CENTRE FOR CYBER SECURITY

Threat Assessment:

The cyber threat against Denmark 2022

1st edition August 2022.

Table of Content

CENTRE FOR CYBER SECURITY

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

1. edition August 2022.

The cyber threat against Denmark 2022

The purpose of this threat assessment is to inform decision-makers of public authorities and private companies on the cyber threat against Denmark. The threat assessment outlines the different types of cyber threats facing Denmark and can be used as part of the basis for public authorities' and private companies' cyber security risk assessment efforts.

Key assessment

- The threat from cyber espionage is **VERY HIGH**. The persistent cyber espionage threat emanates from Russia and China, in particular, and regularly results in cyber attacks on Danish targets. Parts of the Danish society face a persistent, active and serious threat, particularly against entities affiliated with the Danish foreign and defence ministry but also against public authorities and private companies in other critical sectors.

- The threat from cyber crime is **VERY HIGH**. Ransomware attacks are the most serious cyber crime threat facing Denmark. Cyber crime organizations are characterized by cooperation, division of labour and specialization, which contributes to maintaining the very high threat level of cyber crime.

- The threat level from cyber activism is raised from **LOW** to **MEDIUM**. The CFCS has raised the threat level against the backdrop of an increase in cyber activist attacks against European NATO countries in connection with the war in Ukraine. It is possible that especially pro-Russian hackers will attack targets in Denmark.

- The threat from destructive cyber attacks is **LOW**. It is less likely that foreign states harbour intentions to conduct destructive cyber attacks against Denmark at present. Destructive cyber attacks are often launched by states in connection with conflicts or geopolitical tensions. Several foreign states have the capability to launch destructive cyber attacks.

- The threat from cyber terrorism is **NONE**. The absence of a cyber terrorism threat is in part rooted in the fact that militant extremists have limited intent to conduct cyber terrorism and in part that they do not have the capabilities required to launch cyber attacks that create the same devasting effects as conventional terrorism.

- Foreign states, including Russia, actively use cyber attacks in their attempts to influence public opinion in other countries. However, it is likely that at present Denmark is not a priority target for influence operations by foreign states.

Introduction

Russia's invasion of Ukraine in late February 2022 has significantly changed the security policy landscape. The future seems more uncertain than before the invasion and this uncertainty extends to the cyber realm. Consequently, in March 2022 the Centre for Cyber Security (CFCS) under the Danish Defence Intelligence Service published a threat assessment titled "The cyber threat against Denmark in light of Russia's invasion of Ukraine", in which the CFCS described the impact of the Russian invasion on the cyber threat landscape.

Thus the purpose of this publication is to assess the cyber threat against Denmark in a broader context than the Russian invasion alone. Because even though the uncertainty and tensions that characterize the current situation raise the risk of misunderstandings and escalation, the CFCS still assesses that all threat levels, except the threat from cyber activism, remain unchanged.

The cyber threats facing Denmark were already serious before the invasion of Ukraine and will remain so irrespective of how the situation in Ukraine develops. Foreign states and criminal hackers in particular continue to pose a significant cyber threat to Denmark. Russia, China and criminal hacker groups regularly launch cyber attacks on Danish public authorities and private companies. Some of these attacks are launched in direct response to the war in Ukraine, but cyber attacks have been a persistent challenge since even before the Russian invasion – and will continue to be a source of concern irrespective of the war.

Cyber crime poses one of the most serious cyber threats to Denmark. Cyber crime is the source of serious financial repercussions to both public authorities and private companies. In certain cases, cyber crime has led to disruption of critical services abroad.

Cyber espionage is politically and financially motivated. Foreign states continue to conduct cyber espionage aginst Danish targets aimed at gaining access to sensitive and valuable information that Danish organizations want to keep protected. If this type of information is compromised, it may be exploited to weaken Denmark's foreign policy position or to prepare for future conflicts, ultimately potentially affecting Denmark's national security.

In this year's cyber threat assessment, the CFCS assesses not only the threat from cyber crime and cyber espionage but also the threat from cyber activism, destructive cyber attacks and cyber terrorism and shed light on the threat from cyber-enabled influence operations.

Cyber-enabled influence operations also a threat

Cyber attacks are but one of many types of activities used by foreign states in their influence campaigns. Foreign states also engage in influence activities that do not involve cyber attacks.

The threat from cyber-enabled influence operations shares some similarities with the threat from cyber activism, as they both rely on many of the same attack techniques. However, the threat from cyber activism and the threat from cyber-enabled influence campaigns emanate from threat actors with different capabilities. The threat from cyber activism emanates from individuals and non-state hacker groups, while the threat from cyber-enabled influence campaigns emanates from foreign states. In addition, the two types of attack differ in the sense that cyber activists launch attacks to draw maximum attention to a specific cause, while states launch the same type of attack to sway public opinion without disclosing who is pulling the strings.

The threat level for cyber activism is raised to MEDIUM while the other threat levels remain unchanged

The CFCS assesses that Denmark is facing a **VERY HIGH** threat from cyber espionage and cyber crime. The CFCS raises the threat level for cyber activism from **LOW** to **MEDIUM** based on an increase in the number of pro-Russian cyber activist attacks against targets in European NATO countries. In addition, Danish public authorities and private companies also face a **LOW** threat from destructive cyber attacks. The threat from cyber terrorism remains **NONE**.

A **VERY HIGH** threat level indicates that cyber attacks are highly likely to occur. The CFCS determines threat levels based on an assessment of the threat actors' capability and intent to launch cyber attacks. A **LOW** threat level indicates that a cyber attack is less likely but not unlikely to occur. A **LOW** threat level does not equal the absence of a threat. This aspect is important to emphasize – particularly in relation to the threat from destructive cyber attacks where the CFCS assesses that there are significant capabilities but limited intent. All it takes to change the threat level is a change in intention, which means that threat levels may change with little or no warning. The change in the intention of cyber activists is exactly what prompted the CFCS to raise the threat level, as the capability of cyber activists to launch cyber attacks against Denmark already existed.

