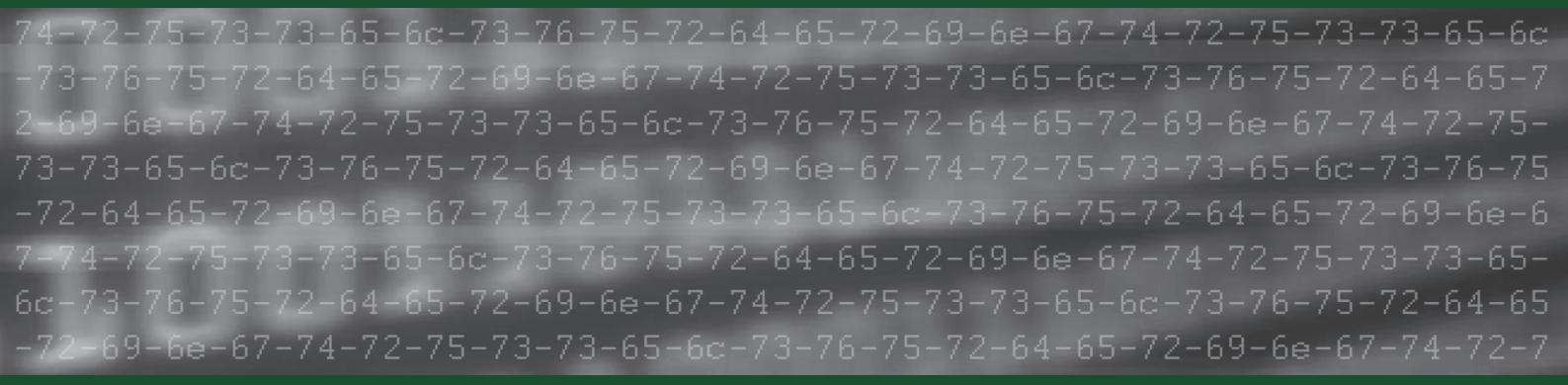
CENTRE FOR
CYBER SECURITY

Threat Assessment

The cyber threat against Denmark



Threat Assessment Branch under the Centre for Cyber Security

May 2018

CENTER FOR CYBERSIKKERHED

The cyber threat against Denmark 2018

This annual, national threat assessment describes the overall cyber threat against Danish public authorities and private companies. Cyber espionage carried out by states and cyber crimes poses the greatest threat. The threat is dynamic.

Key Assessment

- The threat from cyber espionage is **VERY HIGH**. The threat is in particular directed towards Danish public authorities of strategic, political and economic relevance to foreign states. Some foreign states also carry out cyber espionage against Danish companies. In general, foreign states are increasing their efforts to disguise their cyber espionage activities.
- The threat from cyber crime is **VERY HIGH.** Cyber crime is a global phenomenon affecting Danish public authorities, private companies and citizens. Cyber crime aimed at extorting money from public authorities, private companies and citizens is a particularly significant threat. Some cyber criminal networks are engaged in organized, long-term activities and state-sponsored hackers are likely also involved in cyber crime.
- The threat from cyber activism is **MEDIUM**. Cyber activists rarely focus on Danish public authorities and private companies. However, some hacker groups and individuals associated with cyber activist networks have significant capabilities and resources to carry out cyber attacks. Some states likely use certain cyber activist networks as a cover in attempts to influence public opinion in other countries.
- The threat from cyber terrorism is **LOW**. Militant extremists have limited skills and resources to carry out serious cyber attacks, and despite declaring their interest in conducting cyber terrorism, they currently lack the capabilities for doing so.
- Some states use cyber attacks to consolidate their power, including the use of destructive cyber attacks and hack and leak of politically sensitive information. Danish private companies and organizations operating in certain conflict areas are at a higher risk of destructive cyber attacks.

Introduction

The Centre for Cyber Security (CFCS) under the Danish Defence Intelligence Service (DDIS) defines cyber threats as malicious attempts by an actor to cause disruptions or gain unauthorized access to data, systems, digital networks or digital services. Alternative use of the Internet for malicious purposes such as recruitment of terrorist groups via social media or online sale of narcotics is not included in our definition of a cyber threat.

