stolen sensitive information being leaked or sold to the highest bidder. Double extortion per se does not trigger changes to the threat level, but the phenomenon adds a new dimension to the cyber crime threat. Consequently, it is crucial that private companies, public authoritities and organizations familiarize themselves with the different aspects of the threat in order to effectively protect themselves against the threat.

The cyber threat remains a significant risk

The threat levels for cyber crime and cyber espionage have been set at "very high" since CFCS released its first assessment of the cyber threat against Denmark in 2016, and there are no indications that the cyber threat will move down the threat ladder in the years to come.

Several circumstances facilitate hacking. All IT systems contain vulnerabilities that can be identified and exploited by hackers through the plethora of information and tools

available online. Uptime and functionality often take precedence over IT security. Finally, the human factor constitutes a vulnerability that cyber criminals can exploit in connection with phishing emails.

Hackers generally run a low risk of being caught as it is easy to remain under the radar and maintain anonymity online. Attempts at catching perpetrators behind cyber offences often transcend borders, hampering detection and prosecution.

The free and open Internet often provides hackers with easy access to their victims. Telecom providers have a legal obligation to deliver all traffic that does not pose a threat to the tele-infrastructure, including cyber attacks, to their customers and ensure free access to all Internet services – including hacker infrastructure and websites.

As long as easy-to-hack devices exist that offer high rewards at low risk, there are no indications that the general cyber threat will diminish in the next few years.

Fighting hackers is not a losing battle

Most hacker attacks are averted thanks to advanced technology as well as informed and vigilant companies and citizens. However, just as many people do not install home security systems until after they have been robbed, many hacker attacks succeed due to cyber security negligence. In the same way that door locks, security cameras and vigilance may deter burglars, basic cyber security measures and well-trained diligent employees may help prevent or mitigate most hacker attacks.

Thus, hackers have far from won the battle for the digital domain. As cyber security becomes a central priority to organizations, private companies and public authorities, cyber resilience will improve, reducing the risk of serious cyber attacks.

A detailed and nuanced understanding of the cyber threats facing Denmark will promote cyber resilience.

Enjoy your reading!

Cyber crime

The threat from cyber crime is **VERY HIGH**, meaning that Danish public authorities, private companies and citizens are highly likely to become targets of attempted cyber crime within the next two years.

In this assessment, the term cyber crime is used to collectively 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. The ability of cyber criminals to develop and adapt their tactics to new realities and the specialized cooperation that takes place among cyber criminals serve to stress the significance of the threat.

Cyber crime poses a wide range of threats to Danish society
CFCS assesses cyber crime to be the most widespread cyber threat against Denmark now and in the long term.

The most common type of cyber crime activities continues to be broad attacks, including phishing, exploitation of known vulnerabilities in popular IT systems and exploitation of weak remote access systems, against a large number of potential victims across the Danish society. As a result, most Danes can expect to be targets of attempted cyber crime.

Criminals use tools and attack techniques typically developed for specific criminal purposes, such as theft of personal information, extortion through ransomware or exploitation of IT systems for cryptocurrency mining. The diversity of the attacks indicates that cyber crime involves a range of illicit enrichment crimes, including theft, extortion and fraud.

Cyber criminals are resilient and adaptable
Cyber crime is motivated by the prospect of financial gain. Consequently, many cyber criminals adapt quickly when profit opportunities arise, when new tools are developed, or when external circumstances change their business landscape so to speak. As a result, the threat from cyber crime evolves continuously, continuously adding new elements to the cyber threat landscape.

Since 2019, several cyber criminal groups have focused on executing or supporting targeted ransomware attacks. As mentioned in the introduction, in 2020 these hacker groups started extending the scope of their extortion activities by threatening to leak sensitive information harvested in connection with ransomware attacks.

Selected events cyber crime 2020

February
Australian transportation company Toll Group reveals that it has suffered a ransomware attack.

The global service company ISS became the victim of a ransomware attack that also affected its Danish branch.

April
Danish pump manufacturer DESMI revealed that it was a victim of a targeted ransomware attack.

The danish agricultural company Danish Agro falls victim to a targeted ransomware attack.

May
GlobalConnect was compromised once again with the attack affecting systems belonging to many of its clients, including the pharmaceuticals procurement company Amgros.

Entertainment and media law firm Grubman Shire Meiselas & Sacks fell victim to a ransomware attack. The attackers initially demanded a $21 million ransom, which later rose to $42 million when the attackers threatened to leak stolen data.

Australian transportation company Toll Group reveals that it has suffered a ransomware attack for the second time in 2020.

July
Garmin hit by a ransomware attack with the malware WastedLocker. The initial ransom demand was for $10 million. Garmin reportedly payed the ransom.

August
Argentina's immigration agency, Dirección Nacional de Migraciones (DNM), suspended operations for over four hours after its systems were attacked by NetWalker ransomware

September
The hackers behind the leak site "Happy Blog" claims to have hit the Nordic eyewear chain Synsam Group, which includes Danish Profil Optik.

The US company Universal Health Systems was hit by a ransomware attack that affected access to IT systems at 400 clinics and hospitals in the United States.

November
The Ritzau news agency reports that they have been hit by a hacker attack.

Some of the leading hacker groups even suspended their activities for extended periods of time in the spring of 2020 to develop and test new tools for such attacks.

Ransomware attacks
Ransomware attacks render data and systems inaccessible to the victim, often through encryption, holding them hostage for ransom, typically in the form of cryptocurrency.

Targeted ransomware attacks are a subgroup of ransomware attacks in which hackers take their time to patiently and carefully encrypt large sections of their victims' IT infrastructure in one procedure. The victims are subsequently extorted for hefty ransoms.

In 2020, hackers who had previously mainly focused on theft of financial information from, for instance, the hospitality industry turned their focus to new targets and attack techniques. This shift in focus was likely prompted by the COVID-19-induced collapse in this industry's revenue, making it a less appealing target for hackers. One such group is the Carbanak hacker group that started launching targeted ransomware attacks. Notoriously known for targeting payment systems in the hospitality industry and the retailing sector with the purpose of stealing credit card information, the group was forced into exploring new avenues of crime due to the outbreak of COVID-19.

Cyber crime is an industry
The cooperation that exists between cyber criminals was one of the factors facilitating Carbanak's quick redirection of activities to targeted ransomware attacks. The cooperation, specifically the exchange of services among criminal hackers on market-like conditions, is known as Crime-as-a-Service (CaaS). This cooperation increases the specialization and effectiveness in the cyber-criminal community, creating robust and organized supply chains, whose activities include facilitation of targeted ransomware attacks.

State-sponsored hackers also engaged in cyber crime
Some countries use cyber crime to promote their own strategic interests. An example in point is North Korea's use of digital bank robberies, cyber attacks against crypto stock exchanges, and distribution of cryptocurrency-stealing malware to steal assets worth billions of Danish kroner. Some of the money from these illegal activities has been used to facilitate North Korea's nuclear programme.

