CENTRE FOR CYBER SECURITY

Threat assessment:

The cyber threat against Denmark 2023

1st edition, May 2023.

Table of contents

CENTRE FOR CYBER SECURITY

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

1st edition, May 2023.

The cyber threat against Denmark 2023

The purpose of this threat assessment is to inform decision-makers of 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 the cyber security risk assessment efforts of public authorities and private companies.

Key assessment

- The threat of cyber espionage against Denmark is **VERY HIGH**. While matters of security and foreign politics, such as the Arctic, NATO and the EU, are of particular interest to cyber espionage threat actors, critical infrastructure is also a target of espionage.

- Cyber espionage undermines Danish political, economic and security interests. It is likely that foreign states use cyber espionage in preparation for destructive cyber attacks.

- The threat of cyber crime against Denmark remains **VERY HIGH**. Well-organized ransomware groups target all levels of society.

- The CFCS assesses that the majority of cyber criminals are financially motivated, opportunistic and independently operating non-state actors.

- The threat of cyber activism against Denmark is **HIGH**, making it likely that Danish private companies and public authorities will fall victim to cyber activist attacks in the short term. Pro-Russian cyber activists are very active against NATO countries, including against Denmark, and they have developed a formalized attack method and bolstered their capabilities.

- The threat of destructive cyber attacks is **LOW**. It is less likely that foreign states currently harbour intentions to conduct destructive cyber attacks against Denmark. However, the CFCS assesses that hacker groups affiliated with foreign states are preparing themselves to be able to conduct destructive cyber attacks at short notice.

- Danish organizations that are active in Ukraine or delivering products or services related to the war in Ukraine could be more at risk of falling victim to a destructive cyber attack or becoming collateral victims of destructive cyber attacks targeting Ukraine.

- The threat of cyber terrorism is **NONE**. Militant extremists have limited intent to conduct cyber terrorism and do not have the capabilities required to launch cyber attacks that create the same devastating effects as conventional terrorism.

Introduction

Europe and the rest of the world are facing a new security reality as a result of Russia's invasion of Ukraine. The war could drag on for years and will shape relations between Russia and the West, including Denmark. It is against this backdrop that we need to understand the current threat landscape – including in the digital domain.

The threat landscape is constantly evolving, and while most cyber attacks are not linked to the situation in Ukraine, it is through this lens that many people now understand the world. When, for example, the Danish island of Bornholm experiences power outages or when other critical functions are disrupted, the population needs to know whether it was an accident or a deliberate act.

In the case of an actual cyber attack, the need arises to identify the perpetrators behind the attacks. Is it a case of greedy criminals or has a foreign state singled Denmark out as a cyber target?

Threat assessments prepared by the CFCS are divided into categories addressing different types of cyber attacks, including cyber espionage, cyber crime, cyber activism, destructive cyber attacks and cyber terrorism. Our aim is to determine the motivation and the type of threat actor behind any given cyber attack. For instance, we assess that cyber crime is often perpetrated by individuals or groups that are opportunistic and motivated by financial rewards – and not operating at the behest of a state. Even though ransomware attacks also target critical infrastructure, they are not necessarily orchestrated by the Russian state. Danish critical infrastructure companies often have characteristics that could make them attractive targets for cyber criminals.

Similarly, we assess that the wave of DDoS attacks targeting both Danish and European targets over the past few years was launched by activist hacker groups in a move to express their political views. Pro-Russian hackers have been particularly active in 2022 and early 2023.

It is not always easy to determine the motivation behind a cyber attack, just as an attack is often multifaceted. Criminals may pursue political agendas affecting their target selection, or they may be loosely affiliated with states pointing them in a certain direction. Also, activist hackers may be short of money, prompting them to put their technical skills to use for economic gains.

Even though the challenge is far from new, the need to understand the threats facing Denmark is more urgent than ever. The current security situation has increased the need to determine whether a cyber attack is perpetrated by criminal groups or a foreign state.

The threat level for cyber activism has been raised to HIGH, while the other levels remain unchanged

Even though the impact of the war in Ukraine has been deep, most of the threat levels in this year's threat assessment remain at the same level as last year. However, that does not necessarily mean that the threat is unchanged. Cyber threats develop constantly, following developments within geopolitics, technology, etc.

The CFCS assesses that the threat of cyber espionage is still **VERY HIGH.** Danish public authorities and private companies are highly likely to fall victim to cyber espionage attempts within the next two years. Russia and China, in particular, are known for using cyber attacks to gain access to knowledge, primarily on matters of Danish security and foreign politics.

Similarly, the threat of cyber crime is **VERY HIGH**. Anyone can fall victim to cyber crime, and we assess that cyber criminals motivated by financial gain are often well-organized and adept at overcoming government security measures.

The threat level of cyber activism is **HIGH** – its highest level since the CFCS published its first annual cyber threat assessment in 2016. The threat can be directly linked to the war in Ukraine and the numerous pro-Russian hackers who have taken to their keyboards to show their support for Russia, repeatedly targeting Danish victims. The development also means that targets in Denmark are now likely to fall victim to cyber activist attacks, in particular DDoS attacks. It does not mean, however, that the consequences of cyber activist attacks have grown more serious.

The threat of destructive cyber attacks is **LOW**. We still assess that Danish public authorities and private companies are less likely to fall victim to destructive cyber attacks. However, it is likely that state-sponsored hacker groups are developing the capability to launch destructive cyber attacks against critical infrastructure in Denmark. As several states have destructive cyber capabilities, the threat very much depends on the intention of these states. Consequently, the threat to Denmark could change with little or no warning.

Finally, the threat of cyber terrorism remains **NONE**. Cyber terrorism is defined as cyber attacks aimed at creating effects similar to those of conventional terrorist attacks. The threat level has been set at **NONE** for several consecutive years. However, the CFCS closely monitors developments in the threat of cyber terrorism, as the Centre for Terror Analysis under the Danish Security and Intelligence Service (PET) assesses that there is a significant threat of conventional terrorism.