The threat picture is multi-faceted. In this assessment we will focus on the motivation behind cyber attacks by outlining and assessing cyber activities aimed at conducting and launching cyber espionage, cyber crime, cyber activism or cyber terrorism as well as state-sponsored destructive cyber attacks.

The threat levels are based on an analysis of the actors' intent and cyber capabilities. Our assessment of an actor's cyber capability is based on its available human and material resources, ranging from technically skilled hackers, developers of malware and information on targets that is useful for social engineering scams to IT infrastructure, time, funds and access to information. Thus, an actor's cyber capability depends on available resources as well as the ability to exploit them.

This threat assessment is based on the current threat picture operating with a warning horizon of 0 to 2 years. However, cyber threats are dynamic in nature and constantly changing, both at a general level and in relation to individual public authorities or companies. Threat and probability levels applied in this assessment are defined at the end of the report.

The chapter on cyber crime has been aligned with the National Cyber Crime Center (NC3) under the Danish National Police, and the chapter on cyber terrorism has been aligned with the Center for Terror Analysis (CTA) under the Danish Security and Intelligence Service (DSIS).

Cyber espionage

The threat from cyber espionage is **VERY HIGH**.

Several countries have significant cyber capabilities used in espionage against other states, including espionage against Denmark. Cyber espionage poses a security and economic threat to Denmark and Danish interests. The threat is highly active from specific countries, which are actively engaged in cyber espionage activities against Danish authorities and companies.

The threat from cyber espionage against Danish public authorities will persist in the long term and is thus a basic condition. Compared to traditional espionage conducted by human agents, cyber

espionage is a relatively risk-free method for foreign states to collect information. The states can potentially gain access to networks worldwide, and their attacks are often difficult to detect. In addition, the states can use relatively simple means to hide the identity of the attacker and thus avoid attribution and potential sanctions in case the attack is detected. Consequently, states with cyber espionage capabilities will continue to attack targets of strategic, geopolitical and economic relevance.

The threat of cyber espionage is especially directed at the Danish public authorities that hold information of strategic, political and economic importance. Foreign states persistently target authorities that are vital to Danish foreign, defence and security policy. Consequently, the Danish Ministry of Foreign Affairs and its representations abroad have repeatedly been targets of cyber espionage attempts. Similarly, there have been persistent attempts at espionage against the Danish Ministry of Defence as well as against Danish institutions and individuals affiliated with the Danish Defence and NATO.

Unlike physical threats, the threat of cyber espionage transcends geographic boundaries. Foreign states can conduct cyber espionage against, for instance, Danish troops deployed abroad by compromising authorities and staffs in Denmark. Conversely, a foreign state may also gain vital information on the Danish Defence by compromising Danish troops deployed abroad.

Cyber attacks have also been directed against Danish diplomatic representations abroad. The threat against Danish representations emanates in part from foreign states wanting to spy against Denmark and Danish foreign policy and in part from foreign states wanting to use Danish representations as a platform for cyber espionage activities against the countries or regions where the representations are located. The aim of cyber espionage against Danish representations may be to identify the embassy's contacts to local organizations and individuals. Some Danish representations may also be of interest to foreign states due to their roles in international organizations.

Danish companies are exposed to financially motivated cyber espionage

Some foreign states also conduct cyber espionage against Danish private companies. Industrial espionage via the Internet is an attractive method for states to steal intellectual property and technologies from other countries that have spent time and resources developing it. Thus, foreign states will continue to collect data and steal intellectual property that could support their economic interests or enable them to gain a competitive edge over their competitors in the international market. Therefore, the threat of industrial espionage has a special focus on research-heavy companies, but could also be directed against fast-growing companies, companies operating in conflict areas or companies active in the field of strategic resources such as oil and gas.

State-sponsored hacker groups also direct cyber attacks at companies and subcontractors that can be used as a platform for gaining access to information on their end targets. The growing use of subcontractors and outsourcing of IT operations and infrastructure may increase the vulnerability of Danish public authorities and private companies to cyber espionage as subcontractors often have access to sensitive client information.

In 2017, certain state-sponsored hacker groups have specifically targeted subcontractors offering cloud solutions and data storage services globally. By compromising these subcontractors, the state actors have been able to gain remote access to client networks and steal information. Because the states exploited the subcontractors' trusted networks and used legitimate usernames and passwords, it proved difficult for the victims to distinguish between legitimate and illegitimate activity. In some instances, the actors also gained access to client data stored on the subcontractors' own servers.