Within the past year alone, North Korean groups have launched attacks against organizations dealing in cryptocurrency in more than 30 countries.

The exchange of tools and services takes place in closed Internet forums and through established personal collaboration relationships. Here, cyber criminals sell and exchange a variety of tools, including malware, access to compromised victims, etc. Thus, CaaS enables hackers to procure the services and accesses they need to launch cyber attacks, saving them the trouble of developing such tools themselves. This approach helps create value chains between criminal hackers, enabling them in their cyber criminal activities.

Today, several criminal hacker groups and networks are teaming up to launch targeted ransomware attacks, which can be a most profitable business. In the cases where the cooperation takes in a more organized form, the hackers will often specialize in specific parts of the attack or provide defined services against a share of the total profit.

Some groups even organize their ransomware attacks as a complete platform economy enterprise that is comparable to commercial solutions such as Airbnb with the operators of certain ransomware tools providing infrastructure and access to the victims to a network of other hackers who get a share of the profit against launching the actual attack.

REvil uses network of affiliates
The network behind the REvil ransomware, also known as Sodinokibi, uses platform economy as a business model with the network operators overseeing the development and maintenance of the ransomware while using a network of affiliates to launch the attacks on its behalf. The operators recruit the hackers on Russian hacker forums, etc. The operators use ID numbers to trace affiliated hackers, who are automatically awarded their share of whatever profit the attacks yield.

In addition to launching targeted ransomware attacks, REvil also threatens to release stolen victim data by auctioning it off on its website "Happy Blog" if ransom demands are not met. The network attacks public authorities and private companies indiscriminately across borders. Denmark has not escaped such attacks, and in 2020 the network threatened to leak data stolen from the Nordic eyewear franchise Synsam, which also includes the Danish company ProfilOptik.

The consequences of cyber criminal attacks are mounting
The phenomenon of hackers teaming up to launch targeted ransomware attacks is a global trend that proves just how agile cyber criminals are at tapping into new sources of income. Since 2019, targeted ransomware attacks have become part of the cyber threat landscape in Denmark, with Danish organizations and public authorities regularly falling victim to this kind of cyber criminal activity.

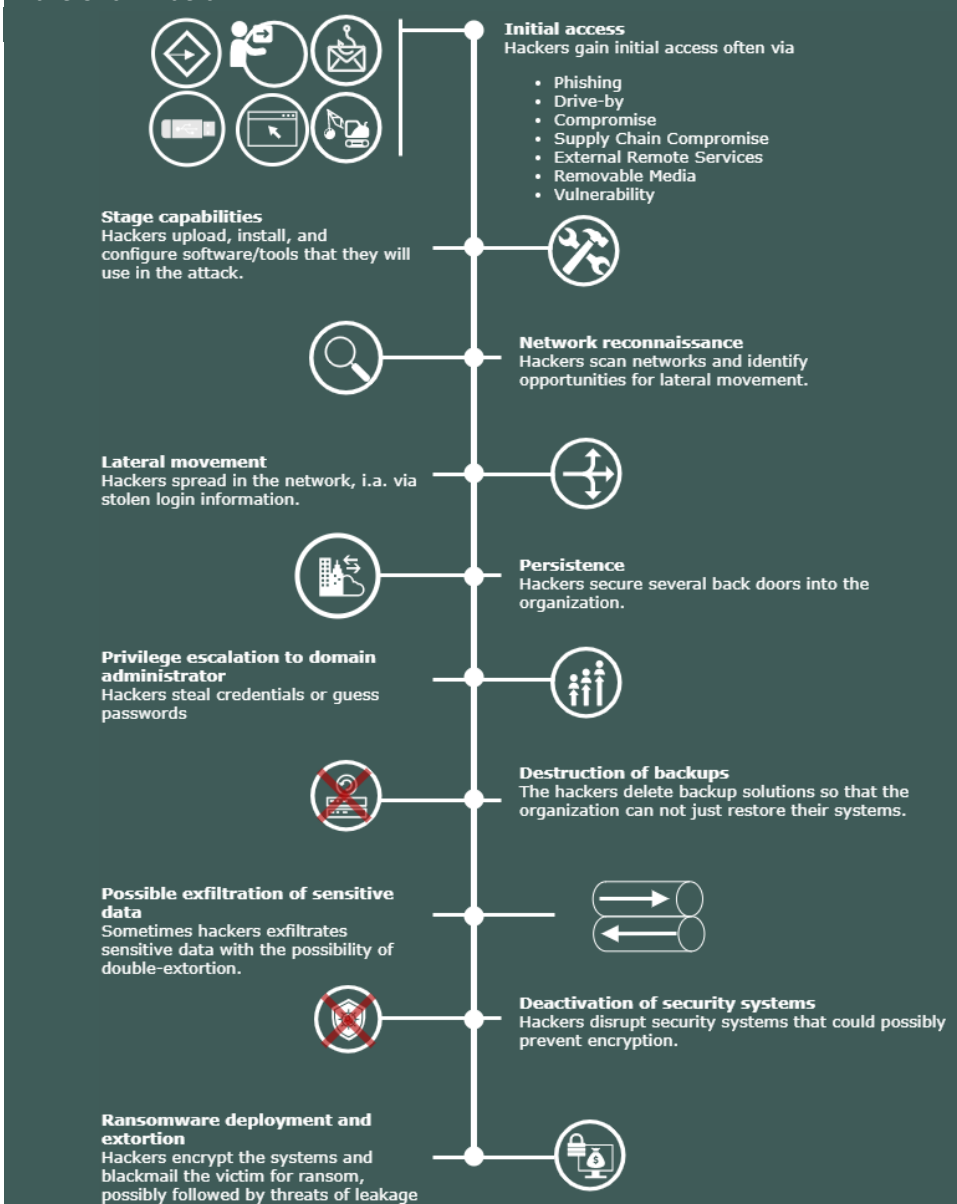
In 2020, the potential impact of targeted ransomware attacks grew increasingly serious as cyber criminals chose to tighten the digital thumb screw in several areas. By way of example, the phenomenon of double extortion now means that the victims not only lose access to critical IT systems, they also face the risk of having their business or sensitive information leaked to the public or sold to other cyber criminals.

It has become standard practice for many cyber criminal groups to leak stolen information if the ransom demand is not paid. Several Danish victims have had their data leaked in connection with targeted ransomware attacks or through compromise of cooperation partners.

Cyber criminals also try their luck with other types of extortion. In 2020, CFCS observed a wave of so-called Ransom Denial of Service (RDoS) attacks in Denmark in which cyber criminals threaten to launch a Distributed Denial of Service (DDoS) attack if their victims fail to pay the ransom demand. However, sometimes such threats are idle, as not all criminal actors have the capabilities required to realize their threats.

