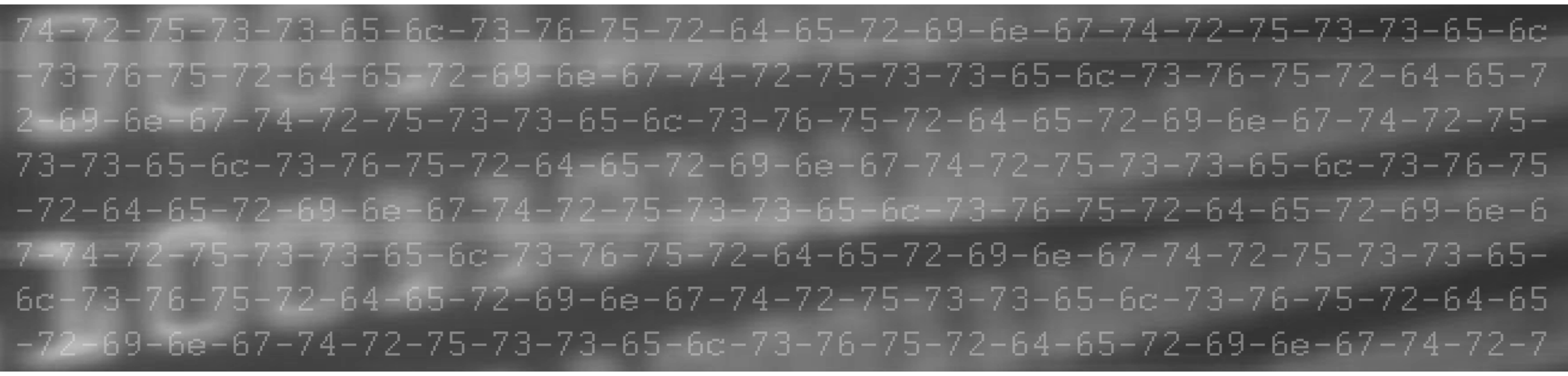
CENTRE FOR
CYBER SECURITY

Threat Assessment

The Cyber Threat Against Denmark 2019



Threat Assessment Branch under the Centre for Cyber Security

April 2019

Centre for Cyber Security
Kastellet 30
DK-2100 Copenhagen

Telephone: +45 3332 5580
E-mail: cfcs@cfcs.dk
www.cfcs.dk

10.04.2019

Threat Assessment: The Cyber Threat Against Denmark 2019

The purpose of this annual national threat assessment is to describe the overall cyber threat against Danish public authorities and private companies. Cyber espionage carried out by states and cyber crime pose the greatest threat.

Key Assessment

- The threat from cyber espionage is **VERY HIGH**. The threat is in particular directed towards the parts of the state which engages in foreign, security and defence politics. The threat is also directed at public authorities and private businesses within sectors that are critical to the functioning of the Danish society, as each sector holds valuable information of interest to foreign states. A number of states try to carry out cyber espionage against Danish interests, which is a development that continues as more states are expanding their cyber capabilities.
- The threat from cyber crime is **VERY HIGH**. In all sectors Danish public authorities and private companies should continuously expect to be exposed to cyber crime. The impact of certain types of cyber crime can have severe consequences for public authorities and private companies within sectors that are critical to the functioning of the Danish society potentially and thereby for the Danish society.
- The threat from cyber activism is **MEDIUM**. Cyber activists rarely focus on Danish public authorities or private companies. However, some hacker groups and individuals associated with cyber activist networks have significant capabilities and resources to carry out cyber activism. Thus, the threat from cyber activism can rise suddenly if attention of activists towards Danish public authorities or private companies arises.
- The threat from cyber terrorism is **LOW**. Militant extremists have in few cases shown interest in conducting cyber terrorism, but they still lack the capacities for doing so.
- In the short term, it is less likely that foreign states will launch destructive cyber attacks against critical infrastructure in Denmark. However, Danish private companies and public authorities can become collateral victims of destructive cyber attacks against targets outside of Denmark.
- Technological development such as the Internet of Things and artificial intelligence will bring new opportunities for the society but also increase the attack surfaces for hackers. There will also be an increased risk of cyber attacks resulting in physical damage as units connected to the Internet increasingly control physical systems.