The CFCS uses the Danish Defence Intelligence Service’s threat levels and probability degrees explained at the end of the threat 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 of cyber espionage to Denmark is still **VERY HIGH**. Danish public authorities and private companies are highly likely to fall victim to cyber espionage within the next two years.

Foreign states continually attempt to compromise Danish private companies and public authorities to steal information. Foreign states primarily conduct cyber espionage against Denmark in order to gain access to information on matters of security and foreign policy and on the Danish Defence. It is likely that Denmark is a target of politically motivated cyber espionage as a result of its membership of NATO and the EU. Denmark's geographical location and role in the Arctic also adds to the threat of cyber espionage from foreign states.

In addition to politically motivated cyber espionage, foreign states also conduct cyber espionage aimed at promoting their economic interests and at gaining access to information in support of technological advances. Successful cyber espionage attacks undermine Danish political and economic interests.

Finally, the CFCS assesses that cyber espionage is a prerequisite for destructive cyber attacks. Consequently, it is likely that foreign states that conduct cyber espionage campaigns against Denmark could also use the insights they gain to prepare future destructive cyber attacks.

Russia and China are trying to steal information on Danish defence and foreign policy issues

The main threat of cyber espionage emanates from Russia and China. Both states have significant cyber capabilities which they use to compromise victims across the world, including in Denmark.

Russia and China, in particular, are interested in gaining access to information on matters of security and foreign policy as well as Danish defence capabilities, including equipment and personnel. Information on military and dual-use technology as well as Danish research is also at risk of cyber espionage.

Cyber espionage motivated by military interests could also impact critical sectors that are either currently supporting or likely to provide future support to the Danish armed forces. Sectors of interests include transport, energy, research and shipping.

In addition, it is likely that organizations with an indirect or less obvious connection to the defence, or security and foreign policy realm could become targets of politically motivated cyber espionage, including Danish private companies, public authorities, research institutions, NGOs and think tanks. Such organizations could become targets if they are perceived by adversaries as supporting Danish defence or foreign policy, for instance by providing services, information or products to Danish actors operating within these areas.

In addition to organizations which in one way or another could be linked to Danish foreign and defence policy, private companies and public authorities providing services to several sectors and authorities are also facing a threat. For instance, cyber espionage could be used against companies delivering IT services across sectors and organizations. Suppliers could also be used as stepping stones for cyber espionage attacks.

Foreign states are, for instance, trying to gain access to information by means of exfiltration of emails from compromised organizations. Besides the content of the individual emails, compromised email systems could also allow foreign states insight into the different forms of cooperation between Danish private companies and public authorities. This information could be used to launch new attacks on other victims, etc.

Foreign states conduct both targeted and broad espionage against Denmark
The CFCS assesses that Denmark is a target of cyber espionage at the same level as other NATO and EU countries. This is due to the general interest of foreign states in security and foreign policy issues and an interest in the West's view on international agendas, conflicts and events.

In addition, certain circumstances make Denmark a cyber espionage target. For instance, it is likely that Denmark's geographical location in the Baltic Sea and close to the Baltic countries contributes to the threat of cyber espionage, especially from Russia.

In addition, both Russia and China have strong interests related to the Arctic. Cyber espionage is a means for both countries to increase their latitude and interests in the Arctic, potentially at the expense of Greenland, Faroese and Danish interests.

Cyber espionage against Greenlandic targets affected public services for citizens

Greenland targets are regularly exposed to cyber espionage attempts. For instance, on 25 March 2022, Naalakkersuisut's Digitization Agency detected a security breach in the central administration. To mitigate the breach, communication going in and out of Greenland via the administration's servers was shut down, cutting off the access to websites through the secure login solution NemID and delaying the payment of social benefits and bills. Head of Naalakkersuisut Múte B. Egede said to Greenland media outlets that the incident was caused by a cyber espionage attack.

States conduct cyber espionage to promote their own interests
Foreign states use cyber espionage to promote national security and international and bilateral interests. Both Russia and China use cyber espionage to gain access to different kinds of information that could be harnessed to challenge Western norms and strenghten their respective international influence. Cyber espionage could, for instance, allow foreign states insight into Denmark's negotiation positions and foreign policy agenda.

Cyber espionage is used strategically to garner information over time and tactically to gain more specific knowledge on concrete events or areas.

In addition to Russia and China, a number of regional actors in Asia, the Middle East and Latin America conduct cyber espionage. These actors mainly use their capabilities against rival states in their neighbouring areas. Like China, some of them also monitor individuals and organizations that are critical of the regime or otherwise considered a threat.

States also conduct espionage to promote economic and technological interests

The CFCS assesses that foreign states also conduct cyber espionage against Danish targets to promote their own economic interests and technological development objectives. Espionage for financial gain could aversely affect Danish private companies and public authorities in connection with larger tender rounds, to name but one consequence. Research, technology and innovation-related organizations also fall victim to cyber espionage for finacial gain.

States conduct espionage against leading companies

Cyber espionage for fiancial gain could, for instance, be directed against Danish companies that are at the cutting edge internationally. For instance, in 2020, a number of foreign states targeted international pharmaceutical companies that were developing COVID-19 vaccines.

Cyber espionage against critical sectors will grow increasingly common in the future

It is likely that the threat of cyber espionage against critical sectors will increase in the future. International politics are becoming characterized by growing competition and opposition. Decisions that were previously regarded asentirely within civilian, technical or financial realms are now matters of national and international security. This includes fields such as supply chains, energy and technological developments.

Cyber espionage actors also launch other types of cyber attacks

The threat of cyber espionage is complex, as cyber attacks that are primarily aimed at gaining information could also open the door to other types of cyber threats. For example, hackers who conduct cyber espionage could also use their access to compromised systems to launch other types of cyber attacks later on.