Ransomware attacks are preventable

As a rule, targeted ransomware attacks are not easy to launch, and hackers must have extensive control over their victim's IT systems before encryption is possible. A targeted ransomware attack may thus infect an organization's IT systems and lie in wait for days, weeks or even months before deploying and encryption occurs. During this period, the victim may have time to react and avert attacks if they know which warning signs to look for. The phases of a typical targeted ransomware attack are shown below:



Danish hackers also conduct cyber crime

CFCS assesses that the threat from cyber crime mainly emanates from foreign organized hacker groups and networks that launch attacks on a massive scale against victims worldwide. However, Denmark also has its share of cyber criminals.

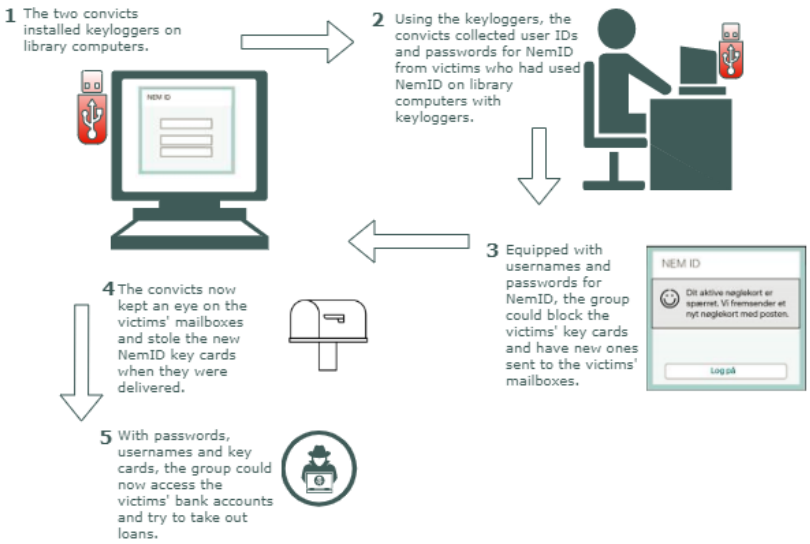
In December 2020, the Danish Eastern High Court sentenced a 38-year-old man to three years in prison, confiscating approx. DKK 22.4 million obtained through hacking and fraud in connection with online poker games. The man was found guilty of having installed malware on his victims' computers, allowing him to view their screens and read their hands while competing against them in an online poker game.

Unlike their foreign-based peers, Danish cyber criminals can exploit their physical access to potential victims and their knowledge of the Danish language and national IT solutions such as NemID.

Keyloggers

Keyloggers log keystrokes on keyboards, making it possible to steal personal information from the users, including keyed-in credit card information, usernames and passwords to, for instance, NemID – Denmark's common secure logon solution – mail accounts or social media.

In 2020, the Danish Police thus arrested 11 Danes in a case of serious data fraud involving NemID. The individuals indicted are charged with having installed keyloggers on publicly accessible library computers with a view to illicit financial enrichment. So far, two have been sentenced to two and a half and three years in prison respectively, while nine still await sentencing. The case is part of a larger case in which two of the indicted have prior convictions for similar crimes and for planning acts of terrorism. The fraud case, which dates back to 2016-2017, progressed as follows (above illustration):



CFCS cooperates with other public authorities and private companies to shut down websites that are identified as being designed to mimic websites belonging to Danish public authorities and whose aims include stealing NemID usernames and passwords or payment details. In 2020, CFCS identified some 500 websites which, operating from a host of methods, tried to rob Danish citizens of their personal information. The majority of these sites have subsequently been blocked by the Danish Police or taken down by the hosting providers, most of whom are not based in Denmark.

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 within the next two years.

Cyber espionage is a persistent threat. For the past six years, CFCS has assessed the threat from cyber espionage against Denmark to be at the highest possible level on the scale. Foreign states continuously attempt to steal valuable information from Denmark. Incidents and attempted attacks continuously serve to substantiate this assessment.

In 2020, several attacks worldwide came into the public spotlight when authorities and companies, in an attempt to protect others against similar attacks, publicly described and condemned attacks that had been launched against them.

States steal knowledge to promote national interests

The motives of foreign states for conducting espionage can be divided into two main categories. States conduct espionage to obtain information that is relevant in a security policy context, from overall strategic knowledge to knowledge specifically related to military planning. States also conduct cyber espionage in order to promote their own industries and economy.

The threat from cyber espionage is thus mostly directed against Danish public authorities and organizations that are engaged in foreign and security policy matters. Using cyber espionage, foreign states can obtain knowledge of Danish interests, considerations and decisions in connection with major international issues or foreign policy negotiations. This type of knowledge will allow the perpetrating state to counter Danish interests or to put Danish negotiators and decision-makers under pressure.

Furthermore, the threat is directed at companies that hold knowledge of interest to foreign states, including commercial business secrets such as information about contracts, tenders, new technology, research or other types of intellectual property. When Danish companies are exposed to cyber espionage, this may harm Denmark's competitiveness and Danish economy.

In some cases, targets of cyber espionage may also include companies that have access to information that could prove valuable for foreign states in the future, including in connection with military conflicts where private companies play a role in maintaining security of supply and in supporting the military. In other words, foreign states may use

cyber espionage against companies to build a capacity to launch destructive cyber attacks against the companies concerned in connection with critical conflicts.

COVID-19 still high on the 2021 global agenda

Research related to COVID-19 is an example of knowledge that may be valuable to foreign states and which may thus be an attractive cyber espionage target.

Over the past year, several cyber attacks have been directed against organizations involved in the efforts against COVID-19. A case in point is the claim by South Korean national intelligence service NIS that North Korean hackers had tried to hack into databases belonging to pharmaceutical conglomerate Pfizer. According to NIS, the purpose of the hacking attempt was to steal COVID-19 vaccine data.

Several countries, including the United States, Canada and Great Britain have on several occasions accused foreign states of conducting cyber espionage against COVID-19 research.