Other state-sponsored hacker groups have specifically targeted large Western law and consultancy firms within the investment industry in a bid to gain access to relevant and often sensitive information from the companies themselves as well as from their clients.

Cyber espionage is connected to other threats

We assess that foreign security and intelligence services are typically responsible for the cyber espionage campaigns. Cyber espionage is for these foreign services one of several available intelligence collection tools that can be used against Danish public authorities and private companies.

Thus, cyber espionage may be linked to more traditional forms of espionage. Foreign services may use information that is available on social media or that is collected through human sources in their cyber attacks. Information collected from cyber espionage may also be used in other types of espionage activities.

Cyber espionage may also facilitate other types of cyber attacks and threats. Cyber espionage may grant an opponent access to sensitive information that can subsequently be used for extortion attempts or be leaked to the public in an effort to influence public opinion. Information collected through cyber espionage may also be used in destructive cyber attacks, especially if the espionage gave access to critical infrastructure or information relevant for destructive cyber attacks. A company or public authority that has already been compromised is thus more vulnerable to this type of threat.

Cyber espionage is often carried out by state-sponsored hackers working directly for security and intelligence services. However, some states outsource espionage activities to hacker groups or legitimate IT security companies that for instance offer vulnerability scans and IT security advice.

The use of middlemen has made it easier for these states to conceal their involvement and more convincingly deny any knowledge of cyber espionage operations.

Increasing number of countries with extensive cyber capabilities

Several countries have developed cyber capabilities that pose an active or potential threat to Denmark. Below is a list of countries with extensive cyber capabilities for carrying out cyber espionage and other types of political and financially motivated cyber attacks.

Russia

Russia is still a leading and highly active actor in the cyber realm. Russia has extensive capabilities for carrying out cyber espionage and destructive cyber attacks that can underpin its strategic and security policy interests and bolstering its military operations. Russia has invested intensively in its capabilities to promote its interests in the West and has been known to use cyber attacks to achieve this goal.**China**

China

China has advanced cyber capabilities, which it uses for defensive and offensive purposes alike. China has just concluded a major military reorganization of its cyber capabilities, likely allowing Chinese actors to conduct more sophisticated cyber espionage campaigns that are harder to detect. Chinese intelligence services have repeatedly been accused of extensive cyber espionage campaigns against public authorities and private companies on a global scale. Following a short-term drop in activity level between 2016 and 2017, China is once again actively using its cyber capabilities.

Iran

Over the past few years, Iran has improved its cyber capabilities. In addition to cyber espionage activities, Iranian hacker groups may have been behind simple destructive cyber attacks that wiped data on thousands of computers. These attacks targeted the chemical, oil and gas industry in Saudi Arabia and Qatar.

North Korea

For several years, North Korea has developed a significant capability to launch different types of cyber attacks, including simple destructive cyber attacks. These attacks have especially targeted South Korea, but North Korea is likely also willing and able to launch large-scale cyber attacks against targets in other countries. In addition, it is likely that North Korea is engaged in cyber crime abroad.

Other countries

Other nations are also developing their cyber capabilities. In recent years, new regional actors from Latin America, the Middle East, South Asia and Southeast Asia have entered the cyber scene. Although these countries primarily focus on their neighbouring countries, Danish private companies or diplomatic representations operating in the region may also be exposed to cyber attacks.

Cyber crime

The threat from cyber crime is **VERY HIGH**.

Cyber crime is a global phenomenon, and Danish public authorities, private companies and citizens are all potential targets of cyber crime. Cyber crime often transcends national borders, posing a threat to victims worldwide.

In this threat assessment, the term cyber crime refers to individuals and networks that use cyber attacks to commit financially motivated crimes, for instance, theft of money or financial and personal data, fraud or extortion.

Cyber criminals will continue to pose a substantial threat to Danish public authorities, private companies and citizens in the long term. Cyber criminals are creative in their effort to make financial gain using various methods to perpetrate cyber attacks, some displaying increased sophistication and complexity.

Some cyber criminal networks are engaged in organized, long-term activities. Some cyber criminal groups have the capabilities to conduct targeted and advanced cyber attacks aimed at defrauding or blackmailing public authorities and private companies into paying very large sums of money. Other networks have specialized in attacks aimed at compromising a substantial number of victims across the world. Although these attacks are not technically advanced, they are well-organized, frequent attacks on an almost industrial scale.