Introduction

The cyber threat has become an everyday reality to Danish public authorities and private companies. The cyber threat in 2018 was still very active, although larger cyber incidents were not as serious as the ones seen in 2017 where WannaCry and NotPetya attacks disrupted everything from hospitals to shipping terminals across the world. The Centre for Cyber Security under the Danish Defence Intelligence Service (CFCS) assesses that the threat landscape will not evolve in a more positive direction as technological advancements and the digitalization of Danish society continuously give new opportunities for hackers. Development trends impacting the cyber threat is described in the last chapter of this year's assessment of the cyber threat against Denmark.

CFCS 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. In addition, CFCS describes hackers' use of destructive cyber attacks as well as hack and leak attacks.

The threat levels are based on an analysis of the actors' intent and cyber capabilities. CFCS assessment of an actor's cyber capability is based on the actor's 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, as cyber threats are dynamic in nature and constantly changing, public authorities as well as private companies need to adapt quickly to change in the cyber threat landscape. Threat and probability levels applied in this assessment are defined at the end of the report.

Cyber Espionage

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

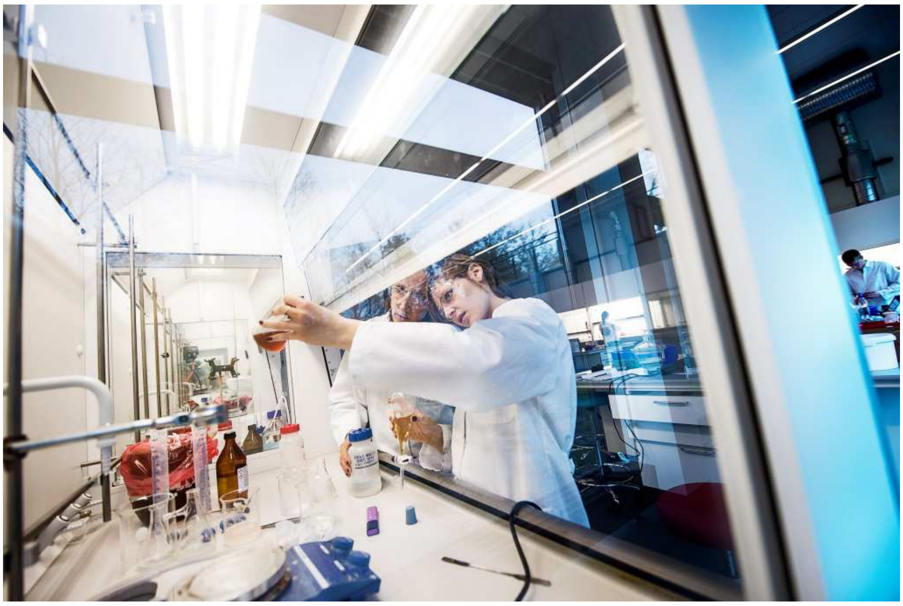
Cyber espionage poses a significant security and economic threat to Danish public authorities, sectors and private companies. CFCS assesses that the threat in particular emanates from foreign states and their intelligence services, which regularly attempt to steal information from Danish public authorities and private companies.

The threat of cyber espionage is especially directed towards certain segments in the Danish public sector, in particular the Danish Ministry of Foreign Affairs, the Ministry of Defence and their affiliated institutions and individuals affiliated with the Danish defence and NATO.

The threat from cyber espionage is also directed towards public authorities or private companies that are critical to the functioning of the Danish society, including the energy, finance, health, shipping, telecommunications and transport sector. CFCS assess that the threat from cyber espionage against the energy, healthcare and shipping sector is VERY HIGH whereas the threat from cyber espionage against the financial, telecom and transport sector is HIGH. Hence the threat level from cyber espionage is not equally high for all sectors, but foreign states have both the intent and capacity to conduct cyber espionage against all sectors.

Cyber espionage against public authorities and private companies operating in sectors critical to the functioning of the Danish society may be politically as well as financially motivated. Each sector holds valuable information of interest to foreign states. The threat against the healthcare sector for example is directed at healthcare data, research and technology that may be exploited by foreign states to develop and improve their own healthcare systems and living standards. The threat against the energy sector is particularly directed at knowledge that may promote foreign states' energy sector- and politics, but also against systems and networks, which can be used for destructive cyber attacks.

Public authorities and private companies across all sectors face the same challenge; foreign states may steal the data and use it themselves or share it with domestic companies. In addition to causing damage to the affected Danish company or public authority it may also pose an economic risk to Denmark. It may hurt Denmark's international competitiveness when foreign companies gain access to stolen



Foreign states have among other things an interest in conducting cyber espionage against research, which Denmark use ressources to develop information on research, systems or confidential information about tenders and contracts that Danish companies have spent time and resources developing or negotiating.