Threats with the same threat levels may have very different consequences

Cyber threat levels are designed to give a broad indication of the likelihood of cyber attacks against Danish private companies and public authorities. Threat levels do not, however, indicate the likelihood of a successful attack or its potential consequences.

For example, the consequences of a successful cyber activist attack versus a destructive cyber attack will be very different. The threat from destructive cyber attacks is **LOW**, but successful destructive cyber attacks can have very serious consequences, at worst causing death or personal injury or disruption of critical functions. The threat from cyber activism, on the other hand, is **MEDIUM**, but cyber activist attacks will often only inflict reputational damage to an organization or cause short-term website disruptions, for instance.

The CFCS uses the Danish Defence Intelligence Service's threat levels and probability degrees explained at the end of this assessment. In this assessment, the CFCS describes the threat in the short term, operating with a time frame of 0-2 years.

Enjoy your reading!

Cyber espionage

The threat from cyber espionage against Denmark remains **VERY HIGH**. This means that Danish public authorities and private companies are highly likely to fall victim to cyber espionage within the next two years. Entities with a relation to the policy areas of the Danish foreign and defence ministry are priority targets of cyber espionage, while the threat is also directed at public authorities and private companies in other critical sectors. The threat from cyber espionage is ever-present and results in regular cyber attacks on Danish targets. Some public authorities and private companies are under constant threat, while the threat facing others may vary over time.

The serious threat from cyber espionage is rooted in the interest of foreign states, including in particular Russia and China, in gaining access to information on foreign, security and defence policy issues. Espionage seeking information on these topics may give foreign states insight into Danish foreign and security policy decisions and military capabilities and plans. In some cases, the information pursued may have an impact on Denmark's national security. Information of this nature stolen by foreign states may be used to undermine Denmark's foreign policy sway. Thus, the consequences of cyber espionage far exceed those of regular IT security incidents or operational difficulties.

The CFCS assesses that Russia's invasion of Ukraine has not resulted in a change in the cyber espionage threat level against Denmark, a level that was already **VERY HIGH** before the invasion. It is highly likely that following the invasion of Ukraine, Russia will remain just as intent on conducting cyber espionage against public authorities and organizations in Denmark that may impact on Danish foreign, security and defence policies as it was prior to the invasion.

The threat from cyber espionage targets foreign and defence policy in particular

Cyber espionage is rooted in political and financial motives. Parts of the Danish society are facing a persistent, active and serious threat. The threat is significant especially towards targets with relations to the policy areas of foreign- and defence policy. Authorities and companies affiliated with these policy areas are continuesly victims of cyberespionage attemtps.

For a number of years, public authorities and private companies in the shipping, energy and defence industries have been under a very high threat from cyber espionage. Foreign states may have an interest in targeting specific companies, technologies or information. For instance, foreign states, including China, are typically interested in equipment and technology that can be used for both civilian and military purposes. In addition, recent years have seen an increased threat to the transport and research sectors.

The threat from cyber espionage is linked to the foreign policy challenges that Denmark is facing. Russia's and China's ambitions in Denmark's neighbouring region and the Arctic are some of the motivations behind their cyber espionage attempts against Danish public authorities and organizations occupied within these areas. In

addition, Denmark participates in several foreign and security policy cooperation frameworks, including the EU and NATO, which also hold the interest of China and Russia.

The CFCS assesses that Russia's invasion of Ukraine has not resulted in a change in the cyber espionage threat level against Denmark, a level that was already **VERY HIGH** before the invasion. It is highly likely that following the invasion of Ukraine, Russia will remain just as intent on conducting cyber espionage against public authorities and organizations in Denmark that may impact on Danish foreign, security and defence policies as it was prior to the invasion.

Other parts of the Danish society exposed to a more varied threat
The threat from cyber espionage is also directed at other parts of society. Here, the cyber espionage threat varies over time and generally follows the shift in priorities of foreign states' intelligence services.

In 2021, the CFCS raised the cyber espionage threat level from **HIGH** to **VERY HIGH** for the transport sector and Danish universities and research institutions.

The heightened threat against universities and research institutions emanates from several foreign states conducting cyber espionage against research institutions worldwide. In recent years, the CFCS has seen multiple cyber attack attempts against Danish universities and research institutions. Foreign states have different motives for conducting cyber espionage against research institutions and universities. Some foreign states are driven by the ambition to achieve competitive and strategic advantages by stealing sensitive or valuable information. Other foreign states likely conduct espionage to advance their own research programmes and development of critical services such as critical infrastructure. It is likely that foreign states also try to conduct cyber espionage against universities and think tanks in order to gain insight into research based contributions to current foreign and security policy related issues.

The increased threat against the Danish transport sector may be motivated by security policy interests. Due to their role in supporting the Danish armed forces or other countries' military operations, parts of the transport sector may also be of interest to foreign states. Collection of information on the transport sector, which is part of Denmark's critical infrastructure, may also be used in the preparation of destructive cyber attacks or physical attacks against the sector.

In 2022, the CFCS lowered the threat level for cyber espionage against the telecom sector from **HIGH** to **MEDIUM** compared to the 2019 threat assessment. The adjustment took place against the backdrop of a new analysis indicating that even though it is possible that foreign states are planning cyber espionage activities against the telecom sector in Denmark, it is likely not a high-priority target.

Cyber espionage also affects victims randomly, as foreign states also launch opportunistic cyber attacks, for instance in connection with vulnerability disclosures or supply chain attacks in which foreign states compromise multiple organizations within a short time span. Following the initial compromise, the foreign states will seek to identify access points, data or accounts worth pursuing.

Exchange Server Zero-day vulnerabilities widely exploited

On 2 March 2021, Microsoft and US company Volexity released a number of reports and blogs describing a cyber campaign targeting Microsoft Exchange servers by means of several zero-day vulnerabilities. In July 2021, the United States, among others, attributed some of the attacks on Microsoft Exchange Servers to Chinese state-affiliated hackers. The campaign compromised several sectors in, primarily, the United States, including research and education institutions, think tanks, NGOs and the defence industry. Microsoft has dubbed the hacker group behind the attacks HAFNIUM.