The more targeted and advanced cyber attacks have been directed against especially the financial sector and health sector worldwide. However, cyber criminals' activities are driven by financial motives, and they are quick to adapt their tactics to target new victims and find new sources of income. Cyber criminals are showing increasing interest in stealing cryptocurrencies, likely due to their increasing value.

Cyber crime ranges from sophisticated attacks against for instance financial systems to simple cyber attacks that could, in principle, be carried out by criminals with very limited hacking skills, such as simple, fraudulent e-mails directed at citizens and corporate employees.

Cyber extortion by means of ransomware is one of the most prominent threats to citizens, private companies and public authorities. Ransomware is a popular tool of choice among cyber criminals as it allows them to install malware that encrypts data on the victim's computer and demand ransom to restore the victim's access to the data. In addition to having financial consequences for the affected organization, ransomware attacks could potentially affect society in general, as they cause disruption to vital services such as hospitals or transportation.

Cyber criminals also use other means than ransomware to extort their victims, for example by launching Distributed Denial of Service (DDoS) attacks or by threatening to publish stolen data.

Exact figures as to the number of cyber attacks against public authorities and private companies are absent, because many businesses fail to report the cyber attacks to law enforcement or other relevant authorities for fear of jeopardizing their reputation or because they are unaware that they have been compromised.

Cyber criminals cooperate in networks

The degree of organization amongst cyber criminals behind more advances cyber attacks varies from lone cyber criminals with advanced IT skills to established networks and groups. The groups vary in size and level of organisation, ranging from organized criminal networks to loosely coupled networks cooperating on an ad hoc basis. Some of the groups may be specialised in certain types of cyber attacks, for instance ransomware attacks or targeted attacks against payment systems.

Developers, users and providers of various cyber criminal tools and services form a cyber criminal ecosystem. Tools used by cyber criminals include different types of malware as well as tools for exploiting vulnerabilities on IT systems, so-called exploit kits. Cyber criminals also use so-called botnets to spread malware through large volumes of phishing e-mails and some cooperate with other types of criminals, for instance, to steal cash from ATMs.

Cyber criminals use online forums accessible only though anonymisers like TOR to sell malicious tools and services hiding their activities from the general public. This exchange of tools and services, also known as Crime-as-a-Service, enables criminals with limited IT skills to constitute a threat. Thus, the threat from well-organized and powerful networks that share and sell their tools contributes to the overall threat from cyber criminals.

Cyber criminals and other criminal networks exploit the latest technology in cryptocurrencies and anonymous transaction methods for money laundering, among other things. Combined with alternative banking platforms, these transaction methods allow criminals to move large sums of money without attracting attention from the authorities.

Law enforcement operations against cyber criminal networks and criminal marketplaces are key tools in the fight against cyber crime creating short term disruptions of criminal activities. Unfortunately, these operations have limited long-term impact on cyber crime as criminal networks and marketplaces are often quickly replaced by new cyber criminal actors and marketplaces.

State-sponsored hackers are likely also behind cyber crime

We assess it likely that state-sponsored hackers are also behind financially-motivated cyber attacks. Several countries, including the United States, Great Britain, Canada, Australia and New Zealand have officially attributed the May 2017 global WannaCry ransomware attack that infected more than 300,000 computers worldwide to North Korea. In 2016, hackers stole nearly USD 100 million from the Bangladesh Central Bank. Since then, similar attacks have been directed at banks

in other countries, including Taiwan-based Far Eastern International Bank in October 2017. Several security companies have attributed these attacks to hacker groups, which we assess are affiliated with North Korea.

Also, state-sponsored actors likely disguise their attacks as cyber crime. A likely example of this is the so-called NotPetya attack, which appeared to be a global ransomware attack emanating from Ukraine, though the victims were denied the possibility of regaining access to their files by paying ransom

The hackers likely attempted to disguise the attack as a ransomware attack to create uncertainty about the nature and origin of the attack, possibly heightening their resolve to carry out a destructive cyber attack that ultimately had serious implications for Ukraine as well as well as countries across the globe, including Denmark.