To illustrate, there have been several examples of state-sponsored cyber espionage haking groups launching other types of attacks abroad such as destructive cyber attacks and cyber-enabled influence operations.

According to Microsoft, a state-sponsored hacker group has been engaged in cyber espionage, destructive cyber attacks and cyber-enabled influence operations against targets in Ukraine. Microsoft has dubbed the group DEV-0586 and describes how hackers from DEV-0586 have conducted cyber espionage against Ukrainian targets and also destructive wiper attacks and defacement attacks against Ukrainian websites.

Cyber crime

The threat of cyber crime against Danish public authorities and private companies is still **VERY HIGH**. Cyber crime is the most prevalent cyber threat to Denmark and dominates the threat landscape and affects our everyday lives. The threat will continue to have serious consequences for private companies, public authorities and ordinary citizens, for instance in the form of service disruptions and financial losses.

The CFCS uses the term cyber crime collectively to describe actions where hackers use cyber attacks to commit crime for financial gain.

What is a ransomware attack?

Ransomware attacks involve attempts by criminals to extort public authorities or private companies by rendering their data and systems unavailable, often through encryption. The criminals typically demand ransom payment in cryptocurrency in exchange for the decryption key needed to restore the data and systems. The criminals also often threaten to leak stolen information unless the ransom is paid.

Cyber criminals are a threat to all aspects of society

Anyone can find themselves in the crosshairs of cyber criminals. Some ransomware operators deliberately target critical infrastructure with the aim of causing serious operational disruptions in an attempt to ramp up the pressure on companies and authorities to pay a high ransom. Other hackers deliberately steer clear of attacking critical infrastructure, likely in the hope of avoiding government attention.

Another factor that determines how ransomware operators choose their targets is the financial position of the potential victims. The higher the company turnover, the higher the potential ransom demand.

Small and medium-sized businesses, however, are not immune to the threat of ransomware. Opportunistic cyber criminals target victims that are easy to compromise. As small businesses are not necessarily as concerned about cyber security, they potentially become easy targets for cyber criminals.

An ordinary workplace… with modifications

It is highly likely that Danish private companies and public authorities will continue to fall victim to frequent cyber crime attempts. The cyber criminal community is robust and made up of groups and individuals cooperating and trading with each other across borders.

The organized cooperation between cyber criminals has several negative consequences for their potential victims. Cooperation bolsters the capabilities of the cyber criminals, as they get the opportunity to specialize and streamline their attacks. Cross-border cooperation also contributes to making the cyber criminal

community robust and resilient against attempts by individual countries at deterring or punishing the criminals.

Skilful ransomware operator teaches other criminals

In 2021 and again in 2022, a cyber criminal group known as Conti suffered a data breach that revealed internal chat messages and step-by-step guidelines to ransomware attacks. These guidelines have likely been used to assist and train other hackers affiliated with the group – also known as affiliates. The instructions were precise and user-friendly enough to enable less tech-savvy hackers to launch relatively advanced ransomware attacks.

Conti was a very active ransomware group that was responsible for numerous serious attacks worldwide. Conti shut down most of its infrastructure in the spring of 2022.

Some cyber criminal groups are making efforts to organize in ways that mirror traditional companies as evidenced by the data breach suffered by the cyber criminal hacker group Conti. Internal chat messages revealed that Conti was made up of several departments with different areas of responsibility and their own distinct budgets. It also revealed that Conti made regular salary payments to some 80 employees, regularly recruited new employees on online forums, and that its internal structure was a classic organizational hierarchy.

Much of the trade and cooperation between cyber criminals take place on Russian-language online forums. However, that does not mean that all members on the forums are Russians or Russian residents. Cyber criminals reside all over the world.

Photo: Andre M. Chang/Zuma/Ritzau Scanpix

Cyber crime has no boundaries

Cyber criminals can be found anywhere in the world and use it-infrastructure that spans several countries. However, cross-state cooperation could make cyber criminal activities more difficult. In January 2023, infrastructure associated with the Hive ransomware group was seized as part of a coordinated law enforcement effort involving several countries. For instance, the FBI took over the group's web leak site.

Connections between cyber criminals and states

The CFCS assesses that most cyber criminals are financially motivated, opportunistic in nature and non-state affiliated.

However, it is likely that links exist between some foreign states and cyber criminals with varying degrees of formalization and closeness. In this context, North Korea stands out as a special example of very close and formalized cooperation. Here, state-sponsored hacker groups likely commit cyber crime in order to acquire funds for the state.

It is likely that some foreign states have recruited cyber criminals to conduct cyber espionage. The CFCS assesses that when media outlets and IT security companies hint at links between the Russian state and cyber criminals, it is often a case of Russia tasking cyber criminals to conduct espionage-focused cyber activity.

Recruitment of cyber criminals may serve multiple purposes. Firstly, it is a relatively easy way to increase the state's cyber capabilities. Secondly, it may provide the state with the opportunity to condemn cyber attacks launched by actors that are not officially affiliated with the state itself.

It is also highly likely that some foreign states exploit the cyber criminal community to obtain malware, for instance malware sold on online cyber criminal trading forums. Consequently, the cyber criminals do not necessarily know that they are cooperating with or selling to a state actor. Just as recruitment of cyber criminals is a means for states to expand their cyber capabilities, so is the acquisition of malware sold on cyber criminal forums. And again, states are able to sow confusion by launching attacks under disguise of being cyber criminals.

Russian FSB officers accused of paying cyber criminals to hack Yahoo

In 2017, US authorities indicted two officers from the Russian Federal Security Service, FSB, for hiring two criminal hackers, a Russian national and a Canadian citizen born in Kazakhstan, to steal sensitive information.