The threat from cyber espionage is therefore particularly directed towards research-heavy companies, fast-growing companies, companies operating in conflict areas, or companies active in the field of strategic resources such as natural resources or critical infrastructure.

If a foreign state compromises Danish companies or public authorities in order to conduct cyber espionage against them, they may become vulnerable to other types of threats. Cyber espionage may provide an opponent with access to sensitive information that could subsequently be leaked in order to influence public opinion in connection with an election, political or topical issues. Cyber espionage may facilitate destructive cyber attacks, particularly if it grants access to critical systems or specialist information.

Several states pose a cyber threat to Denmark

CFCS assesses that an increasing number of foreign states pose a cyber threat to Denmark and that this development will continue as cyber attacks become a central instrument of political tools for several countries. Both powerful and less powerful states are improving and using their cyber capacities as cyber espionage is a relatively risk-free method for foreign states to gain access to desirable information.

CFCS assesses that a small number of foreign states are trying to conduct cyber espionage against public authorities and private companies across the world, including Denmark. The greatest cyber threat against Denmark emanates from these states. Russia and China, in particular, hold sophisticated cyber capacities and are extremely active in the cyber realm. It is likely that Iran and North Korea use their cyber capacities against targets worldwide.

Other foreign states primarily use their cyber capabilities against public authorities, private companies and citizens in their neighbouring region. CFCS assesses that these states also pose a cyber threat to Denmark, as it is likely that they attempt to spy against Danish representations in the region. For example, in May 2018, an employee in a Danish embassy in Asia was targeted with spear phishing by a hacker group likely affiliated with another Asian state. The attack failed. CFCS assesses that these states try to compromise Danish representations partly to gain knowledge of Danish national security and foreign policy in the region and in order to gain access to knowledge about the country or region where the representation is located. Some Danish representations may also be of interest to foreign states due to their roles in international organizations.

Foreign states that primarily use their cyber capabilities in their neighbouring region also pose a cyber espionage threat to internationally deployed Danish troops. For instance, foreign states may gain access to sensitive information on the Danish Armed Forces by compromising Danish troops deployed internationally.

State-sponsored hacker groups conduct cyber espionage against subcontractors

State-sponsored hacker groups also launch cyber attacks against subcontractors that can be used as a platform for gaining access to information on their end targets.

Hacker groups have amongst other directed their attention towards subcontractors offering different cloud solutions and data storage services. By compromising these subcontractors, foreign states have had remote access directly to client networks from where they could steal information.

Because the state actors were able to exploit the subcontractors' trusted networks and used legitimate usernames and passwords, it has proven difficult for the victims to distinguish between legitimate and illegitimate activity. In some of the cases, the actors also gained access to client data stored on the subcontractors' own servers.

Most public authorities and private companies use subcontractors. It is relevant for all sectors to understand what kind of access the subcontractors have to the authorities' or companies' networks.

Cyber attacks against subcontractors

APT10 is a hacker group that for years has managed to steal information from their victims by attacking subcontractors. The group was responsible, among other things, for a campaign called Cloudhopper. The campaign was called Cloudhopper because APT10 targeted cloud service providers in order to use them as a platform to compromise to their clients.

APT10 has targeted many different public authorities and private companies across the world amongst other to steal intellectual property.

On 20 December 2018, the US Department of Justice and the FBI charged two Chinese citizens of being affiliated with the hacker group APT10.

Cyber Crime

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

It is a complex threat consisting of many different types of cyber crimes. The threat ranges from simple cyber attacks launched by criminals with almost no IT-skills to advanced cyber attacks launched by well-organized hacker groups that are likely state-sponsored. In this threat assessment, the term cyber crime refers to perpetrators that use cyber attacks to commit financially motivated crimes.

The various types of cyber crime have different consequences and not all public authorities or private companies will be targets of all types of cyber crime. However, Danish public authorities and private companies across all sectors should expect to be targets of one or more types of cyber crime.

Frequent attacks by cyber criminals pose a persistent threat to Denmark

One type of cyber crime networks seek to compromise as many victims as possible in order to maximize their profits. These attacks are typically less advanced and yield lower returns per victim, but hackers will attack numerous victims at once, and they will attack again and again. These criminal networks pose a persistent threat to public authorities, private companies and citizens.

In order to reach as many victims as possible, cyber criminals spread their malware through phishing emails or infect websites visited by the victims. Some criminals send large volumes of phishing emails to thousands of recipients. The attacks are typically launched by an ecosystem of cyber criminals who have specialized in malware development, development and operation of technical infrastructure or handling of compromised victims. The exchange of services between these criminals also enables criminals with limited IT skills to commit cyber crime.