The WannaCry and NotPetya attacks

WannaCry
The WannaCry ransomware began to spread to computers worldwide in May 2017. This ransomware variant was able to automatically encrypt files on the victim's computer, delete original files and demand ransom to unlock the files again. At the same time, the ransomware installed a backdoor on the victim's computer, allowing the attacker to install additional malware. The WannaCry ransomware was able to spread to local networks and through the Internet by exploiting a vulnerability in the Server Message Block file sharing protocol, version 1 (SMBv1).

NotPetya
The NotPetya malware attack was carried out in June 2017, and like the WannaCry attack, it infected numerous computers worldwide, initially masquerading as ransomware. Although NotPetya demanded ransom, it did not have the functionality of enabling its victims to regain access to their data which is otherwise theoretically the case with ransomware. Consequently, the NotPetya attack was categorized as a destructive cyber attack and not as a ransomware attack.

Examples of cyber attacks conducted by cyber criminals

Below is an overview of common types of attacks carried out by cyber criminals. The list is not exhaustive.

Ransomware attacks

Like other types of malware, ransomware is often spread through phishing e-mails or by infected websites visited by the victim. Ransomware encrypts the victim's data, usually demanding payment in cryptocurrencies such as Bitcoin in exchange for granting access to the data again. There are many types of ransomware. In certain cases more targeted attacks have been carried out against for instance administrative networks in specific companies and public authorities. The health care sector abroad, in particular, has become a prime target of ransomware attacks demanding sizeable ransoms to restore data.

Infection with other types of malware

Cyber criminals continue to distribute other types of malware, including malware used to steal personal and financial data that can be sold or exploited by criminals. Some malware, so-called banking Trojans, specifically targets users of Internet banking systems. Criminals are increasingly focusing on stealing cryptocurrency from their victims. A newer type of malware used by cyber criminals steals the computer power of victim devices to generate cryptocurrencies, so-called crypto mining.

Attacks against financial systems

Some cyber criminals have specialized in targeted cyber attacks against banks and point-of-sale systems used in for instance retail. Attacks against point-of-sale systems are aimed at stealing credit card information which is then sold in bulk on the criminal marketplace. Russian banks, in particular, have been targeted by cyber criminals stealing large sums corresponding to hundreds of millions of Danish kroner. Exchanges trading cryptocurrencies have also been targeted by cyber criminals. In January 2018, hackers stole cryptocurrencies worth more than DKK 3 billion from a Japanese cryptocurrency exchange. In Denmark as well as abroad, there have been examples of hackers using malware to compromise ATMs and force the machines to dispense cash.

Targeted extortion

A more recent trend involves groups specializing in stealing sensitive corporate and client information for extortion purposes. Criminals also threaten to launch DDoS attacks as a means of extortion, often demanding very large sums of money from their victims. A hacking group calling itself Dark Overlord attracted a lot of media attention when it leaked an episode of the Orange is the New Black TV series, following an attempted blackmail of the producer of the show. Danish telecom company "3" was exposed to a similar threat in February 2017, when cyber criminals threatened to publish data stolen from the company.

Fraud

So-called BEC (Business Email Compromise) scams are aimed at defrauding companies and organizations of money by sending false requests for wire transfers in e-mails purporting to be from a senior corporate executive in an attempt to trick employees into transferring funds. This type of fraud is also called CEO fraud. The false e-mails are often sent from non-corporate e-mail accounts, but hackers have also been known to use compromised e-mail accounts belonging to corporate executives. The sending of fake e-mails from compromised e-mail accounts may increase the likelihood of a successful fraud attempt. A 2017 survey conducted by the Danish magazine Berlingske Business concluded that more than half of the surveyed companies had been subject to attempted CEO fraud.

Cyber activism

The threat from cyber activism is **MEDIUM**.

Cyber activism is typically rooted in ideological or political motives. Cyber activists may target individuals or organizations which they deem opponents to their cause.

Cyber activists use a variety of simple cyber attacks, ranging from DDoS attacks which cause disruption or suspension of service to website and social media defacement. Some cyber activists also leak sensitive information acquired through hacking of for instance personal email accounts in a bid to attract attention to their cause.

Though examples of cyber activism against Danish public authorities and private companies are rare, some hacker groups and individuals associated with cyber activist networks have significant capabilities and resources. Consequently, the threat may suddenly increase, if Danish public authorities or private companies land in the crosshairs of cyber activists.