According to the indictment, the FSB officers, of whom one had a history of committing cyber crimes according to open sources, paid the criminals to hack into Yahoo's network as well as Yahoo and Google email accounts.

According to the US authorities, the hackers shared information from select email accounts with the FSB officers, including information from the email accounts of Russian anti-government journalists and data from US companies, officials and diplomats.

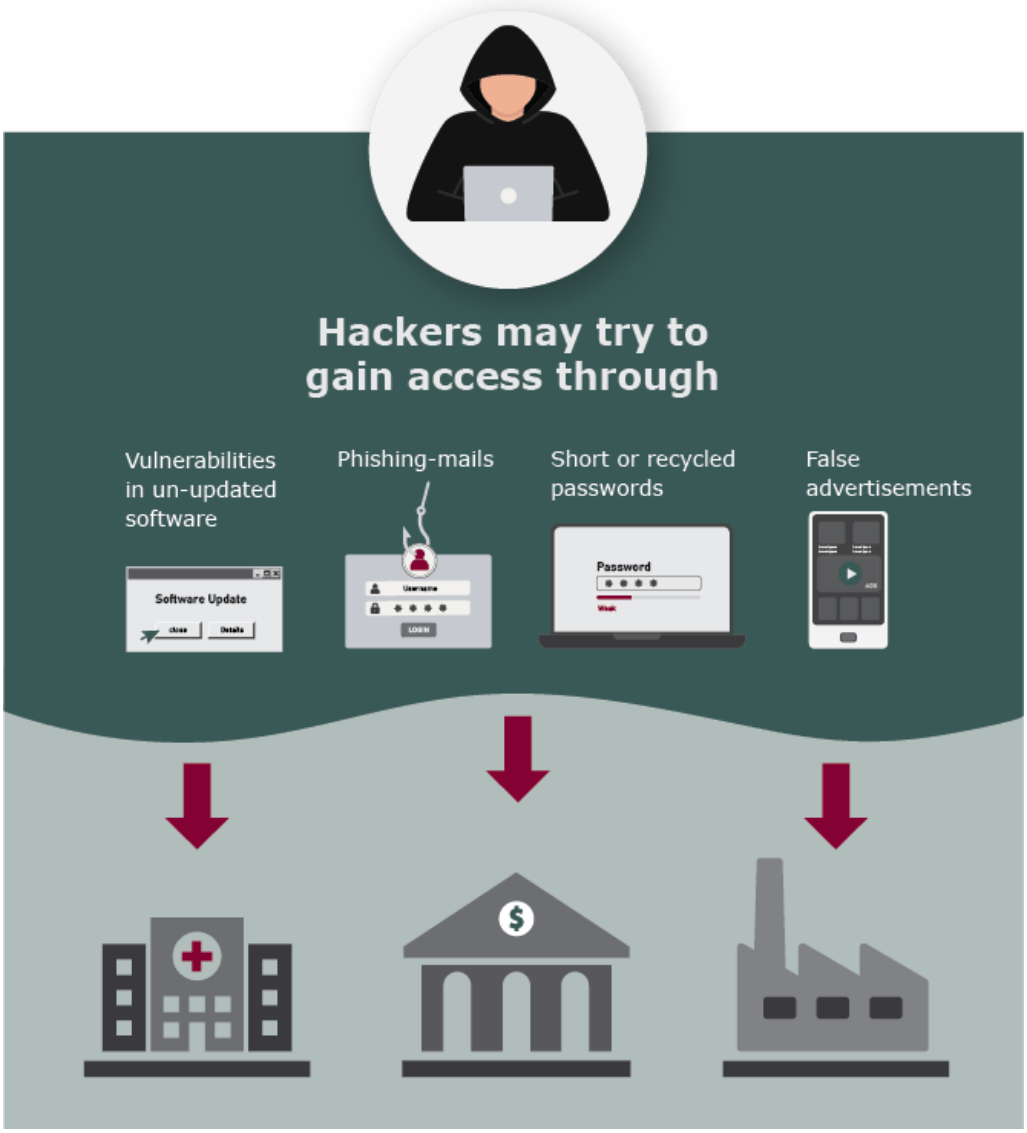
At the same time, the Russian hacker enriched himself by stealing credit card information and gift cards from the compromised email accounts. According to the indictment, the FSB officers helped him avoid arrest.

The Canadian hacker was arrested and extradited to the United States where he pleaded guilty. In 2018, he was sentenced to five years' imprisonment.

Another aspect of the relations between states and cyber criminals is whether states do enough to fight cyber criminals in their respective countries or deliberately avoid intervening as long as the cyber criminals primarily target foreign countries. The United States has accused Russia and China of, on several occasions, having turned a blind eye to activities by cyber criminal actors despite being aware of their identities and actions.

Criminals also extort without encrypting data

While data encryption attacks have caught a lot of attention in recent years, cyber criminals also extort private companies and public authorities without encrypting any data. Some criminals steal data from private companies, threatening to leak or sell the stolen information unless a ransom is paid. Even though this type of attack does not affect operations to the same extent as data encryption attacks, the victim may still suffer severe consequences. In addition to the immediate consequences, such as potential GDPR fines, reputational damage and loss of clients and market value, the attacks may have long-term consequences if any trade secrets are disclosed.



Some cyber criminals specialize in gaining access to systems, selling this access to other hackers. This allows them to spend all their time and resources on gaining access before quickly moving on to the next victim. The buyers could, for instance, use the acquired access to launch ransomware attacks.

Actors engaged in this type of extortion use many of the same techniques as ransomware operators in terms of putting pressure on the victims to pay. For instance, criminals post the names of their victims on so-called "Dedicated Leak Sites". IT security companies have described several examples from abroad where cyber criminals have contacted the employees or clients of the victim about the stolen information. In other cases, criminals try to make the stolen information easily accessible through ordinary internet searches.