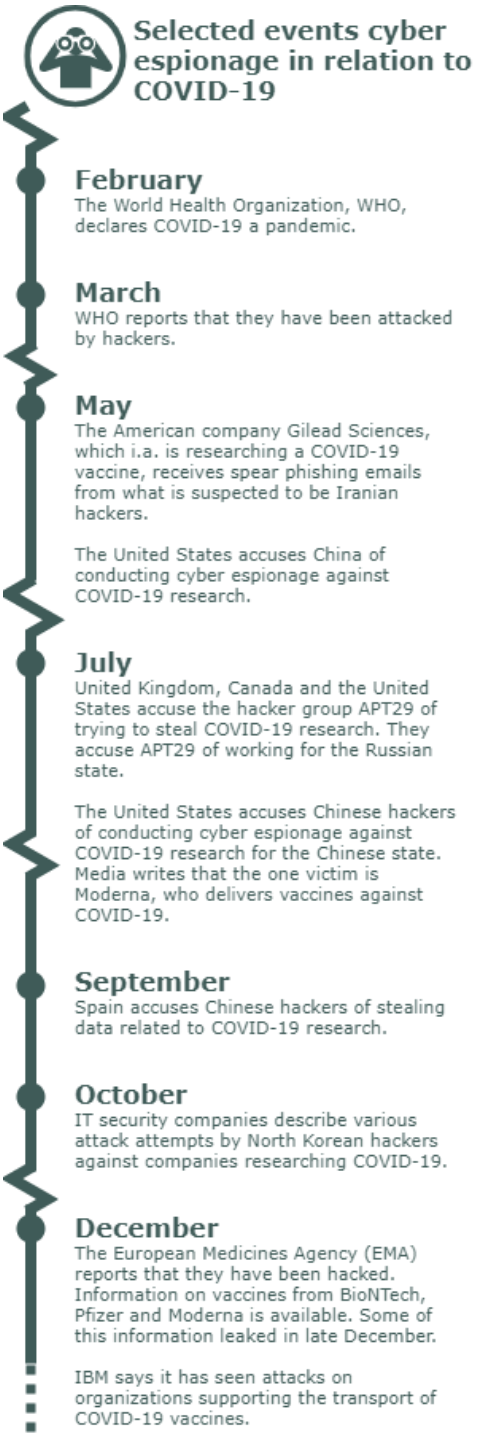
States pursue all avenues to get access

Once the actors behind cyber espionage have picked out a target, they are very persistent in their attempts at penetrating the victim's systems. If they fail to establish direct access, they look for alternative ways into the systems.

Suppliers are thus used as entry points for attacks in so-called supply-chain attacks. By compromising suppliers, hackers can access targets that are otherwise strongly protected, just as they can access multiple targets in one go. Suppliers with a legitimate and privileged access to their clients' IT systems, including software providers or IT service providers, are particularly attractive targets for hackers. Hackers prey on the fact that it can be difficult to detect and counter attacks launched through suppliers.

The SolarWinds hack was a serious threat

In December 2020, the FireEye security company discovered one of the most extensive publicly known cyber espionage attacks ever conducted. Organizations worldwide, including in Denmark, had been compromised via the Orion software provided by the SolarWinds software company. Notable companies like Microsoft and Deloitte fell victim to the attack. Companies such as Microsoft act as suppliers themselves to companies worldwide, and access to supplier companies could potentially allow hackers to tunnel deeper into the systems of their clients in a double supply chain attack.



CFCS assesses the compromise through the SolarWinds software to constitute a very serious threat. Espionage was the likely motive behind the compromise.

According to open sources, the attack was conducted by hackers who compromised SolarWinds. In March 2020, the hackers added malicious code to legitimate SolarWinds Orion software updates. According to SolarWinds, nearly 18,000 clients worldwide downloaded the compromised updates. The malicious code gave the hackers initial access to the victims' systems, which they could then further exploit. CFCS assesses that the actor exclusively used the accesses against the most interesting victims.

CFCS knows of more than 50 organizations in Denmark that have used the compromised version of the Orion software, thus installing a backdoor into their networks. CFCS is still looking into whether the backdoors have been used to further compromise the victims in order to steal data.

Private email accounts belonging to staff are alternative attack entry points that states can abuse to access employer networks. Many employees use the same computer or mobile phone for both private and work-related activities, and some even recycle passwords, using the same password to both private and job-related accounts. Hackers have been quick to exploit this practice. Also, the fact that many have worked from home during the COVID-19 pandemic has blurred the lines between people's private and professional digital lives. As a result, the digital front line has moved into people's private spaces, a trend that will be dealt with in more detail in the chapter on trends and tendencies.

States are usually very patient in their cyber espionage activities. Having entered a system, a state-sponsored hacker group will usually conduct its espionage clandestinely long before launching more risky activities that will potentially set off alarms in the victims' systems. It can thus be hard to detect state-sponsored hacker groups.

APT28 – the hacker group that does not always fly under the radar

APT28, one of the most notorious hacker groups, became widely known after US authorities charged it with hacking the Democratic National Committee (DNC) in 2016. APT28 was charged with leaking information stolen from the DNC with the purpose of influencing the 2016 US presidential election. According to US authorities, APT28 is affiliated with the Russian military intelligence service GRU.

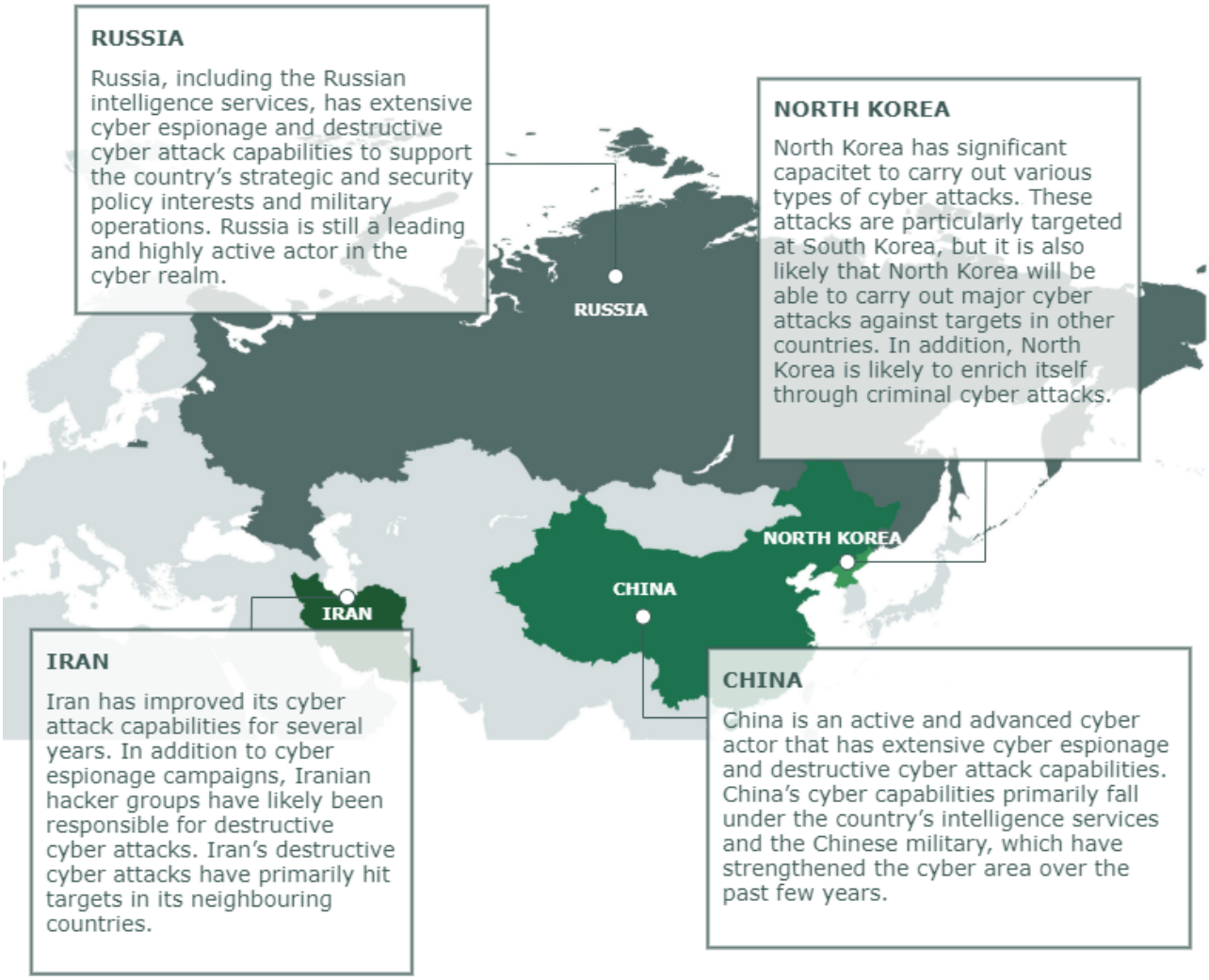
New cyber attacks are continuously attributed to APT28. In December 2020, the Norwegian security service PST informed that APT28 was the likely perpetrator behind a cyber attack against the Norwegian parliament.