That was the case in September 2017, when DDoS attacks likely launched by Turkish cyber activists temporarily shut down the websites of the Prime Minister's Office, the Danish Ministry of Foreign Affairs, the Danish Ministry of Immigration and Integration and Danmarks Nationalbank, the central bank of Denmark. Throughout 2017, the group, which calls itself Aslan Neferler Tim, has repeatedly claimed responsibility for cyber attacks against European countries, claiming that they have offended Turkish leaders, Turkish national pride or Islam.

The attacks illustrate that cyber activists sometimes launch attacks against authorities

Faketivists – fake activists

There have been numerous examples of state-sponsored hackers posing as cyber activists on the Internet. The popular term for these hackers is faketivists.

Hackers calling themselves Anonymous Poland are an example of such faketivists. In 2016, the group leaked information from the World Anti-Doping Agency (WADA) and the Court of Arbitration for Sport (CAS). In 2017, Anonymous Poland posted comments online about the election in Catalonia and the conflict in Ukraine.

However, a security company investigating the WADA and CAS compromises attributed the attacks to the hacker group known as Fancy Bear. US authorities claim that this group was responsible for the attack on the Democratic National Committee in 2016. We assess that it was also responsible for the attack on the Danish Ministry of Foreign Affairs in 2015, and for the attacks on the Danish Ministry of Defence and affiliated agencies in 2015 and 2016. In our assessment, a foreign intelligence service was likely behind the attacks (Source: CFCS publication: En aktør, mange angreb (in Danish), CFCS website).

and companies which they perceive as symbolic targets even though the targets may be unrelated to the issue that has caught the activists' attention. Aslan Neferler Tim supports relatively specific issues, whereas other hackers form part of more loosely affiliated cyber activist networks supporting numerous different issues. Anonymous is likely the most well-known example of a loosely affiliated network of hackers.

Loosely affiliated hacker networks like Anonymous have been known to engage in social media mobilization to warn of future attacks as was the case following the Catalonia vote on independence on 1 October 2017. In October 2017, hackers who claimed to belong to Anonymous warned that a campaign would be launched against the Spanish authorities. Subsequently, various websites were targeted in cyber attacks and information gained through hacking was leaked to the public. The cyber activism in connection with the Catalonia vote on independence also serves to illustrate that sometimes cyber activism goes hand in hand with more traditional political activism.

Some groups use simple cyber attacks as a means to disseminate militant extremist views, for example the United Cyber Caliphate (UCC) hacker network, which sympathizes with the Islamic State terrorist organization. Other groups and networks pursue different agendas when conducting cyber activism, such as fighting militant extremism on social media. Despite their ideological differences, some of these otherwise diverse groups use the same type of language and symbols, such as the so-called Guy Fawkes masks, which have become widely associated with cyber activists.

Finally, cyber activist groups are used as a cover in attempts to influence public opinion in other countries. An example of this is the US presidential election in 2016 when, according to US authorities, emails from the Democratic National Committee was compromised and leaked by Russian hackers.

Cyber terrorism

The threat from cyber terrorism is **LOW**.

We assess that militant extremists have insufficient capabilities and resources to carry out complex cyber attacks, and even though some extremists have expressed an interest in carrying out cyber terrorism attacks, they do currently not possess the capabilities to do so. The threat of cyber attacks against Denmark with the intention of creating the same effect as conventional terrorism – such as cyber attacks causing personal injury, property damage or widespread damage to critical infrastructure – is thus low.

Over the past year, several hacker groups sympathising with the Islamic State have made efforts to bolster their cyber capabilities by forming a hacker network called United Cyber Caliphate (UCC).

However, its skills and resources remain limited so far. At present, the UCC is only capable of carrying out simple cyber attacks aimed, in particular, at creating attention and disseminating Islamic State propaganda. The UCC has not been able to carry out targeted attacks. Consequently, the network has primarily targeted websites with low IT security, ranging from dance instructor websites to car enthusiast websites.

So far, Islamic State in Iraq and the Levant (ISIL) leadership has not officially recognized the UCC. The threat from hackers supporting ISIL or other extremist terrorist groups could increase, though, if groups such as ISIL choose to support the UCC or other hacker groups in future. In the short term, it is less likely that ISIL or other Sunni extremist terrorist groups will support the development of cyber capabilities to the extent that the threat of cyber terrorism will rise as a result.