BEC scams still result in large financial losses

Business Email Compromise (BEC) is still a widespread type of cyber crime scam that can be very costly to the victim. BEC scams involve criminals trying to defraud private companies and organizations of funds through fake money transfer requests. In some cases, cyber criminals compromise a legitimate company email account or email accounts of company cooperation partners, subsequently luring the employees into wiring funds to fraudulent accounts. The criminals may send fake invoices or falsify information on legitimate invoices. The possibilities of defrauding organizations and individuals through compromised emails are bounded only by the limits of the criminals' imagination.

Municipality defrauded of DKK 277,000

In July 2022, the municipality of Næstved was defrauded of DKK 277,000. The email account of a city council employee had been hacked and was used to send fake invoices to a financial officer working with the municipality. The hacker had gained access to the employee's email through a phishing email sent from a local electrician that had also been compromised by the hacker. The employee had previously been in contact with the electrician and thus did not suspect any foul play. Detecting phishing emails may prove a particular difficult task, especially if the cyber criminals insert themselves into existing and legitimate business conversations, a tactic also known as email thread hijacking.

Criminal hackers engage in BEC scams in order to make a quick and easy profit. Oftentimes, cyber criminals do not even have to compromise an email account. All they have to do is make an email sent to the victim appear legitimate. For instance, they can set up an email account that mimics a legitimate email address from the recipient's workplace. Cyber criminals can also use information on the company or authority and their employees to make the fraudulent emails appear convincing.

There is a digital arms race with organizations trying to protect their business against cyber criminals – for example BEC scammers – and the cyber criminals developing new tools to bypass these security measures. The criminals are creative and cooperate to ensure their attacks are successful.

Cyber activism

The threat of cyber activism against Denmark is **HIGH**. The CFCS raised the threat level from **MEDIUM** to **HIGH** in January 2023.

Danish private companies and public authorities are likely to become targets of activist cyber attacks in the short term. The CFCS raised the threat level of cyber activism based on the high level of activity among pro-Russian activist hacker groups against NATO countries, including Denmark, as well as their more formalized attack methods and increased capabilities.

Cyber activism is carried out by individuals and groups that use cyber attacks to attract maximum attention to their agendas or to punish organizations that are perceived as adversaries to their causes. Cyber activists – or hacktivists - are typically driven by ideological or political motives, ranging from political single-issues to opposition against those in power.

The DDoS attacks that have targeted Denmark often follow the same blueprint.

Pro-Russian hackers hit targets in Denmark
Danish organizations will likely also fall victim to hacktivist attacks in the future. The surge in pro-Russian cyber activist attacks against targets in Europe and NATO countries triggered by the growing tensions between Russia and the West is a key contributor to the current threat landscape facing Denmark. Conversely, the threat posed by Danish cyber activist environments continues to be very limited.

Danish Defence websites were targeted in activist DDoS campaigns

A pro-Russian cyber activist hacker group was likely behind DDoS attacks launched on 8 December 2022 against several websites belonging to the Danish Ministry of Defence. The group is one of many pro-Russian groups to have launched DDoS attacks against targets in European NATO countries since Russia's invasion of Ukraine in February 2022.

The group most often targets public authorities. Ahead of attacks, the group calls on its followers on Telegram to participate in joint DDoS attacks against designated targets. The group provides tools and target lists to followers wanting to participate in the attacks.

Sometimes cyber activists attack targets that they consider anti-Russian or symbolic of the support provided by foreign countries to Ukraine. Over the past year, pro-Russian cyber activists have more or less constantly conducted hacktivist campaigns, grouping their targets under specific themes that are either country-specific or extend across multiple countries. In both cases, the designated theme could be sector-specific. The hackers have focused on authorities and companies in the transport, financial and defence sectors. Danish targets have been hit in different types of campaigns, including an attack targeting European ministries of defence, and one targeting the Danish financial sector.

Cyber activists pose a threat to Danish companies and authorities

Pro-Russian hackers regularly launch attacks on critical sectors in Western countries. It is likely that Danish targets are at risk of new compromises, in particular if Denmark were to fall into the crosshairs of pro-Russian hacker groups, for instance when enforcing sanctions on Russia or providing military support to Ukraine.

Cyber activists hit back

Activist hackers also launch retaliatory attacks against authorities and companies in countries that enforce the sanctions imposed on Russia. In many cases, the hackers direct their attacks against organizations working within the same sectors as their sanctioned Russian counterparts.

In June 2022, a pro-Russian cyber activist hacker group used its Telegram channel to call for attacks on Lithuanian infrastructure in retaliation for Lithuania's enforcement of restrictions on rail transport of goods to Kaliningrad. Similarly, a pro-Russian activist hacker group launched a DDoS attack against a Finnish military academy in response to Finland's military training of Ukrainian soldiers. Germany and Latvia too have been targets of retaliatory attacks by pro-Russian cyber activists.

Attacks by pro-Russian cyber activists are, for instance, directed against sectors affiliated with the defence establishment such as logistics companies working with transport of equipment, etc. An example of this was the October 2022 DDoS attack by a pro-Russian activist group against airports, marine terminals and logistics companies in the United States. Prior to the attack, the group had posted a list of targets on their Telegram channel, calling on their followers to generate traffic on the websites belonging to these targets to render them inaccessible.

In the first months of the war, cyber activists on both the pro-Ukrainian and the pro-Russian side of the conflict constituted a threat to Denmark. After the outbreak of the war, many cyber activist attacks were also waged against Russia or foreign companies designated as Russian friendly by pro-Ukrainian hackers. While pro-Ukrainian cyber activists are still active, the biggest threat to Denmark emanates from pro-Russian cyber activists.