The type of malware spread by cyber criminals depend on the potential for profit. Some malware combine the characteristics of different forms of malware to maximize their potential profit. The malware called Svpeng is an example of malware targeting mobile Android devices. The malware can be used to steal information from the victim's mobile phone as well as encrypt the phones content. Hackers using Svpeng malware can profit both by abusing login credentials to banking apps and by demanding ransom to decrypt data on the phone.

In 2018 there was a general trend of fewer ransomware attacks whereas there was an increase in malware exploiting IT systems to generate digital currency also known as crypto mining malware. Over the past few years, there has been a rise in cryptocurrency theft from cryptocurrency exchanges and private individuals; a rise that is likely due to increased value of and speculation in cryptocurrency.

Hackers also try to compromise companies that store personal information of citizens, which could be abused in different ways to create profit. Such information can be a civil registration number or credit card information.

In late 2018, cyber criminals infected a number of online stores in Denmark and internationally in order to skim payment information when customers bought goods online. Hackers injected malicious code on the online stores' websites, which stole payment information. Competition among cyber criminals to steal credit card information has become so fierce that cyber criminal groups have been known to sabotage each other on the website of the same compromised online stores.

Examples of data theft

In June 2018, Ticketmaster UK revealed that credit card information from its customers possibly had been compromised. Danish Ticketmaster customers who had bought tickets during a specific period were advised by Ticketmaster to monitor their account statements for evidence of fraud.

In the autumn of 2018, the Danish company Bahne's online store was attacked by hackers who attempted to steal payment information from its customers. Bahne advised its customers to take preventive measures and cancel the credit card used to make the online purchases as the information could be abused by cyber criminals. As a result of the attack, Bahne's online store was rendered unavailable for a couple of hours on Black Friday. In early January 2019, the online store was once again attacked and was closed for two months and moved to a new platform.

Cyber criminals also conduct extortion attacks without use of malware. This year, for example, a number of Danish people have been targeted with extortion attempts, so-called sextortion where cybercriminals extort the victim by claiming to have obtained private information, images, or video of the victim. In many cases criminals have provided a password, which the victim has used on a webpage in order to increase the credibility of the extortion threat. From the cases that CFCS has knowledge of the passwords emanate from preceding leaks or hacked databases available on the Internet and passwords are thus typically several years old.

In some extortion attempts it appears as if the email has been sent from the recipient's own email address, adding credence to the scammers' claim that they have access to the victim's email account. This is a trick however, where criminals have forged the sender address with a technique called spoofing.

The cases of sextortion that CFCS has knowledge of have proven to be allegations and empty threats. CFCS recommends that you do not respond to the email and do not pay ransom.

Cyber attacks by criminals may disrupt critical national functions

There are cyber criminal networks, which pose a threat to private companies and public authorities that are vital to the functioning of the Danish society. These networks launch targeted attacks and thus have fewer victims. In return, though, the profit can be much higher as they have a higher success rate in compromising vital networks and systems. As to hacker groups that use ransomware or steal data, their focused cyber attacks might put significant pressure on the victim with respect to paying ransom in exchange for access to their data.

Cyber attacks launched by these criminal networks may have serious consequences for private companies and organizations that are vital to the functioning of the Danish society. Potential consequences include supply stops, significant financial losses, downtime or loss of reputation. At worst, it may have serious social consequences and erode public confidence in the critical national functions. The threat from more targeted attacks is also directed at companies, which are not vital to critical national functions. Such attacks can have serious consequences for the companies in question, but the social consequences are less severe.

An example is the cyber criminal group behind the ransomware known as SamSam. SamSam attacks have in particular targeted the healthcare sector, educational and public institutions in several countries, though mainly in the United States. SamSam ransomware has repeatedly targeted hospitals, affecting the critical national services provided by the hospitals. A US hospital that was hit by a targeted SamSam ransomware attack in early 2018 decided to pay the ransom corresponding to approx. DKK 300,000. US authorities claim that the two alleged perpetrators behind the SamSam attacks earned about DKK 40 million in their attacks.

Over the past few years, there have been a number of targeted cyber attacks against foreign banks in which cyber criminals managed to steal large amounts of money. The hackers compromised the banks' IT systems and subsequently made unauthorized transfers via financial networks such as SWIFT. In August 2018, for example, an Indian bank lost approx. DKK 85 million in a cyber attack. Several security companies have attributed some of these digital bank robberies to hacker groups which CFCS assesses are affiliated with North Korea.