Photo by: Andy Wong/AP/Ritzau Scanpix

Russia and China pose the most significant cyber espionage threats

Russia and China, which both have advanced cyber espionage capabilities, pose the most significant cyber espionage threat. Both countries pose a constant threat to Danish public authorities and private companies.

Russia has a serious arsenal of cyber tools which it employs systematically to promote its national interests. Cyber espionage may also be used to prepare destructive cyber attacks.

China conducts extensive cyber espionage all over the world, including against Danish public authorities, private companies and organizations. China's military and intelligence services hold powerful cyber tools and capabilities, allowing it to gain full and permanent access to organization information. China poses a constant and active threat in pursuit of promoting its national security and foreign policy as well as its economic and commercial interests.

However, Russia and China are not the only countries whose priorities include expanding their cyber capabilities. It is highly likely that an increasing number of foreign states will pose a cyber threat to Denmark in the future. The CFCS assesses that Iran, North Korea, Vietnam, Pakistan and India, among others, have the capabilities to conduct cyber espionage. It is likely that these states generally have little interest in attacking Danish targets. At present, these states primarily use their capabilities to target countries in their neighbouring area. However, Danish private companies and public authorities located in or close to these countries may fall victim to cyber espionage. Either because compromised targets may be used as stepping stones for cyber attacks against other targets, or because the states have an interest in gaining access to information on Danish foreign and security policy in the region and information on the host country or region of the organization. Danish universities and research institutions whose knowledge, cooperation partners or research is of interest to one or more of these countries are also at risk of cyber espionage.

Map of selected countries with cyber espionage capabilities.

Foreign states use an array of cyber espionage techniques

Cyber espionage typically targets IT systems and networks that contain information such as emails and documents which hold the interest of foreign states. The possibility for foreign states to gain access to this information varies and depends on the victims' IT systems and the attacker's tools and capabilities. Consequently, foreign states use an array of attack techniques.

Attack methods could be simple attacks such as so-called brute force attacks, in which hackers use large numbers of possible usernames and passwords to gain unauthorized access to a system. In addition, hackers create false websites where victims are lured into entering their usernames and passwords. The spread of malware through phishing is still a widely popular attack technique.

More advanced attacks may occur through an organization's suppliers, for instance via a software supply chain attack in which attackers hide malware in otherwise legitimate software updates distributed by the suppliers to their customers. Cyber espionage may also be directed against other suppliers and cooperation partners that may be exploited as stepping stones for attacks against other organizations that are of interest to foreign states. Compromised organizations may also be used as involuntary infrastructure in future attacks done by the hackers.

The attacks may be directed at the targeted organization's entire network or parts of it such as a ministry's IT systems or networks serviced by an external supplier. On a smaller scale, attacks may also target specific computers and email accounts.

Cyber attacks may also be conducted by exploiting IT system vulnerabilities such as hardware and software errors, lack of updates or misconfigurations. In some instances, the detection of vulnerabilities in common IT systems means that a wide selection of organizations become potential targets.

Foreign states often use the same tools and techniques as other types of hackers to attack their targets. Recycling of techniques and tools allows the attackers to economize their resources and attack multiple targets at once or over a prolonged period. Russia and China have the capabilities to conduct multiple simultaneous espionage campaigns across the world, including in Denmark. However, recycling of techniques and tools makes it easier to detect the attacks and use the lessons learned from previous attacks to help prevent future attacks.

Foreign states launch brute force attacks, including against Denmark

Even though foreign states such as Russia and China have advanced cyber capabilities, they also use more simple attack techniques.

In the summer of 2021, UK and US authorities published a so-called Cybersecurity Advisory, in which they described how the Russian military intelligence Service GRU had orchestrated a global brute force campaign that ran from 2019 to 2021. The campaign enabled GRU to access sensitive information such as login credentials and emails.

The CFCS assesses that Danish organizations regularly fall victim to cyber espionage attempts by means of brute force attacks by foreign states.

Cyber crime

The threat from cyber crime is **VERY HIGH**, indicating that Danish public authorities and private companies and citizens are highly likely to be exposed to cyber crime attempts within the next two years.

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

Denmark is regularly exposed to many different types of cyber crime, which – just like other types of crime – generally consists of different types of theft, fraud and extortion.

Extortion through ransomware attacks is currently a key part of the threat landscape. However, the threat from cyber crime is dynamic and will likely evolve in the future. There are multiple factors driving this development, including changes in the use of digital services, which cyber criminals can exploit, and new cooperation opportunities for cyber criminals. This development will likely continue within the spectrum of theft, fraud and extortion.

Russia's invasion of Ukraine has sparked several reactions in the cyber criminal community, but CFCS assesses that the invasion has not had any significant impact on the threat from cyber crime against Denmark.

Cyber crime affects all parts of Danish society

The threat from cyber crime is very active and affects all parts of Danish society, both now and long-term. In general, cyber criminals have favourable conditions to commit cyber crime. They are for instance able to work anonymously and cooperate with other cyber criminals, sharing tools and techniques online.

As some types of cyber crime rely on targeting as many victims as possible, for example through phishing emails spread to thousands of recipients, including in Denmark, it is highly likely that almost all Danish citizens and private companies will be exposed to cyber crime attempts. Other types of cyber crime more specifically target Danish public authorities and private companies, offering cyber criminals the chance to extract millions from each victim.

Denmark is facing a global billion-worth cyber crime industry which continues to attract new hackers and pose a constant threat to Denmark.

Ransomware attacks may carry serious consequences
At present, extortion through ransomware attacks is the most visible and serious cyber crime threat to the Danish society. Cyber criminals encrypt key IT systems belonging to public authorities and private companies and withhold the key needed to decrypt the systems until the victims pay the demanded ransom. Cyber criminals also often threaten to leak the stolen data if the victims refuse to pay. Targeted ransomware attacks against public authorities and private companies have been an integral component of the threat landscape in Denmark over the past couple of years.

In 2021, several companies across Denmark fell victim to ransomware attacks, including Danish utility company Kalundborg Forsyning, wind turbine maker Vestas, IT company AK Techotel and the largest hotel chain in the Nordic Countries, Nordic Choice Hotels, which also runs hotels in Denmark.