The cyber activist landscape is complex

Even though cyber activists are not state actors but act on their own initiative, links may exist between some activists and different national authorities. The possible affiliation between cyber activists and foreign states and the frequency in cyber activist attacks across national borders combine to create a grey zone that has the potential for conflicts to spread and intensify. This could happen if, for example, the attacks have a devastating effect or disrupt critical infrastructure. Prior to Russia's invasion of Ukraine, the number of activist cyber attacks were on the decline, but the war has generated strong activity in parts of the activist environment.

During the course of the war, activist hackers have launched attacks with the purpose of intensifying the consequences of conventional attacks. As an example of this, a pro-Russian hacker group launched a DDoS attack against a Ukrainian online seller of emergency generators. The attack came in the wake of Russian missile attacks against power stations and was intended to prevent private citizens in Ukraine from buying power generators for home use. Another example is an activist attack reportedly carried out by a pro-Ukrainian hacker group on the rail system in Belarus. The attack interrupted the signal systems, necessitating a switch to manual control mode. The aim of the attack was likely to disrupt the transport of Russian troops and equipment to Belarus prior to the invasion of Ukraine.

DDoS attacks are the weapon of choice for activists

DDoS attacks are the preferred weapon for cyber activist hackers, as they have the dual advantage of not requiring advanced technical skills while at the same time attracting attention to the activist agenda. While DDoS attacks disrupt operations, they do not have lasting or destructive consequences to the victim's systems.

The growing support for activist attacks has added new members to the groups that make their resources available as botnets that can be used for DDoS attacks. The pooling of resources made possible when new members join the groups can increase the strength of the DDoS attacks and make them harder to mitigate.

In addition to launching DDoS attacks, a number of pro-Russian hacktivists are also involved in the execution and promotion of information campaigns. These groups use manipulated or fabricated information to shape the mindset of certain communities in an effort to promote Russia's strategic interests. In information operations, hack and leak attacks can help bolster the effect of the campaign.

Pro-Russian groups have also launched attacks using tactics that are most often associated with other kinds of actors. For instance, an activist group has launched ransomware attacks against Western targets, encrypting user data, as would be the case in a financially motivated attack.

However, instead of leaving a ransom note, the hackers leave a link to a pro-Russian Telegram channel containing propaganda posts.

Other times, activist hackers use defacement attacks, altering the visual appearance of the victim's website, for instance by posting a new text or picture on the front page of the website. Both pro-Russian and pro-Ukrainian hackers have used this type of attack, with the latter using it mainly to spread information on Russia's invasion of Ukraine to the Russian population.

Cyber activists use social media to call for attacks

Cyber activism is typically driven by ideological or political motives. The war in Ukraine has seen the emergence of activist environments that use the Russian-developed messaging app Telegram as a platform to coordinate and call for activist cyber attacks.

The pro-Russian hacker groups are part of a volatile online environment where groups continuously emerge, vary in activity level over time and, in some cases, ultimately vanish. While the attacks by pro-Russian cyber activists are based on a common anti-Western agenda, they do not necessarily coordinate their activities across the different groups.

The CFCS assesses that pro-Russian hackers are also motivated by media spotlight. Hackers continuously follow the media's coverage of their attacks, sharing any mention with their followers, etc. Competition is also rife among the different pro-Russian hacker groups, which is evident for instance by their insistence that the media and other hacker groups unambiguously attribute the attacks to the rightful perpetrator. Extensive media coverage of cyber activist attacks against Danish targets could thus contribute to making Denmark a more attractive target for pro-Russian cyber activists.

The pro-Russian activist groups will likely keep their motivation to attack targets in the West, including in Denmark, for the duration of the current crisis between Russia and the West.

Destructive cyber attacks

The CFCS assesses that the threat of destructive cyber attacks against Denmark is still at the level **LOW**. Danish companies and authorities are less likely to become the targets of destructive cyber attacks in the short term.

It is likely, however, that state-sponsored hacker groups are preparing to launch destructive cyber attacks against critical infrastructure in Denmark. The threat to Denmark could increase with little or no warning if, for instance, the political situation were to escalate in the direction of a military confrontation between Russia and NATO.

Globally, the number of destructive cyber attacks reached an all-time high in 2022. Most of the known attacks were launched by Russia and directed against Ukraine.

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

Limited intention of destructive cyber attacks against Denmark
It is less likely that foreign states, including Russia, currently have intentions of launching destructive cyber attacks against Denmark. However, Danish organizations that operate in Ukraine or provide products or services related to the war in Ukraine could be at a higher risk of attacks or collateral cyber damage from attacks directed against Ukraine.

Destructive cyber attacks are mainly used by states ahead of and during armed conflicts, with the war in Ukraine being the most recent example of this. Several states have the capabilities needed to conduct destructive cyber attacks.

States build destructive capabilities in times of peace – also against Denmark
Despite it being less likely that foreign states currently intent to launch destructive cyber attacks against Denmark, it is nevertheless likely that state-sponsored hacker groups, in particular Russian ones, are preparing for destructive attacks against critical infrastructure in Denmark. Having prepared in advance, the hacker groups can, with little or no warning, initiate destructive attacks, should the intention change.

States use tools such as cyber espionage in preparation for destructive cyber attacks that could be launched in the event of an escalating crisis or war, etc. Preparation often involves mapping of organizations, systems and network units such as industrial control systems.

Having obtained knowledge of organizations and their systems, hackers can customize new malware, just as they can install so-called backdoors on compromised systems for use in subsequent destructive attacks, enabling the groups to launch destructive attacks at short notice if the intentions of states with destructive capabilities were to change.

Wiper malware – the weapon of choice

By far the majority of destructive cyber attacks use the so-called wiper malware to destroy the victim's systems or network. Wiper malware strikes by deleting or encrypting files on the targeted system or network, rendering the files and devices inoperable or hard to restore.