Some of the attacks have affected the services of the financial institutions. This was also the case on 13 February 2019, when the Maltese bank (Bank of Valletta) temporarily suspended all its' businesses to counter a cyber attack in which hackers tried to steal close to DKK 100 million. Amongst other the bank closed its branch offices and ATMs on Malta and closed down its website.

In a few incidents, hackers have deleted or encrypted financial institution's data in connection with such digital bank robberies. It was likely done as an attempt to cover their tracks or prevent the victim from detecting the robbery.

Cyber Activism

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

Cyber activists rarely focus on Danish public authorities or private companies. However, some hacker groups and individuals affiliated with cyber activist networks have significant capabilities and resources to carry out cyber activism. Thus, the threat may rise suddenly if attention of cyber activists towards Danish public authorities or private companies arises.

The purpose of cyber activism is to draw the largest possible attention to a specific cause. Social media is often used as a platform to warn of future attacks or call for attacks unlike for example cyber espionage where hackers attempt to hide their activities.

Networks with an interest in Denmark

There is a limited cyber activist community with interest in- or of launching activities against Danish public authorities or private companies. There have been few cases involving Danish cyber activists, and the NC3 has in some cases identified the activists and contributed to prosecuting them.

Cyber activism is motivated by everything from animal welfare to anti-capitalism

Cyber activism is typically driven by ideological or political motives. Cyber activists often target individuals or organizations, which they deem opponents to their cause. Cyber activists sometimes launch attacks against authorities and companies which they perceive as symbolic targets even though the targets may be unrelated to the issue that has caught the activists' attention.

It may prove extremely difficult to predict what will trigger cyber activist attacks as well as the potential targets. Cyber activists are driven by very different motives and views. Loosely affiliated networks of hackers such as the hacker group Anonymous comprise activists focusing on various subjects ranging from Internet freedom, animal rights, climate, support for whistle-blowers, anti-capitalism and the fight against militant Islamists and right wing extremism. There have also been examples of nationalist hacker groups and networks supporting terrorist groups.

Attack motivated by animal rights issue

During a campaign under the slogan OpDenmark and OpBeast, approx. 350 Danish websites were targeted by DDoS attacks during the period 2013-2014. The campaign sought to change Danish legislation on animal sex.

Internationally, there have been a number of cyber activist attacks in connection with diplomatic or military conflicts. Consequently, the threat against Denmark may rise if Danish public authorities or private companies become embroiled in such foreign conflicts.

Recurring campaigns and physical political activism may warn of future cyber activism

Though cyber activist attacks are often relatively spontaneous, it will in some cases be easier to predict cyber activist attacks. This is particularly in connection with recurring campaigns and in connection with physical political activism, which is oftentimes accompanied by cyber activism.

Some cyber activism campaigns are repeated year after year. For example, repeated DDoS attacks are launched by hackers affiliated with the hacker group Anonymous against central banks and other financial institutions in connection with the anti-capitalist #OpIcarus campaign. This campaign has occurred several times since 2016.

Cyber activism also increasingly accompanies traditional political activism. This was the case in late 2018, when hackers sympathizing with the yellow vests in France launched several DDoS attacks and hack and leak attacks against the websites of a number of French authorities and private companies, including French law enforcement agencies, the ministry of foreign affairs and the defence ministry.

Cyber activists attacked French public authorities and private companies to show support for the Yellow Vest protests

The capabilities of cyber activists and their level of organization vary
The capabilities of cyber activists and their level of organization, or lack thereof, vary greatly, making it difficult to assess the extent of cyber capacities available for cyber activist campaigns.

For instance, the loosely affiliated hacker network Anonymous consists of both organized hacker groups with capacity and intent to launch cyber attacks as well as sympathizers with no capability or intent to launch cyber activist attacks. Some cyber activist attacks are thus launched by hacker groups comprising relatively permanent members while others are launched by individual hackers. Occasionally, individual hackers, hacker groups and networks pool their skills and work together on specific campaigns.

Individual hackers are able to launch high-profile cyber attacks with relatively simple means. Illustrative of this is the December 2018 Twitter breach involving the leak of personal data affecting up to 1000 German politicians and public figures, a case that attracted great publicity in both Germany and Denmark. A young German man, who was arrested in January 2019, confessed to having used hacking to gain some of the information. The German authorities announced that the man had used relatively simple means to gain unauthorized access to the victims' accounts. According to the media, he gained access by exploiting the victims' weak passwords.