The serious repercussions of ransomware attacks are not confined to the targeted authorities and companies but can extend to critical societal functions as well.

A case in point is the May 2021 ransomware attack on US oil company Colonial Pipeline. The attack forced Colonial Pipeline to halt all pipeline operations for six days, causing long lines at gas stations along the US East Coast. The attack was a testament to how ransomware attacks can threaten critical supply chains.

Several factors support the current threat from ransomware
Ransomware hackers are well-organized and follow tried and tested techniques for cyber attacks. In addition, ransomware attacks have turned into a profitable criminal business activity capable of sustaining an entire ecosystem of specialized criminal hackers. As a result, hackers are able to conduct more and increasingly effective ransomware attacks.

Hackers have developed profitable business models, such as so-called Ransomware-as-a-Service platforms. The operators running the platforms develop and maintain specific ransomware malware and infrastructure which they share with other hackers in exchange for a part of the ransom payments. These platforms have contributed to lowering the threshold for who can commit ransomware attacks, increasing the number of cyber criminals capable of launching this type of attack.

So far, criminal hackers have proved quite resilient to external pressure and changes in conditions. Intervention by authorities and IT security companies, the dependence on online markets and services by other hackers as well as frequent disruptions internally in the criminal community present a continous, significant challenge to the hackers. However, criminal hackers are generally good at adapting, for example by launching new ransomware variants and developing new ways to cooperate.

Criminal hackers use a wide array of techniques for financially motivated crime
Ransomware attacks are but one way for criminal hackers to conduct financially motivated cyber crime. For instance, criminal hackers also employ cyber attacks to steal financial and personal information which they can exploit or sell to other criminals.

For years, theft, abuse and selling of credit card information have been steady components of the criminal hacker community with digital markets on the dark web.

As a preventive measure, the financial sector in Denmark and other countries has increased protection against credit card abuse by introducing multi-factor authentication in connection with financial transactions. Despite this initiative, there is still a substantial market for sale of stolen credit card information on the dark web.

Hackers avail themselves of several different techniques to steal credit card information, including by compromising companies that hold financial information on their clients, by compromising payment systems or websites that offer online payment or by affecting more or less random victims via phishing.

Criminal hackers also target newer types of digital assets such as crypto currencies and virtual currencies associated with online gaming.

While extortion and theft are widely popular techniques with criminal hackers, some criminal hackers specialize in fraud, including Business Email Compromise (BEC). In this type of fraud, cyber criminals hack company or authority executives, subsequently posing as the executive and authorizing wire transfers to their own accounts.

As cyber crime can include many different types of criminal activity, criminal hackers can choose from a wide range of attack techniques. In order to be able to hack into their victims' systems, cyber criminals spread malware through phishing or exploit known system vulnerabilities and leaked usernames and passwords. Once cyber criminals have compromised a victim, they may in some cases sell access to the compromised network to other criminals or deploy additional tools and malware in order to gain wider access to the victim's network.

Hackers are adaptable and benefit from a robust and anonymized community

Today, the cyber criminal community is extensive and capable of appealing broadly to new hackers, offering different opportunities for cooperation, division of labour and specialization. Conditions for cyber criminal activities will likely remain favourable in the years to come, keeping the threat from cyber crime at a very high level.

Hackers generally benefit from an environment that facilitates anonymity and confidentiality. Technologies such as crypto currencies, anonymization tools such as TOR and VPN services as well as hacker forums and market places on the dark web all serve to aide hackers in their pursuit of malicious activities. The anonymity and network based cooperation between hackers makes the community robust and resilient towards intervention by authorities. If a network is shut down, other hackers are quick to step in and take over, just as new networks may emerge.

However, the anonymity that protects hackers is a two-edged sword, as it also makes it relatively easy for hackers to defraud each other. Consequently, hackers are trying to build trust by establishing a positive reputation among their peers. Some groups donate millions to middlemen on hacker forums to serve as a visible guarantee to their partners. Other groups, typically the more well-established ones, have formed longstanding ties with selected partners.

The reliance on specific technologies and services makes cyber criminals vulnerable to interventions against cryptocurrencies and hacker forums. However, the rise in targeted ransomware attacks has demonstrated that criminal hackers are generally quick to adapt to new conditions. New attack and extortion techniques as well as new organizational structures are relatively quickly copied and spread across the cyber criminal community.

As US authorities ramped up pressure on certain hacker groups following the 2021 Colonial Pipeline attack, many hackers were quick to switch over to new ransomware platforms.

Russia's invasion of Ukraine leaves no significant impact on the cyber crime threat

There has been several reactions from criminal hackers to Russia's invasion of Ukraine. Russia, in particular, is home to several criminal hacker groups and networks.

Though hackers behind the Conti ransomware have, for instance, threatened to retaliate if the West attempts to attack critical infrastructure in Russia or Russian-speaking countries, the CFCS assesses that, the Conti group is still mainly driven by financial motivation.

In the wake of their threats, the hackers behind the Conti group suffered a data leak exposing several of its members and tools. Several competing ransomware groups have stated that they are apolitical, citing that their networks comprise hackers in Russia, Ukraine and other countries. In addition, some criminal hacker forums have banned discussions on the war or excluded Russian hackers.

Despite the threats made by some criminal actors, the CFCS knows of no examples of well-established criminal hacker groups having thrown away the chance of financial gain by launching destructive cyber attacks or ransomware attacks that offer no prospect of decryption. Organised criminal hackers make a living from cyber crime and enter into integrated criminal supply and value chains in which the profit from, for instance, ransomware attacks is distributed between multiple actors. If criminal hackers were to use these capabilities to launch destructive cyber attacks, this would be a breach of the value chain, potentially hampering their possibilities of forming future profit-driven cooperation with other criminals.

Russia's invasion of Ukraine thus has not significantly changed the cyber crime threat against Denmark.

Cyber activism

The threat from cyber activism against Denmark is **MEDIUM**. On the 18th of May 2022, CFCS raised the threat level from **LOW** to **MEDIUM** on the basis of a number of cyber attacks launched against European NATO countries by pro-Russian cyber activists.