The charges state that though APT28 has major resources, it also avails itself of relatively simple attack methods, including spear phishing emails and brute force attacks.

APT28 is also known under alternative names such as Fancy Bear, Sofacy and Pawn Storm.

The above illustrates just how focused and persistent foreign states can be in their attempts at accessing systems belonging to targets of interest. Occasionally, foreign states also use private individuals to physically facilitate cyber espionage, in which case the cyber threat also poses a serious concern even to systems that are segmented from the Internet.

THE CYBER CAPABILITIES OF SELECTED STATES



Some state-sponsored cyber attacks are also opportunistic with hackers running scans to find vulnerable systems and identify possible entry points. One motive is to build up an infrastructure that can be used as a stepping-stone for attacks against other targets while seizing on any opportunities to steal interesting information along the way. CFCS knows of several examples of state-sponsored cyber attacks where the list of victims suggests that most of them were attacked exclusively because network vulnerabilities were detected, not because they were a prioritized target per se.

APT41 – the hacker group that also feathers its own nest

In September 2020, the US Department of Justice charged five members of the APT41 hacker group with having orchestrated years of extensive cyber espionage against US and foreign companies and organizations. Open sources also link the group to extensive cyber espionage – including against several large German pharmaceutical companies. Having mainly availed itself of different publicly available hacker tools, the group has used spear phishing, exploited known vulnerabilities and used supply chain attacks to gain initial network access.

The US indictment cites that links exist between APT41 and the Chinese state. However, the APT41 hackers have also used the state-sponsored hacking activities for their own gain by using the initial compromises to conduct cyber criminal activities.

APT41 is also known under names such as Winnti, Wicked Panda and Wicked Spider.

Private actors also engage in cyber espionage

CFCS assesses that in rare instances cyber espionage extends beyond being a tool for foreign states and is also used by private actors, such as commercial companies or private detectives. As a result, organizations that would not normally catch the attention of foreign states may nevertheless become targets of cyber espionage. However, states are behind most cyber espionage activities, or they hire civilian hackers to carry out the activities on their behalf. One of the reasons why cyber espionage is rarely perpetrated by private individuals is likely their limited will and capacity. In case private actors do have the necessary will, they will often require others to do the hacking for them against payment. The involvement of a third party implies a risk that not many companies are ready to take.

In the few known foreign incidents of cyber espionage conducted by private individuals the goal was to target trade secrets or sensitive information that could help increase the company's competitive edge over critics or rivals.

WireCard critics – long-time targets of hacking attempts
In the summer of 2020, it became known that for years the Indian company BellTroX Infotech Services had likely conducted cyber espionage on behalf of various clients. Though the identity of these clients remains unknow, they likely include private detectives.

Some of the likely victims of BellTroX Infotech Services include journalists and short-sellers who had accused German WireCard, an international supplier of electronic payment and risk management services, of fraud. One of the victims, a years-long recipient of spear phishing emails, was also approached and interrogated by private detectives hired by WireCard. In June 2020, WireCard filed for bankruptcy after revelations that many of the company's business activities were misleading. WireCard is currently being investigated for extensive financial fraud.

The hacking campaign attributable to BellTroX has been described in detail in a report by the Citizen Lab titled Dark Basin. In the report, Citizen Lab also describes how critics of the US oil and natural resources company Exxon were targets of BellTroX's attacks.

Destructive cyber attacks

CFCS assesses that the threat from destructive cyber attacks against Danish public authorities and private companies is **LOW**, meaning that Danish private companies and public authorities are less likely to become targets of destructive cyber attacks within the next two years.

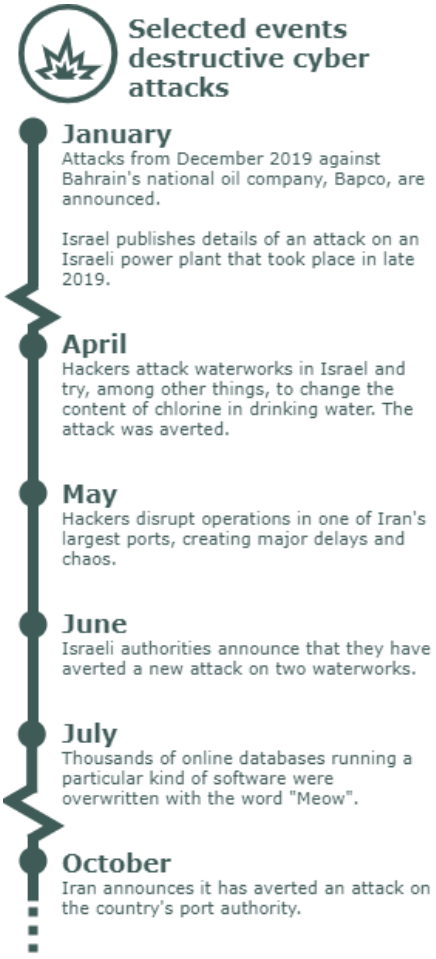
Though several foreign states hold the capabilities for destructive cyber attacks, it is less likely that they are currently intent on executing this type of attack against Danish targets.

Globally, destructive cyber attacks are still a rare occurrence. By far the majority of destructive cyber attacks launched until now have not resulted in physical damage but have been limited to data destruction through deletion or encryption without the possibility of recovery.

What is a destructive cyber attack?

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

- death or personal injury
- extensive property damage
- destruction or manipulation of information, data or software, rendering it unfit for use unless extensive restoration is undertaken



States do not have intention to carry out destructive cyber attacks against Denmark

The repercussions of successful cyber attacks may be very serious and include disruption of critical services such as power, transportation and Internet connection, or extensive destruction of data and units. Consequently, this potential threat holds serious consequences.