Examples of cyber activist attack methods

DDoS attack: Overwhelming a webpage with a flood of data traffic is still a widely used method among cyber activists in order to disrupt a webpage.

Defacement: By using this method, cyber activists compromise websites or social media profiles, where they post messages or pictures.

Hack and leak attacks: Some cyber activists leak sensitive information by hacking personal mail accounts in a bid to promote their cause.

State-sponsored hackers behind faketivism

State-sponsored hackers have also been known to pose as cyber activists in order to manipulate public opinion in other countries. The popular term for these hackers who claim to be non-state-sponsored hackers, is faketivists.

The threat from faketivism can increase in connection with political, strategic or financial issues where foreign states have a vested interest in affecting the outcome. The threat can also rise in connection with deepening political or military conflicts.

The incident involving the World Anti-Doping Agency (WADA) and several other anti-doping organizations, which were compromised by a hacker group known as Fancy Bear Hack Team posing as cyber activists is an example of faketivism. The group leaked information they had hacked for, for example about Danish swimmer Pernille Blume. In October 2018, US authorities publicly accused several Russian intelligence officers of being behind these attacks and several other hack and leak attack campaigns.

Cyber Terrorism

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

Militant extremists have in a few cases expressed an interest in conducting cyber terrorism, but CFCS assesses that they still lack the capacities to do so. Currently they are only capable of conducting simple cyber attacks aimed at promoting and disseminating propaganda for ISIL and other militant extremist groups. Consequently, there is a low threat against Denmark with the intention of creating similar effects as conventional terrorism, such as cyber attacks causing personal injury or widespread damage to critical infrastructure.

Over the past years, several hacker groups sympathising with the terrorist organization Islamic State in Iraq and the Levant (ISIL) have made efforts to bolster their cyber capacities by forming joint hacker networks. United Cyber Caliphate (UCC), formed in 2016, is the best known example of such networks. So far however, this has not improved the skills or resources of militant extremists to use cyber attacks.

The ISIL leadership has still not officially recognized the UCC or other hacker groups. The threat from hackers supporting ISIL or other extremist terrorist groups may suddenly increase, if groups like ISIL decide to support the UCC or other hacker groups. In the short term, it is less likely that ISIL or other Sunni extremist terrorist groups will support the development of cyber capacities to the extent that the threat from cyber terrorism will rise.

Militant extremists with sufficient financial resources may purchase more sophisticated cyber capacities than the ones they currently possess. However, the cyber tools currently available for purchase are not sufficiently advanced to cause the same effect as conventional terrorism.

Destructive Cyber Attacks

CFCS assesses it less likely that foreign states will launch destructive cyber attacks against critical infrastructure in Denmark in the short term. However, the threat level may increase in the event that Denmark becomes embroiled in political or military conflict with countries with destructive cyber attack capacities.

Destructive cyber attacks

CFCS defines 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.

CFCS assesses that there is a possibility that foreign states have tried to compromise companies and public authorities that are vital to the functioning of the Danish society in order to develop capacities to launch destructive cyber attack against critical Danish infrastructure at a later point. CFCS views the number of targeted attacks in 2017 on organizations in the Danish energy sector with concern.

Danish organizations may become collateral victims of destructive cyber attacks against targets outside of Denmark

In the short term, destructive cyber attacks against targets outside of Denmark may end up affecting Danish companies and public authorities, especially on those operating in countries such as Saudi Arabia, South Korea and Ukraine where foreign states are likely to have launched destructive cyber attacks.

The 2017 NotPetya attack in Ukraine showed that destructive cyber attacks can spread to organizations located outside these countries. Private companies operating in these countries may also be singled out as specific targets for destructive cyber attacks. Illustrative of this is the December 2018 destructive cyber attack against Italian oil subcontractor Saipem. Saipem is amongst other a subcontractor for the Saudi-owned oil company Saudi Aramco. Saudi Aramco has been targeted twice earlier with destructive cyber attacks with variants of the same malware Shamoon malware, which was used against Saipem. The destructive cyber attack targeting Saipem destroyed data on several hundreds of the company's computers worldwide.

Destructive cyber attacks are rare and mostly aimed at destroying data

CFCS's definition of destructive cyber attacks covers cyber attacks with very different consequences, ranging from data deletion to physical destruction. Destructive cyber attacks often result in destruction of data by deletion or making it unavailable with malware or tools, popularly known as wipers. Destruction and manipulation of data in industrial control systems have in some cases resulted in operational disruption and breakdown. In one incident dating back several years, a destructive cyber attack caused physical damage outside IT-systems.