The threat level **MEDIUM** indicates that there is a general threat against Denmark and that Danish private companies and public authorities may possibly fall victim to cyber activist attacks in the short term.

Cyber activism is carried out by individuals and hacker groups that use cyber attacks to generate as much attention as possible to a specific cause or to punish organisations. Cyber activism is typically motivated by different ideological or political concerns, ranging from single issues to resistance towards power structures. Cyber activists attack victims whom they perceive as symbolic targets or opponents to their cause.

Cyber activists have the capabilities to launch different types of cyber attacks, ranging from simple DDoS and website defacement attacks to more resource-demanding hack and leak operations.

The war in Ukraine raises the threat level

Russia's invasion of Ukraine has especially intensified activities in cyber activist communities.

The number of cyber activist attacks has dropped over the past few years globally, but Russia's invasion of Ukraine has galvanized some elements of the activist community into action. Initially, most cyber activist attacks were launched in direct response to the war, mainly targeting Russia, Ukraine and Belarus. Since then, cyber activist attacks have also targeted European NATO countries.

The heightened activity level of pro-Russian cyber activist groups also raises the threat from cyber activist attacks against Denmark.

Pro-Russian Killnet behind cyber attacks

The pro-Russian hacker group Killnet has claimed responsibility for a number of cyber activist attacks in connection to the war in Ukraine. For instance, Killnet has launched DDoS attacks against authority websites, banks and TV stations in several European countries.

Even though the threat level against Denmark is raised based on pro-Russian activities, actors on both sides of the conflict pose a threat in terms of activist cyber attacks against Denmark. Pro-Russian activists may have an interests in punishing or influencing Denmark's support to Ukraine, while pro-Ukrainian activists may have an interest in punishing organizations affiliated with Russia or in attacking targets in countries whose support to Ukraine is perceived as feeble.

Danish organizations or individuals affiliated with Ukraine are therefore also at risk of being affected by the attacks against targets in Ukraine. Danish victims are, for example, at risk of having sensitive information leaked in connection with hack and leak attacks on organizations in Ukraine.

The threat from Danish activist communities is still very limited

Activist cyber attacks from inside Denmark are rare, and examples are few of conventional activism and protests in Denmark leading to cyber attacks. Within the past few years, disagreement on social or political issues has not led to cyber activist attacks against Danish targets. As a case in point, the Danish protest movement ”Men in Black” staged several protests in Denmark in 2021, without their activities including activist cyber attacks.

Destructive cyber attacks

The CFCS assesses that the threat from destructive cyber attacks against Denmark is **LOW**, indicating that Danish companies and authorities are less likely to fall victim to destructive cyber attacks within the next two years.

What is a destructive cyber attack?

The 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.

Foreign states have no intention of carrying out destructive cyber attacks against Denmark

It is less likely that foreign states currently harbour intentions to launch destructive cyber attacks against Denmark. However, foreign states continue to develop the capabilities to launch destructive cyber attacks with little warning.

Even though it is less likely that foreign states harbour intentions to launch destructive cyber attacks, a shift in their intentions could carry serious repercussions.

The war in Ukraine has demonstrated that destructive cyber attacks are mainly used by nation states in connection with conflicts. Several states, including Russia, have destructive cyber attack capabilities. As a result, the threat from destructive cyberattacks against Denmark may increase with little warning should the political situation escalate towards a military confrontation between Russia and NATO as a result, for instance, of the war between Russia and Ukraine.

So far, there are no known examples of destructive cyber attacks specifically targeting Danish authorities or companies. However, Danish shipping company A.P. Møller-Mærsk were among those that felt the impact of the 2017 global NotPetya attack against Ukraine, which spread to victims across the world.

Destructive cyber attacks can have serious consequences

Even though the threat from destructive cyber attacks is currently **LOW**, the threat presents a serious threat against Denmark as destructive cyber attacks can have devastating consequences.

The potential consequences of a destructive cyber attack include the disruption of critical societal functions and services such as disruption of power supply, transport or Internet activity. A destructive cyber attack may also result in widespread destruction of data and devices.

Destructive cyber attacks may serve other purposes than destroying a specific target. One motive may be to send a political signal to a victim, to potential victims or to a country. Destructive cyber attacks can also have a military aim. Militarily, destructive cyber attacks can for instance contribute to limiting the Danish armed forces' capability to communicate and manoeuvre. It is often difficult to assess the exact intention behind a destructive cyber attack, just as attacks may also be multi-pronged.

Destructive cyber attacks in Ukraine in 2022

Open sources have regurlarily reported on destructive cyber attacks against Ukraine during the war. Non-exhaustive examples include:

- **WhisperGate/WhisperKill** – Wiper attack against Ukrainian authorities, etc. in January 2022
- **AcidRain** – The provider of the Viasat satellite communication fell victim to a destructive cyber attack the day before the onset of the Russian invasion. The attack hampered Ukrainian military communication as thousands of satellite modems in Europe, in particular, were taken out.
- **HermeticWiper** – This attack was launched the day before the Russian invasion against Ukrainian authorities, IT companies and critical societal sectors.
- **CaddyWiper** – In March 2022, a new wiper malware was discovered in Ukraine. So far it has not been possible to identifythe victims in Ukraine of this new strain of wiper malware.

Destructive cyber attacks mainly used in conflict areas

Prior to Russia's invasion of Ukraine in February 2022, there had been few examples of destructive cyber attacks corresponding to the CFCS's definition of a destructive cyber attack. These had been launched in areas characterized by political tension and conflict such as the Middle East and Ukraine.

In conflict areas, the threat from destructive cyber attacks may thus be higher. It is possible that Danish companies and public authorities operating in Ukraine and the Middle East will fall victim to destructive cyber attacks or the results of such attacks in the form of power outages and lack of Internet access.

Up to and since the invasion in 2022, Ukraine has been hit by several different types of destructive cyber attacks, ranging from very simple wiper attacks to more sophisticated attacks against satellite communication. The exact type and number of attacks against Ukraine remain unclear, just as the precise effects of the attacks are unknown.