Militant extremists with sufficient financial resources can also buy its way to more advanced cyber capabilities. However, at present currently attainable cyber tools are not sufficiently advanced to cause the same effect as conventional terrorist activities.

Trends impacting the cyber threat

Certain states use cyber attacks to leverage power struggles

Cyber attack capabilities, including destructive cyber attacks, DDoS attacks, and hack and leaks of politically sensitive information, can be used as potential leverage. In addition, cyber espionage capabilities may give one country a distinct advantage over another.

In the short term, it is less likely that foreign states will launch destructive cyber attacks against critical infrastructure in Denmark. However, destructive cyber attacks against targets outside of Denmark may end up affecting Danish companies and public authorities, especially those operating in conflict areas where foreign states or organized hacker groups with strong cyber capabilities have vested interests, for example in parts of Eastern Europe, the Middle East and East Asia.

Over the past years, countries such as Ukraine, South Korea and Saudi Arabia have been subjected to several destructive cyber attacks against critical infrastructure and industry. These cyber attacks have likely been carried out by state-sponsored actors as part of regional conflicts and tensions.

Though some of these attacks have had a strong impact, they have failed to cause any

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

large-scale property damage or long-term disruption of critical infrastructure. Rather, these attacks can be characterised as political posturing and harassment. The countries responsible for the attacks use them as leverage below the threshold of war. As it is generally difficult to attribute a cyber attack to a specific country, it is hard to retaliate and deter such attacks. This element of doubt works to the advantage of the attacker, and some countries exploit that.

In general, the countries responsible for carrying out destructive cyber attacks have managed to do so without any serious repercussions. The serious worldwide impact of the 2017 NotPetya attack on several international companies demonstrated the strong resolve of the attacker. The increased risk propensity and the lack of consequences for the attacker raise the risk of new destructive cyber attacks, which may cause harm outside the mentioned areas of conflict..

However, there is a growing willingness amongst several states to attribute cyber attacks to specific countries and actors, potentially providing a platform for a more clearly norm building and stand against destructive cyber attacks.

Certain countries have demonstrated the will to use hacking and leaking of politically sensitive information to influence public opinion. In this way cyber attacks are again a tool to influence political agendas and leverage power struggles. This has happened in connection with elections abroad where the attacks have been aimed at adversely affecting the public's view of and trust in specific politicians and at undermining public trust in the democratic process, prompting Western countries to generally prepare against cyber attacks in connection with elections.

Ukraine is a digital battlefield

Ukraine has been a frequent target of cyber attacks, ranging from widespread cyber espionage to destructive cyber attacks against the Ukrainian power grid.

Cyber attacks in Ukraine have also had serious repercussions outside of the country. In 2017, several non-Ukrainian companies, including Mærsk, were affected by the so-called NotPetya attack which had serious financial repercussions. Mærsk estimated the cost of the attack at somewhere between DKK 1.6 to 1.9 billion in lost revenue.

In these incidents, cyber attacks have been but one tool in wider information and influence campaigns, which have included fake online news stories and social media activities. It is possible that cyber attacks, such as hack and leak of sensitive information, may be used to influence public opinion in Denmark. The threat of such cyber attacks could rise in connection with political incidents whose outcome foreign states may have a substantial interest in affecting or in connection with political or military conflicts.

For the countries, that uses these means cyber attacks are an alternative to more traditional means of leverage. Some countries use cyber attacks to undermine regional stability and bolster their own position in conflicts where other means have proven ineffective or inadequate.

States are more determined to disguise their cyber activities

States are making strong efforts in making their cyber espionage activities more difficult til detect. Some state-sponsored hacker groups use considerable resources on technical efforts to disguise their cyber activities, possibly due to the public revelations of cyber operations in which the identities of state-employed hackers have been publically revealed and warrants for their arrest issued.

States use different methods to disguise the origin of their cyber espionage activities with some state-sponsored hacker groups now abandoning their former signature tools. Other state-sponsored hacker groups try to ensure their anonymity by increasingly using publicly available tools used by cyber criminals or legitimate IT security companies and experts alike. When states use publicly available tools instead of their own unique tools, it becomes easier for them to deny their involvement.

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.

Below is the scale of probability the DDIS applies