It is less likely that foreign states currently hold intentions to launch destructive cyber attacks against Denmark. However, as several foreign states possess destructive cyber attacks capabilities the threat level may increase should the intention change. The threat can increase in connection with an intensified conflict or geopolitical tensions between Denmark and states that possess the capacity for destructive cyber attacks.

CFCS assesses that states are behind the majority of destructive cyber attacks. For instance, Russia, China, Iran and North Korea have the capacity required to launch destructive cyber attacks.

So far, there are no known destructive cyber attack incidents that have specifically targeted Danish public authorities and private companies. However, the Danish shipping company A.P. Møller-Mærsk was among the victims of the global NotPetya attack that hit victims worldwide in 2017.

States develop capacity for destructive cyber attacks

States are likely working to develop their capacity for destructive cyber attacks, using tools like cyber espionage to facilitate such attacks.

It is possible that foreign states have attempted to compromise Danish critical companies as part of their efforts to build up capabilities for destructive cyber attacks against Denmark at some later point in time. The fact that Denmark saw several targeted attempts at gaining unauthorized access to organizations in the Danish energy sector in 2017 is a source of concern to CFCS.

The preparation of destructive cyber attacks will often involve mapping of organizations, systems and network units such as industrial control systems. By obtaining knowledge of organizations and their systems, hackers are able to develop custom malware and establish so-called backdoors into compromised systems to be used in subsequent destructive attacks. A backdoor into a system will enable hackers to launch a destructive cyber attack against the system more swiftly, making dormant backdoors a serious potential security breach.

Sandworm: The hackers behind most of the known destructive cyber attacks

Sandworm is a hacker group which, according to US authorities, works for the Russian state. The group is charged with orchestrating several serious destructive cyber attacks, including the 2015 and 2016 power outages in Ukraine, the 2017 NotPetya attack, and the Olympic Destroyer attack against the 2018 Winter Olympics in South Korea.

The group has earned its moniker Sandworm due to references found in its malware to the 1965 science fiction novel *Dune* by Frank Herbert in which giant sandworms play a key part. Sandworm is also known under the names Voodoo Bear and Telebots, among others.

15 October 2020: US authorities accuse six named Russian citizens of being part of the Sandworm hacker group. (Pool/AFP/Ritzau Scanpix)

Motives behind destructive cyber attacks varies

Though the overall purpose of destructive cyber attacks is to cause damage and destruction, the specific motives behind the attacks may differ. One such underlying motive may be sabotage, which may include an actor launching an attack to disrupt or prevent an adversary's access to systems, technologies or information. A destructive cyber attack may also be intended as punishment in connection with a conflict, where the purpose of the attack is to inflict economic damage or other types of resource damage to the victim. Destructive cyber attacks may also be launched as a way of sending the target and other potential victims a signal, or the attacks may be launched as a way of testing and potentially developing capacities.

The exact intention behind a cyber attack is often hard to determine, just as many attacks likely serve multiple motives simultaneously.

NotPetya, one of the world's most devastating cyber campaigns, may have served different purposes. Starting in Ukraine in 2017, the attack soon spread to the rest of the world. Several countries have attributed the attack to Russia. The attack can be interpreted as a punishment of Ukraine, which at the time was locked in a conflict with Russia. The attack could also be interpreted as a signal to the rest of the world of the risks involved in conducting business in Ukraine.

Destructive cyber attacks most common in connection with conflicts
CFCS assesses that most destructive cyber attacks are launched by states in connection with conflicts or geopolitical tensions.

In conflict areas where states have used destructive cyber attacks against civilian targets, including in the Middle East and Ukraine, the threat from destructive cyber attacks may be elevated. Danish companies conducting business across the globe may become targets of attacks that are not directed specifically against Denmark but against companies operating in the conflict areas.

The threat from destructive cyber attacks may also intensify for private companies working for organizations or states that are targets of destructive cyber attacks.

It is possible that Danish private companies and public authorities with a presence in conflict areas, not least in Ukraine and the Middle East, may be impacted by collateral effects of destructive cyber attacks such as power cuts or destruction of data.

Attacks against industrial control systems may result in physical destruction
Destructive cyber attacks against industrial control systems supporting the delivery of critical services may carry particularly grave consequences for society, partly because such attacks may interrupt the delivery of vital services such as power and Internet, partly because they can cause destruction of physical objects and personal injury.

Repercussions of destructive cyber attacks against industrial control systems may be particularly grave as such systems control and monitor industrial processes, including security mechanisms, whose interruption or manipulation may result in dangerous situations.

However, so far only few examples have been recorded of destructive cyber attacks being launched with the likely aim of causing actual physical damage.

There are only a few examples of cyber attacks being launched with the aim of causing actual physical damage

Stuxnet (2010) The only known destructive cyber attack to cause actual physical damage hit Iran in 2010. The hackers behind the attack used the Stuxnet malware to destroy Iranian uranium enrichment centrifuges.

Power outages in Ukraine (2016) The destructive cyber attack that hit the Ukrainian power supply in 2016 could well have resulted in physical damage to equipment, potentially resulting in prolonged power outages. IT security experts

have described how there were indications that the attack was intended to hit control switches and protection relays with Distribution Denial of Service (DDoS) attacks. The hackers failed in this part of the attack, though.

Triton (2017) It is possible that the 2017 cyber attack against the Triconex industrial control system in Saudi Arabia could have resulted in physical damage. The attack targeted a petro-chemical industrial enterprise and the Triconex system used by the targeted enterprise. Triconex ensures the controlled and safe disconnection of production systems in the event of critical errors or problems. Though the attack had the potential to cause physical damage, the security systems successfully shut down the production systems. The shutting down also resulted in the detection of the installed malware. Had the security mechanism been deactivated or manipulated, this could have increased the risk of personal injury or death in and around Triconex as a result of a leak of poisonous gasses or explosions.

States also behind major disruptive cyber attacks

States are also behind very disruptive cyber attacks which, even though they do not fall within CFCS definition of destructive cyber attacks, carry major repercussions. Though still rare, this type of attack has in a few instances abroad resulted in disconnections and disruption of access to and operation of multiple or vital digital systems and services.

The very disruptive attacks typically fall within the grey zone between destructive cyber attacks and cyber activism, due, among other things, to the relative similarity in attack techniques. One such borderline incident took place in the autumn of 2019 when Georgian webhosting provider Pro Service fell victim to a very disruptive attack. US and British authorities alike have publicly accused Russian state-sponsored hackers of being behind the attack, with British authorities claiming that the attack was intended to sow instability and undermine Georgia's sovereignty.

The cyber attack against Pro Service resulted in so-called defacement of more than 2,000 Georgian websites belonging to victims such as the Georgian government, presidential office, civilian courts, local city councils, banks and NGOs as well as large companies and news media. The original contents of the numerous websites were replaced by a photo of Georgian ex-president Mikheil Saakashvili captioned "I'll be back". The hackers then shut down the websites, though all sites were back online 24 hours later.