Wiper malware and how it works

When files are deleted from a hard drive, they are not immediately erased from the drive. Instead, the slot where the file was stored is marked as ready for storing new files. When new files are stored, the data that used to fill the slot is overwritten, and it is only then that the original data is in fact deleted. This is the reason why it is often possible to recreate a file that has been deleted by mistake.

Wiper malware not only deletes data but also overwrites slots with new and useless data. This can be achieved through several methods and is generally a trade-off between speed and thoroughness in the attack. If, on the one hand, the wiper overwrites the data very quickly, it may be possible to restore it. If, on the other hand, the wiper is very thorough, and thus slow, security precautions can detect and intercept the malware.

Not many examples exist of advanced destructive attacks launched at industrial control systems with the aim of causing physical damage. These types of attack typically require customized malware that takes substantial resources to develop. The CFCS assesses that several states are maintaining and developing capabilities for this type of complex attacks.

Even though wiper attacks may seem less serious than attacks aimed at physical destruction, their consequences can be extensive. If, for example, the wiper attack was to delete critical system files with an organization, this would often affect the organization's operations. Also, it could take weeks or even months to restore a well-functioning network. If organizations that provide critical services to society become targets of wiper attacks, the ramifications of the attacks could be profound.

The potentially extensive consequences of wiper attacks are illustrated by the wiper attack against US communications company Viasat. On the day of the Russian invasion of Ukraine, Viasat was targeted by a wiper attack called AcidRain, disabling thousands of satellite modems, in particular in Europe. One ramification of the attacks was that the disruption of satellite communication deactivated the remote monitoring and control of several wind turbines in Germany. It is likely that the purpose of the attack was to interrupt satellite communication between Ukrainian military forces.

Together with the EU and a number of close allies, Denmark has assessed that Russia was responsible for the attack and that Russia was well aware that the destructive consequences of the attack would extend beyond Ukraine.

Wiper attacks in Russia's war against Ukraine in 2022

Since, and even prior to the February 2022 invasion, Ukraine has been hit by several different destructive wiper attacks, ranging from very simple to more advanced attacks as the one mentioned above against satellite communication. Common to the attacks against Ukrainian organizations is that they were constructed in a way to ensure that only the intended targets were compromised. The actors behind the attacks thus made an effort to ensure that the attacks would not spread beyond Ukraine.

As mentioned, the impact of the attack on Viasat extended beyond Ukraine. Even though the target of the attack was likely Ukrainian military communication, the impact of the attack extended far beyond this target. The attack shows that companies that are either physically present in Ukraine or in other ways linked to the country can potentially become collateral victims of destructive cyber attacks.

Power outages in Ukraine

In April 2022, the Ukrainian CERT announced that a Ukrainian energy company had been the target of an attempted destructive cyber attack. In the attack, the hackers used a new version of the so-called Industroyer malware which, in 2016, had previously been used against the energy sector in Ukraine. According to the Ukrainian CERT, the April 2022 attack was averted before the actor managed to cut off the power supply. However, private cyber security companies have described how a brief power outage actually took place and that the attack was likely executed by the Russian state-sponsored hacker group known as Sandworm.

A report by Microsoft describes a destructive attack on organizations in both Ukraine and Poland that took place in the autumn of 2022. The report outlines a fake ransomware attack on the transport sectors in Ukraine and Poland. The attack encrypted files, as would be the case in an actual ransomware attack, but without the possibility of file decryption. Together with the Viasat attack, these attacks are a rare example of destructive cyber attacks hitting Ukraine and a NATO country simultaneously.

The wiper attacks against Ukraine have targeted very different segments of the Ukrainian society, with several attacks being directed at critical infrastructure and government organizations. Other sectors have also been hit, such as retail trade and agriculture. It is, however, difficult to obtain reliable information on the impacts of the different cyber attacks launched during the war.

When can a cyber attack be labelled as destructive?

It is often difficult to establish beyond doubt that the aim of a cyber attack was in fact destructive if the attack is averted before it can do any damage. Different types of cyber attacks often share identical initial phases, and it is only in the final phases that the actual purpose of the attack becomes apparent. However, attempts at destructive cyber attacks may be detected if malware that is already known for its destructive properties is used in the attack. Similarly, the infrastructure that the hackers use can sometimes provide an indication of the identity of the perpetrator. Still, using infrastructure as the only indicator should be done with care, as hackers often compromise other servers to use them as stepping stones to conceal the origin of the attack.

Typically, states are the ones with the capabilities and potentially the interest in launching destructive cyber attacks against other states. So far, activists have lacked the capabilities required to launch wiper attacks. However, some activist groups are likely trying to develop the capabilities for wiper attacks, including in the shape of modified ransomware allowing file encryption but not necessarily decryption.

Cyber terrorism

The threat of cyber terrorism against Denmark is **NONE**. It is highly unlikely that Danish authorities and companies will become targets of attempted cyber terrorism in the short term.

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

The CFCS assesses that militant extremists have limited intentions of launching cyber attacks whose effects are comparable to those of conventional terrorism, and that they lack the capabilities to do so.

For years, militant extremists have exploited the Internet in support of their activities, to plan conventional terrorism, and to propagate their messages of radicalism. However, there have as yet been no examples of terrorists launching cyber attacks with effects comparable to those of conventional terrorism.

The CFCS has monitored the threat of cyber terrorism since 2016, with special focus on militant extremists. The current assessment by the Centre for Terror Analysis under the Danish Security Intelligence Service (PET) is that the threat of conventional terrorism
against Denmark is at the level of significant. For this reason, the CFCS is monitoring the cyber terrorism situation closely, regardless of the fact that the threat of cyber terrorism has for years been set at the level **NONE**.

Perspectives: **Cyber attacks with multiple purposes**

The CFCS's assessment of the cyber threat to Denmark is based on a number of cyber attack categories, such as cyber espionage and cyber crime. It is thus the motive behind the cyber attack that determines how the attack is categorized by the CFCS.