Destructive cyber attacks are rare compared to other types of cyber attacks and have mainly occurred in Saudi Arabia, South Korea and Ukraine. CFCS assesses that the attacks in these countries were likely conducted by state-sponsored actors and that they were mainly part of regional conflicts and tensions.

The attack against Triconex

A cyber attack that could potentially have caused physical damage occurred in Saudi Arabia in 2017. It was publicly known in 2018.The attack targeted a petrochemical industrial plant and a specific system called Triconex used by the facility.

The Triconex system provides a controlled and safe shutdown of production systems in case of vital errors or problems. In this incident, certain conditions meant that the security systems shut down the plant in a safe way, eventually leading to the detection of the malware.

If the security mechanisms had been turned off or manipulated, it could, at worst, have increased the risk of dangerous gas leaks or explosions.

Hackers also conduct simple destructive cyber attacks that are not launched in response to political or military conflicts. Over the past few years hackers have in a few cases shown intent to destroy or encrypt data belonging to financial companies in connection with digital bank robberies, likely in an attempt to cover their tracks or prevent the companies from reacting to the theft. Data destruction- or encryption in digital bank robberies is currently a relatively rare phenomenon, but it may have serious repercussions for the affected financial institution.

Hack and Leak Attacks

Certain countries also use hack and leak of sensitive political information to manipulate public opinion. In this relation cyber attack is a powerful tool to influence political agendas and power struggles. This has happened in connection with foreign elections where the attacks have been aimed at adversely affecting the public's view of and trust in certain politicians as well as undermining public trust in the democratic process. This has prompted Western countries to prepare against cyber attacks in connection with elections.

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

Development Trends Affecting the Cyber Threat

The cyber threat against the Danish society is very much dependent on the existing technologies and societal conditions. Below we describe an array of technological and structural trends that are expected to have an impact on the cyber threat in the coming years.

Generally, digitization is a rising tide, and the physical and digital worlds will become increasingly fused. In addition, computers with artificial intelligence will increasingly carry out functions vital to society and the individual citizen, ultimately increasing society's dependency of digital systems.

Cyber attacks may increasingly affect the physical world

Over the past two years, Denmark has implemented new networks such as Narrowband IoT, Sigfox and LoRaWAN, which along with the Internet and the traditional mobile network support an increasing number of digital solutions that connect the digital and physical world, also known as the Internet of Things (IoT). Illustrative of this is the development of so-called Smart Cities, where IoT solutions help increase efficiency and improve the quality of waste management services, traffic and transport systems and public utility services. In Denmark, several cities have adopted the smart city concept and have, for instance, introduced sensors that are used to measure fill level of trash bins. Another example is a Danish municipality that continually regulates district heating and water supply based on real-time data on the water and heat consumption of the individual household.

The latest 5G mobile technology, designed to support self-driving vehicles and autonomous production systems, is expected to further merge the digital and physical worlds.

Terms

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

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

Internet of Things: Internet of Things, abbreviated IoT, is a term covering everyday devices such as refrigerators and cameras connected to the Internet, allowing the devices to be remotely monitored and controlled and communicate and interact with other devices over the Internet without human intervention needed.

Cloud Computing: Cloud computing refers to the delivery of scalable and flexible IT resources over the Internet. Cloud computing comprises virtual infrastructure, software platforms, applications or services that are rented according to need.

The technology will give new opportunities that benefit society, but it will also open up a wider range of attack surfaces for hackers. If hackers disrupt or manipulate signals sent from and to IoT devices, they may potentially cause physical destruction as devices connected to the Internet increasingly control physical systems.

The growing number of IoT devices may facilitate more and graver cyber attacks

In these years there is a large increase in the number of devices that are connecting to the Internet that traditionally have not been connected. According to some estimates, more than 20 billion new devices will be connected to the Internet by 2020, and other estimates are much higher. Devices range from refrigerators to large industrial control systems that connect to the Internet.

There are numerous risks associated with the increasing number of IoT devices that connect to the Internet, and IoT devices are now considered to be among the type of units on the Internet that are targeted most by cyber attacks.

A cyber attack targeting an IoT device may affect its functionality or compromise the network that the unit is installed to. Often, the goal is to install malware on the device, enabling the attacker to remotely take control of the device and abuse it for other cyber attacks. Compromised IoT devices have typically been used as part of DDoS attacks where the criminal floods the targeted server with traffic, causing disruption and breakdown.