Picture of ex-president Mikheil Saakashvili used to deface websites before they were blacked out.

Cyber activism

The threat from cyber activism is **LOW**, indicating that Danish private companies and public authorities are less likely to become targets of attempted cyber activism within the next two years.

2020 only saw few, smaller activist cyber attacks against Danish targets. The threat from cyber activism typically materializes in connection with events or single causes attracting the attention of cyber activists.

The many protests characterizing 2020 have not reflected in an increase in the number of cyber activist attacks globally. The number of attacks has thus remained stable over the last few years.

It is less likely that Denmark will become the target of faketivism, a phenomenon where states launch cyber attacks under the guise of cyber activism.

Diverse activists behind cyber attacks

The purpose of cyber activism is to use cyber attacks as a tool to generate as much attention as possible around a cause using a variety of attack techniques. There is a wide span in attack complexity – from relatively simple Distributed Denial of Service (DDoS) attacks to more resource-heavy hack and leak operations. Cyber activists thus fall into different categories.

One type of activist supplements their protests, SoMe campaigns and happenings with simple cyber attacks, including, for instance, DDoS attacks.

DDoS attacks are relatively easy to carry out and typically require only minimal planning and technical knowhow. However, the simplicity goes both ways, and private companies and public authorities can relatively easily protect themselves against this type of attack.

COVID-19 forces climate activists to think out of the box
The spring 2020 Danish national lockdown due to COVID-19 also impacted on environmental activists. According to their own newsletter, the Danish branch of the Extinction Rebellion climate group, which used to be engaged in old-school activism, launched very simple DDoS attacks against a number of organizations in May 2020.

Each day, the activists turned to a new victim believed to be a major environmental polluter. Among the organizations that came under attack were BP, Shell, Danish shipping company A.P. Møller Mærsk and the Danish Ministry of Finance. The latter was attacked by Extinction Rebellion on the grounds that the Danish state had provided financial support to the Scandinavian airline company SAS.

The activists used a readily available tool, namely their home computers to send thousands of messages containing excerpts of the UN climate report to the companies' websites with the intention of overloading the websites and causing them to shut down.

Another type of activists uses cyber attacks as a central tool for activism. This group often has advanced technical skills, enabling them to launch sophisticated cyber attacks. An example in point is hack and leak attacks in which hackers steal and release their victims' sensitive information to hurt them.

This type of attack is typically harder to protect against and the consequences of a successful attack may prove more critical than for instance the average DDoS-attacks.

Cyber activism is thus expressed in a diverse range of activities, spanning from opportunistic attacks to more organized campaigns. However, a common denominator across the spectrum of activities is that while the attacks are often launched in response to specific events, there is a continuity in the themes pursued by the various activists and activist groups, for instance climate issues or animal welfare.

BlueLeaks: Black Lives Matter movement stirs Anonymous into action
In June 2020 the Distributed Denial of Secrets (DDoSecrets) hacker group leaked hundreds of gigabytes of data belonging to US and Canadian law enforcement authorities and intelligence services, including more than 16 million rows of data on police investigations, and personal data on more than 700,000 police officers.

According to open sources, the leaked data is from 251 law enforcement websites, of which many were intended for the sharing of data between different branches of the US authorities. All websites used the same software provided by Netsentiel, a company that also hosted data. It is likely that the hacker gained access to the many websites by exploiting a weakness at Netsentiel.

According to the founder of DDoSecrets, the group received BlueLeaks data from a hacker affiliated with the Anonymous hacker group.

Protest movements have limited online presence

The many protests that characterized 2020 were not accompanied by a corresponding increase in cyber activism.

Protests against the handling of the COVID-19 pandemic; the Black Lives Matter movement; the MeToo campaign; and the 2020 US presidential election all led thousands of protesters to the barricades in Denmark and abroad. At the same time, the COVID-19 pandemic has caused several countries to impose a ban on gatherings and restrictions, which in practice has made it more difficult to stage conventional protests.

Though lockdowns and restrictions have complicated traditional forms of mobilization, there has been no general increase in the number of cyber activists attacks globally. Despite incidents such as Blue Leaks and Extinction Rebellion's cyber activism, the number of cyber activist incidents is unchanged from the level seen in the past years.

Unrest and conflicts still feed into cyber activism

It has been several years since the last advanced activist cyber attack against Danish targets. Abroad, however, 2020 saw several examples of advanced cyber activist attacks in connection with conflicts and political unrest.

Such incidents included the leak of information on law enforcement members in the so-called BlueLeaks in the United States and Canada as well as in connection with the election in Belarus, where several official government websites were hacked in September 2020 with hackers posting text and images criticising President Aleksandr Lukashenko and his government.

The Nagorno-Karabakh conflict between Armenia and Azerbaijan also triggered cyber activist attacks, with Armenian cyber activists stealing and leaking classified information on members of the Azerbaijani naval forces online, etc. Armenian cyber activists also continuously launched DDoS attacks against multiple government online portals in Azerbaijan.

State use cyber activism as guise for influence

Posing as cyber activists, some states use a combination of cyber attacks and other types of propaganda tools in influence campaigns.

This was the case when in 2019 several Lithuanian news media became the victims of protracted compromise campaigns by hackers planting fake news on the media websites. The news mainly centred on NATO's presence in Lithuania. In November 2019, the Lithuanian armed forces stated that they suspected the incidents to be part of a larger Russian influence campaign aimed at discrediting NATO's presence in Lithuania.

Such incidents are popularly coined as faketivism, whose purpose mainly is to derail or deflect the public debate, thus cultivating a polarisation in the affected societies.

It is less likely that Denmark will become the target of faketivism. However, it is possible that the threat would grow in connection with issues of particular political, strategic or economic interest that foreign states could have a significant interest in influencing. Also, the threat would likely increase in the event of an intensified political or military conflict between Denmark and foreign states.

Hackers try to undermine trust in COVID-19 vaccines
In December 2020, the European Medicines Agency (EMA) announced that it had been compromised.

The hackers behind the compromise accessed information on Pfizer, BioNTech and Moderna vaccines against COVID-19, among other things. The EMA has subsequently described how the hackers in addition to stealing documents and confidential emails manipulated their contents and leaked them online in an attempt at eroding trust in the vaccines.

Cyber terrorism

The threat from cyber terrorism is **NONE**, indicating that it is highly unlikely that Denmark, including Danish private companies and public authorities, will be exposed to cyber terrorism attempts within the next two years.

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

Cyber attacks of such serious magnitude presuppose technical skills and organizational resources that militant extremists currently do not posses.
Though cyber terrorism may fall outside their skill set, militant extremists are able to conduct other types of cyber attacks. For instance, they have been known to conduct cyber activism.