The majority of the destructive cyber attacks that hit Ukraine during the first months of the war were limited in scope and did not spread beyond the Ukrainian border. This was, however, not the case with the cyber attack against US satellite communication provider Viasat. Even though the attack was likely meant to cripple Ukrainian communication, the consequences extended far beyond.

The attack against Viasat demonstrates that companies that are either physically present in or otherwise connected to Ukraine may feel the impact of destructive cyber attacks whose consequences spread to the companies' clients across borders. The same risk applies to attacks in which malware is deployed that spreads across units and machines.

Viasat was hit by a destructive cyber attack, which had consequences beyond Ukranian borders. Photo by: Mike Blake/Reuters/Ritzau Scanpix

Foreign states continue to develop destructive cyber attack capabilities

Foreign states continue to develop their capabilities to launch destructive cyber attacks at short notice. They use tools like cyber espionage to facilitate such attacks, for example in the event of an escalating crisis or full-blown war.

Cyber espionage may facilitate access to critical infrastructure, which states may try to destroy or disrupt in the event of a serious crisis or war. For instance, in April 2022, Ukrainian authorities averted a Russian destructive cyber attack aimed at cutting the power in parts of Ukraine. Several IT security companies have linked the attack to Russian hackers who, according to the IT security companies, had also previously directed their malware against industrial control systems in the Ukrainian energy sector.

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 customize malware and establish so-called backdoors into compromised systems to be used in subsequent destructive attacks.

In March 2022, US authorities issued a warning that Russian hackers who had previously employed the Triton malware were still actively targeting energy companies across the world. Triton is a destructive malware that affects industrial safety control systems, thus potentially also affecting the physical processes of energy production, etc. State-sponsored hacker groups have long shown an interest in the energy sector, including the Danish energy sector.

Cyber terrorism

The threat from cyber terrorism against Denmark is **NONE**, indicating that Danish authorities and companies are highly unlikely to fall victim to cyber terrorism attempts in 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 bodily harm or major disruptions of critical infrastructure.

The CFCS assesses that militant extremists have limited intention to launch cyber attacks whose impact is comparable to that of conventional terrorism, and that they do not have the required capabilities.

Despite the serious threat from conventional terrorism and the fact that militant extremists have used the Internet for years to support their existence, plan conventional terrorist attacks and launch simple activist cyber attacks such as DDoS attacks and website defacement, there have as yet not been any incidents in which terrorists have launched cyber attacks creating the same effects as conventional terrorist attacks.

Cyber-enabled influence operations

For the purposes of this threat assessment, the threat from cyber-enabled influence operations covers the threat from cyber attacks launched by foreign states aimed at swaying public opinion.

Foreign states' use of cyber attacks in support of influence operations is but one mean to influence public opinion and behaviour in other countries. Overall, influence operations cross both online and offline platforms and have manifested in different forms, from covert campaigns to open influence operations. CFCS does not assess other types of state-sponsored online influence activities.

Ghostwriter – a wide range of influence activities

One of the most extensive influence campaigns seen in recent years has been dubbed Ghostwriter. Ghostwriter covers a wide range of influence activities which have targeted audiences in Lithuania, Latvia, Poland and Germany. The actors behind Ghostwriter have leveraged tools such as website and social media compromises to push specific narratives. The CFCS assesses that state-sponsored hackers are behind some of the Ghostwriter activities.

Cyber-enabled influence operations pose an indirect threat to Denmark

Foreign states, including Russia, actively use cyber attacks to sway public opinion and behaviour in other countries. For instance, it is highly likely that Russia has used cyber attacks in support of influence operations against Ukraine in connection with its invasion of the country.

CFCS assesses that at present Denmark does not constitute a priority target for influence operations by foreign states that have the capabilities for cyber-enabled influence operations.

One of the most well-known examples of cyber-enabled influence operations is the hack and leak of the Democratic National Committee (DNC) in connection with the 2016 US presidential election. US authorities accused Russia of orchestrating the attack.

Though Denmark has not been directly exposed to this type of attack, cyber-enabled influence operations do pose an indirect threat to Denmark. Cyber attacks aimed at undermining trust in democratic values and weaken cohesion among allied countries and international organizations to which Denmark belong such as NATO could potentially have long-term political consequences, also for Denmark.

Danish organizations or individuals with links to countries exposed to a high volume of cyber-enabled influence operations, in particular the Baltic countries, Poland and Ukraine, may also be affected by attacks targeting audiences in these countries.

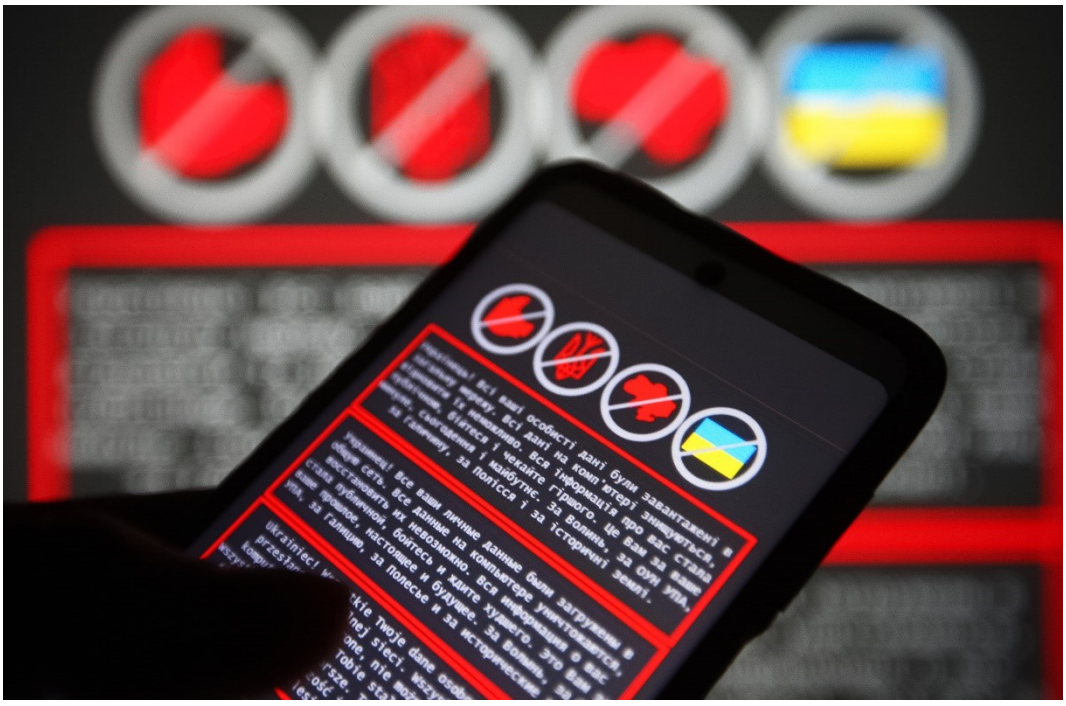
It is likely that cyber attacks are launched on a regular basis, including with the purpose of weakening cohesion within NATO. There have been several examples of attacks on the Baltic countries aimed at undermining support for NATO's presence in the region.