In reality, though, hackers do not necessarily have a single defined purpose, and as a victim it can be difficult to determine what type of attack you are under.

In 2022, the challenge of understanding the individual attacks, and thus the overall threat, has not grown less complicated. The war in Ukraine and the development in the conflict between Russia and the West have emphasized the need to understand cyber attacks and their underlying purposes.

Cyber crime in a new geopolitical reality

The CFCS assesses that by far the majority of cyber criminals are still opportunistic and act independently of states. Over the past year, ransomware groups have targeted companies in the West, including in Denmark, and critical infrastructure has also been targeted. Even though the war in Ukraine has served to sour relations between Denmark as a NATO member country on the one side and Russia on the other, the Russian state is not necessarily the orchestrator of cyber attacks launched against Danish critical infrastructure.

According to IT security companies and US authorities, Russia is a hotspot for cyber criminals. This has sparked public speculation as to whether ties exist between the Russian state and cyber criminals and as to whether ransomware attacks could have other motives than purely financial ones. Such speculation was fuelled in the wake of Russia's invasion of Ukraine when some cyber criminal groups openly declared their support for Russia.

As mentioned in the section on cyber crime, it is likely that cyber criminals, in a few isolated instances, have ties to foreign states. However, when media and IT companies, etc. point to possible links between the Russian state and cyber criminals, it often has to do with cyber criminals contributing to cyber espionage activities.

Technical and human errors can sometimes contribute to victims being left wondering what was the motive behind them being attacked. For example, not all criminals behind a ransomware attack leave a ransom note. Sometimes, the criminals do not get in touch for some time and in some cases not at all. In such cases, the victim may be left with the impression that the attack was not motivated by financial gain. However, the absence of a ransom demand could also merely be the result of a mistake or carelessness on the part of the criminals.

Ransomware with political agendas

The CFCS assesses that by far the majority of ransomware attacks are motivated by financial gain. A few cyber attacks have been launched that blur this perception, though.

For instance, in the spring of 2022, criminal hackers launched large ransomware attacks against several Costa Rican ministries. According to open sources, the hackers were trying to put pressure on the government by calling on the Costa Rican population to take to the streets and demand that the ransom be paid.

The attack made the government declare a state of national emergency, but it refused to pay the group's ransom demand. The hackers responded by going so far as to threaten to dislodge the Costa Rican government. Despite these political threats, financial gain was likely the actual purpose of the attack.

Categorization of attacks becomes even more difficult when states use techniques that are reminiscent of criminal activities but serve a different purpose entirely. In this context, destructive cyber attacks are particularly problematic when they are disguised as ransomware attacks, also known as "fake ransomware", with the most notorious example being the 2017 NotPetya attack. NotPetya was a cyber attack which, though it originated in Ukraine, quickly spread worldwide, also claiming victims in Denmark.

The CFCS assesses that NotPetya was in all likelihood a destructive cyber attack masquerading as a ransomware attack.

Most recently Microsoft has, as described earlier, warned that Russia in 2022 used "fake ransomware" attacks against Ukraine and Poland. Such attacks are among the reasons why victims of cyber crime are sometimes left confused as to the motivation of the attack they suffered.

Destructive activism

The war in Ukraine has triggered a wave of activist cyber attacks, with pro-Ukrainian hackers, who were called on at the start of the war to defend Ukraine from their keyboards, being particularly active.

The closer the affiliation between cyber activists and a state, the harder it is to categorize a specific cyber attack – is it a case of activism or a cyber attack committed by a state? Hackers do not stay inside specific categories, and skilled hackers do not necessarily stick to one type of activity in the digital domain. A state-employed hacker may thus well conduct activist cyber attacks on their own time – just like an activist may make money on cyber crime.

The CFCS assesses that activism is commonly seen in the form of less advanced attacks such as defacement, DDoS or hack and leak attacks. There are, however, certain signs that activist cyber attacks are becoming increasingly advanced, which could further complicate our understanding of cyber attacks.

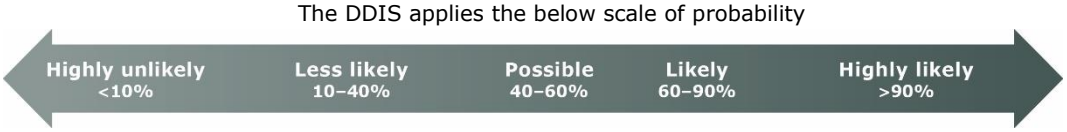
During the war in Ukraine, several activist groups have shown an interest in attacks with physically destructive consequences. Some activist groups allege to have hit critical infrastructure control systems in Russia with destructive consequences. Regardless of whether these attacks have in fact been successful or not, they are indicative of a change in activist intentions. In other words, there are signs that destructive cyber attacks motivated by an activist agenda could become part of the future threat picture, at least in relation to the ongoing war in Ukraine.

Threat levels

The Danish Defence Intelligence Service uses the following threat levels.

NONE	There are no signs of a threat. There are no actors with both the capacity and intention for attacks/harmful activity.
LOW	There are one or more actors with the capacity and intention for attacks/harmful activity. However, either the capacity or the intention or both are limited.
MEDIUM	There are one or more actors with the capacity and intention for attacks/harmful activity. However, there are no indications of specific planning of attacks/harmful activity.
HIGH	There are one or more actors that have the capacity for and are specifically planning attacks/harmful activity or that have already carried out or attempted attacks/harmful activity.
VERY HIGH	There is either information that one or more actors are initiating attacks/ harmful activity, including information about time and target, or that one or more actors are continuously initiating attacks/harmful activity.

The DDIS applies the below scale of probability



The probabilities are estimates, not calculated statistical probabilities.
"We assess" corresponds to "likely" unless a different probability level is indicated.