Lack of capabilities accompanied by very limited intent
So far, militant extremists have not conducted cyber attacks that fall under CFCS definition of cyber terrorism. This is in part due to their insufficient skills, but likely also to the fact that the established terrorist groups generally do not consider a cyber attack a realistic and effective way to create the same level of fear and chaos as a conventional terrorist attack.

There are only very few examples of militant extremists calling for cyber terrorism, which supports the proposition that they lack the capabilities. Similarly, there have been no incidents in which militant extremists have claimed responsibility for any of the destructive cyber attacks that the world has witnessed so far.

Even though terrorist groups do not always claim responsibility for their terrorist acts, CFCS assesses that they would feel compelled to propagandize their cyber attack achievements to emphasize the emergence of a new threat.

Crime-as-a-Service may enable militant extremists to launch certain types of cyber attacks
A phenomenon like Crime-as-a-Service (CaaS), which offers a wide range of hacker tools and services for sale online, may possibly improve the cyber capabilities of militant extremists.

CaaS could potentially allow terrorist groups to purchase services, tools and access that they themselves are incapable of developing or exploiting.

However, it is doubtful that CaaS can facilitate attacks that would fall under CFCS definition of cyber terrorism. The tools exchanged online between criminals have primarily been developed to accommodate financially motivated cyber criminals and not to facilitate cyber attacks that could be categorized as cyber terrorism.

Another barrier includes language and culture. Several criminal networks and hacker forums are Russian-speaking, and the Russian-speaking hacking community is notoriously suspicious of cooperation with non-Russian speaking hackers.

Terrorists behind other types of cyber attacks
In some instances, militant extremists have employed other cyber attack techniques besides cyber terrorism to promote their cause.

These attacks can typically be characterized as simple cyber activism aimed at drawing attention to a specific cause, for example by defacing websites with militant extremist messages.

In addition to cyber activism, terrorist groups can also use the proceeds of cyber crime to finance terrorism. However, such incidents do not count as cyber terrorism either.

Trends and tendencies

The pandemic has brought cyber security concerns from the corporate domain into the private living room

For many people, the pandemic has accelerated the digitisation of the workplace. The spring 2020 national lockdown in Denmark created an acute need to ensure business continuity from home – a transition that required public authorities and private companies alike to make fast decisions on establishing or expanding remote access and digital solutions for online interaction.

This digital transformation has proved to have several benefits. Organizations have developed more flexible work practices, and many have come to see the benefits of virtual meetings over traditional physical ones. The shift to new digital work practices and remote working will likely continue even once the COVID-19 health crisis has eased.

Working from home moves digital frontline into private living rooms

The roll-out of home working has given rise to a number of cyber security challenges, including improperly secured remote access solutions or hasty remote access setup. Hackers are constantly on the lookout for security holes, using known vulnerabilities or insecure passwords to gain network access.

One such pandemic opportunist includes a hacker group that has added a new module to their malware which specifically targets exposed remote access (RDP) connections in order to use them as launch pads for targeted ransomware attacks against high-value victims. CFCS has repeatedly warned that hackers are exploiting RDP connections. Nevertheless, in the second quarter of 2021 more than 4,000 potentially vulnerable RDP ports remain open to the Internet in Denmark, while the corresponding figure is close to five million worldwide.

When computers outside the digital perimeter of an organization connect with organizational systems, they become potential entry points for hackers, increasing the organization's vulnerability. When the digital frontline moves into the private living room of employees, organizations need to be ready to address the cyber security concerns related to working from home.

When working from home, some employees will be less attentive to IT security. They might not consider themselves attractive targets to hackers or give any thought to the fact that if they use their personal home computer for work-related activities, such as emails and meetings, their private computer becomes part of the company IT infrastructure.

If a work-from-home computer has access to core parts of the company IT network, for example via VPN connection, hackers may infect the computer with malware using it as an entry point for access to the company network. As a result, it is vital that the same degree of protection is provided in home computers accessing company data through a VPN connection as in workplace computers.

Arrival of 5G technology in Denmark may change the digital landscape and the impact of the cyber threat in the medium term

2020 saw the introduction of 5G in Denmark. The companies operating mobile infrastructure in Denmark (TDC, 3 and TT Network, which is jointly owned by Telenor and Telia), all managed to switch on 5G before the end of the year. So far, only one company has launched 5G services across the country, while the rest are still in the process of rolling out 5G networks.

So far, the Danish society has continuously moved towards increased digitisation and use of mobile services, and there is nothing to suggest that this trend will reverse. 5G is the best next step in wireless evolution.

While 4G has primarily connected people to the Internet, 5G promises faster speeds, faster response time, and increased device connectivity and more mobile networks dedicated to IoT and industrial automation. However, in the short term, 5G will mainly differ from 4G in that it offers higher data rates, the reason being that 5G will initially operate in conjunction with existing 4G networks.

5G expands the attack surface for hackers

5G promises improved mobile network security. However, lessons learned from 4G show that new technology always contains vulnerabilities, so the future will tell whether 5G will be able to deliver on its full promise. What is certain, though, is that the complexity of 5G will create new attack surfaces in the telecom infrastructure. Decentralized network architecture, edge and cloud computing, and software that replaces physical hardware are fundamental to the high performance of 5G, but at the same time these features expand the attack surface.

The many sensors, products and devices that will likely be connected to the Internet via 5G will also widen the attack surface, first and foremost posing a threat to the users of the equipment but also in the sense that the equipment may become compromised and used as a launch pad for cyber attacks against other users of the Internet or telecom infrastructure.

Physical equipment that is digitally controlled, for instance through a 5G connection, strengthens the linkage between the physical and digital world and may heighten the risk of a cyber attack causing physical harm. Such equipment may include industrial machines, autonomous vessels or healthcare equipment.

The full functionality of 5G will not be available until 2 to 4 years from now at the earliest, as the telecom providers need time to expand 5G coverage and introduce adjustments in the infrastructure that supports advanced 5G services. Consequently, it is less likely that 5G will significantly change the digital landscape in the short term.

5G requires new approaches to counter the cyber threat

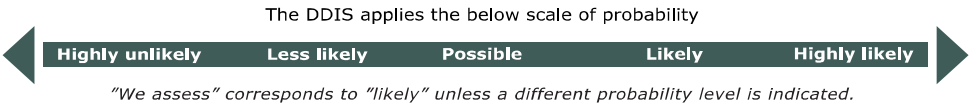
Should 5G become as successful as expected, critical societal functions and company productivity and financial performance will come to rely on the availability, confidentiality and integrity of 5G services. These factors will particularly impact on the services that are reliant on the functions and services that are enabled exclusively by 5G. For such services it will not be possible to ensure availability by use of redundant connections to traditional technologies such as 4G or fixed Internet connections. Discussions

on 5G show how new technologies and the opportunities they present may also have an impact on the cyber threat landscape.

Threat levels

The Danish Defence Intelligence Service uses the following threat levels.

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.



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