Ukraine has also been hit by a number of cyber attacks whose likely purpose was influencing and pressuring the Ukrainian population in connection with Russia's invasion of the country with the use of attack techniques that resemble those used by cyber activists.

For instance, several Ukrainian government websites have repeatedly fallen victim to defacement attacks during the course of 2022, prior to as well as after the invasion. On 14 January 2022, more than 70 Ukrainian government websites were defaced. The attack hit the Ukrainian Foreign and Energy Ministries, the Cabinet of Ministers, and the National Emergency Service. The defacement attack replaced the original content on the websites with a message in Ukrainian, Russian and Polish threatening to leak local citizens' personal data and warning them to expect much worse.

Within recent years, most cyber-enabled influence operations in Europe known to the CFCS have targeted audiences in Ukraine, Poland and the Baltic countries. The aim of these attacks has often been to derail public debate in a bid to promote polarization in the targeted societies.

Foreign states have repeatedly launched influence operations disguised as cyber activist campaigns, popularly known as faketivism. The purpose of faketivism is the same as that of other types of state-sponsored cyber-enabled influence operations.



Screenshot of the defacement attack that hit up to 70 ukrainian websites. Photo by: Pavlo Gonchar/Zuma/Ritzau Scanpix

Limited intention to launch influence operations against Denmark
At present, Denmark is likely not a priority target for influence operations carried out by states with the capacity to carry out cyber-enabled influence attacks.

The threat from influence operations emanates from state-sponsored hackers with significant capabilities. Russia is one of the states that has sophisticated cyber capabilities which it uses to launch cyber-enabled influence campaigns. Knowledge obtained through cyber espionage could be put into use in connection with potential future influence campaigns, for instance in connection with a potential future conflict of interest in the Arctic where Denmark and the Kingdom of Denmark would come to play a more prominent role vis-à-vis Russia.

Influence operations against the Kingdom of Denmark

An attempt at an influence operation against the Kingdom of Denmark is the incident in which a fake letter was sent from Greenland's then Minister of Foreign Affairs Ane Lone Bagger to US senator Tom Cotton in November 2019. The letter circulated online and mentioned Greenlandic-US cooperation, a future referendum in Greenland over independence, and a specific agreement on Greenland's status and US financial support. The aim was highly likely to cause a rift between the constituent countries of the Kingdom of Denmark and distrust between Denmark and the United States regarding the United States' intentions in the Arctic.

Foreign states go beyond cyber attacks in support of influence operations
Cyber attacks are but one of several tools available to foreign states in connection with influence campaigns. Foreign states also engage in influence activities that do not rely on cyber attacks. As an example, state actors offer citizens money, travels, etc. in return for the dissemination of disinformation. Another way for state actors to influence public opinion is to use fake profiles and bots on social media to promote specific messages – the purpose being to create an illusion of popular support or contempt for specific issues in accordance with the state actor's foreign policy goal.

Task Force Countering Influence Campaigns

In September 2017, the then Danish government set up an inter-ministerial task force comprising representatives from the Ministry of Justice (chairman), the Ministry of Foreign Affairs, the Danish Security Intelligence Service, and the Danish Defence Intelligence Service. Its task is to coordinate Denmark's efforts against state-sponsored influence campaigns and to ensure an effective and coordinated response at authority level.

The Task Force Countering Influence Campaigns defines influence operations against Denmark as state-sponsored actors' open or hidden activities aimed at swaying public opinion in Denmark and the world's view of Denmark in an attempt to promote their own interests at the expense of Danish interests. However, it is important to add that influence activities against Denmark's allies and against international organizations such as NATO and the EU may, by extension, also harm Danish interests.

Trends and tendencies

This section deals with trends and tendencies that have or are expected to have an impact on the cyber threat against Denmark.

The digital concentration affects cyber security
IT and the Internet have had a great impact on all our lives, and the development of the Internet has greatly influenced security and the availability of online services on which we have come to depend. This section describes developments that have an impact on the cyber threat and the potential consequences of a cyber attack against one of the major companies that supports the functionality of the Internet.

Today's Internet is dominated by fewer yet bigger tech companies
Since the infancy of the Internet in the 1960s, the world has witnessed not only significant technological advances but also increasing consolidation of the Internet to a handful of large tech companies that have become responsible for delivering and controlling a growing part of the Internet's infrastructure and the software on which many Danish companies and authorities rely.

On the positive side, using the large providers of software, data centres, cloud computing services, and Internet infrastructure often improves the IT security level of the customer organizations. The reason for this is that large tech companies generally use more resources and have more expertise than smaller organizations when it comes to monitoring and securing their infrastructure and services against hackers.

However, as a result of the consolidation, the consequences of a cyber attack targeting one of these large providers or some of their products may affect multiple customers across the world simultaneously. Consequently, a security incident with a single provider may not only have a negative impact on the individual customer and user of the Internet but on society as a whole, including in several countries at once.