IoT devices are often vulnerable as they are designed for one specific purpose, and the network functions enabling the device to communicate via the Internet, are secondary functions. As a result, the devices have poor network security compared to traditional IT equipment, which is designed for Internet connectivity. In addition, many IoT devices are not designed to receive security updates. Consequently, vulnerabilities detected during the product lifetime cannot be patched, allowing hackers to exploit these as long as the product is in use. This is particularly a problem for the IoT devices designed to operate for years without human interaction.

Artificial intelligence systems can be hacked to make harmful decisions
Countries around the world are researching in artificial intelligence and see the strategic benefits of this technology. This also includes Denmark. True artificial intelligence does not exist yet and will probably not come into play anytime soon. The term however, is used about computer programmes that via machine learning are capable of solving specific analytical tasks, which has previously required human intelligence.

However, the use of artificial intelligence may also increase society's vulnerability to cyber attacks. As artificial intelligence is increasingly used to make routine decisions and perform tasks that have previously been carried out by humans, it is vital that the systems remain resilient to cyber attacks, preventing hackers from manipulating the system's decisions. Where the outcome of traditional computer programmes is determined by a series of fixed and verifiable algorithms, with systems of artificial intelligence it can be difficult to prove how the computer reached a given result. This can make it challenging to verify the validity of the result.

Artificial intelligence is expected to play an increasingly important role within in the field of self-driving cars, autonomous industrial systems, medical diagnostics and medication in the healthcare sector.

Increasing use of outsourcing may hamper cyber security
The growth in Internet bandwidth and speed has continuously increased the opportunity for public authorities and companies to outsource infrastructure and operational tasks to subcontractors. As a result, Danish as well as international companies have increasingly outsourced the digital aspect of their business to subcontractors, even to foreign subcontractors. Illustrative of this is storage of data in central data centres, outsourcing of IT solutions to cloud suppliers or of critical infrastructure operations.

From a business point of view, it makes good sense to outsource part of a business, as it may streamline work procedures, allowing the private company or public authority to focus its resources elsewhere. There are, however, many security-related challenges associated with outsourcing as the control of outsourced IT systems and the protection of sensitive business data and IT systems are in fact put in the hands of the subcontractors. Consequently, it may also prove technically and legally difficult in connection with security incidents to re-establish IT systems and determine the origin of the incident. For example, in February 2019, a hacker deleted the contents on the servers of email provider VFE mail. The attack wiped all the customer's e-mails and many could not be restored as backup files were also deleted. The founder of the webmail service tweeted shortly after that the company was likely not to survive the attack.

Centralization of data and IT infrastructure facilitates compromise of multiple victims in one attack

Outsourcing to IT infrastructure providers, data centres and cloud solution services may help to heighten a company's cyber security. This can be achieved as market-leading subcontractors with a large clientele are able to invest a significant amount of resources to protect its infrastructure against cyber attacks.

However, as a result of such centralization, an effective cyber attack against a subcontractor may potentially impact a large number of public authorities and private companies simultaneously, which can have large consequences for society. This problem can be further exacerbated by the trend that the market for cloud computing is increasingly dominated by a few but large global operators.

Simple attack methods remain among the most effective

Even though the cyber threat is constantly changing, hackers continue to use the same method they have used for years. That is because the same attack methods remain effective, as many public authorities and private companies continue to be vulnerable to these.

For instance, phishing-mails remain one of the most effective ways to gain unauthorized access to an organization's information, network or systems. Hackers continue to successfully guess or breach simple or reused passwords. Old vulnerabilities also enable hackers to gain access to the network of public authorities and private companies because their systems are not updated or duly replaced.

CFCS' website, www.cfcs.dk, offers guidelines on how to counter cyber attacks, and we continuously share relevant information about how to counter the cyber threat via Twitter accounts.

Threat Levels

The Danish Defence Intelligence Service (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

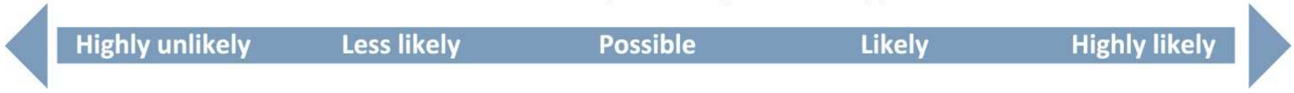


Photo credit list

Photo, page 4:

Foreign states have among other things an interest in conducting cyber espionage against research which Denmark uses ressources to develop
Rode Joachim/Ritzau Scanpix

Photo, page 10:

Cyber activists attacked French public authorities and private companies to show support for the Yellow Vest protests
Michel Spingler/AP/Ritzau Scanpix