The rise of digitalization allows hackers access to multiple victims in one go
As a result of globalization and technological developments, a relatively small number of suppliers dominate the global IT landscape. The spread of certain technologies which are quickly becoming dominant within their respective fields creates a self-perpetuating effect where a growing share of technology and Internet services are left in the hands of a few very large companies.

For instance, today most companies use Microsoft Windows software in their administrative network. This may be an advantage as a large global supplier like Microsoft is able to dedicate many resources to securing its products against hackers. However, the widespread use of Windows also means that hackers only have to develop techniques, malware and exploits that target Windows in order to gain access to a large number of victims in one go. This security challenge not only applies to actual software products but also to the many functions that are featured across software products from different suppliers. A case in point was the serious vulnerability detected and exploited in the so-called Log4j code in November 2021.

Vulnerability in Log4j code leveraged against victims across the world

In November 2021, a serious vulnerability was detected in the Log4j code, which is used to log security incidents within applications and on websites.

The vulnerability can be used as a gateway to deploy malicious code to the unit or server in which the Log4j code is used. The vulnerability is easy to exploit, and in addition the Log4j code is featured in many applications from many different suppliers and is thus used on millions of servers worldwide. As a result, hackers are able to attack multiple servers across the world by using a single attack technique exploiting the vulnerability. This has resulted in a global race between hackers trying to exploit the vulnerability and organizations trying to patch their vulnerable systems.

Company production, email and digital office tools have moved to the cloud

80 percent of all Danish companies with more than 100 employees use cloud computing, with many companies having their email systems and digital office tools provided by a single cloud provider. The use of cloud computing offers a simple and flexible solution for many organizations, but it also means that Internet errors can make it difficult to do your job. In Denmark, Microsoft is the main provider of cloud-based email systems and digital office tools to companies. A breakdown or error in Microsoft's cloud solution may thus affect many large companies in Denmark.

The US companies Amazon, Microsoft and Google dominate the European cloud computing market. Combined, the three companies account for approx. two-thirds of the cloud computing market in Europe. As a result, Internet services and production in many European, including Danish, companies may be cut off or disrupted by a technical error or a cyber attack against the cloud infrastructure of one of these service providers. The consequences may be severe if an outage suffered by a cloud provider affects companies in a critical sector.

Amazon outage affected companies across the world

On 7 December 2021, Amazon Web Services, the world's biggest cloud provider, suffered a major outage that took down the websites of a wide range of major Internet-based companies. The outage affected Netflix, Disney+, Amazon.com, Amazon Prime and a large number of other services.

Content Delivery Networks are critical to the functioning of the Internet

Previously, data between a user and an Internet service was transferred directly between the user's computer and the provider's web server. Today, so-called Content Delivery Networks (CDN) are responsible for 60-70 per cent of all Internet traffic.

CDN providers run transmissions systems and servers worldwide. They are used to minimize latency and optimize speed for internet services by continually copying website content to proxy servers across the world located closer to the end users. Even though there are many CDN providers, most of the CDN data traffic is concentrated with a handful of providers. These providers have become crucial to the functioning of the Internet.

Errors with CDN providers disrupted Internet services also in Denmark

On 8 June 2021, CDN provider Fastly experienced an hourlong global outage caused by a software error in their servers. As a result of the outage, the connection to Internet services and websites was cut across the world. In Denmark, for instance, the website of the Danish TV station TV2 was affected.

On 22 July 2021, a software update triggered an error in the DNS system with the CDN provider Akamai. The error caused a disruption that lasted for up to an hour and impacted availability of some customer websites and Internet services, including those of several banks.

Website access control may be transferred overseas

A recent example of the development of the Internet, which may have a serious impact on security, concerns perhaps the most central function of the Internet called Domain Name System (DNS). DNS acts as the phonebook of the Internet by translating domain names into IP addresses to which the user's computer can connect. Without DNS, the Internet does not work.

Today, a user's Internet provider is typically responsible for translating domain names into IP addresses. However several popular browsers, including Google Chrome, Microsoft Edge and Mozilla Firefox, have been added an optional function capable of encrypting DNS traffic and sending it to another company, for example overseas.

For now, the popular browsers have been coded to use the Internet provider's DNS server as a standard in Denmark. However, the browser provider may choose to change that by updating the browser. In the United States, Mozilla Firefox by default sends all user DNS queries to US third-party provider Cloudflare by default.

In the future, if DNS queries are sent to third-party DNS servers overseas, data and the control of access to websites, including Danish ones, will be transferred to the overseas DNS provider as well. A potential consequence could be poorer security, as any blocking of illegal, harmfull or malicious websites, ruled by a Danish court and enforced by Danish Internet providers will be bypassed. This would also apply to the website blocking that took place during the corona pandemic where criminal hackers tried to exploit the crisis to steal information and money from Danish citizens.

Another consequence may be that potential disruptions due to errors or hacker activity on the foreign third-party DNS service could lead to loss of Internet access across the world.

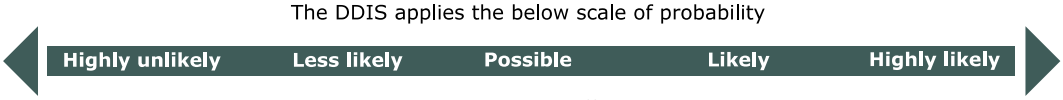
Threat levels

Definition of threat levels

The DDIS uses the following threat levels, ranging from **NONE** to **VERY HIGH**.

NONE	No indications of a threat. No acknowledged capacity or intent to carry out attacks. Attacks/harmful activities are unlikely.
LOW	A potential threat exists. Limited capacity and/or intent to carry out attacks. Attacks/harmful activities are not likely.
MEDIUM	A general threat exists. Capacity and/or intent to attack and possible planning. Attacks/harmful activities are possible.
HIGH	An acknowledged threat exists. Capacity and intent to carry out attacks and planning. Attacks/harmful activities are likely.
VERY HIGH	A specific threat exists. Capacity, intent to attack, planning and possible execution. Attacks/harmful activities are very likely.

The DDIS applies the below scale of probability



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