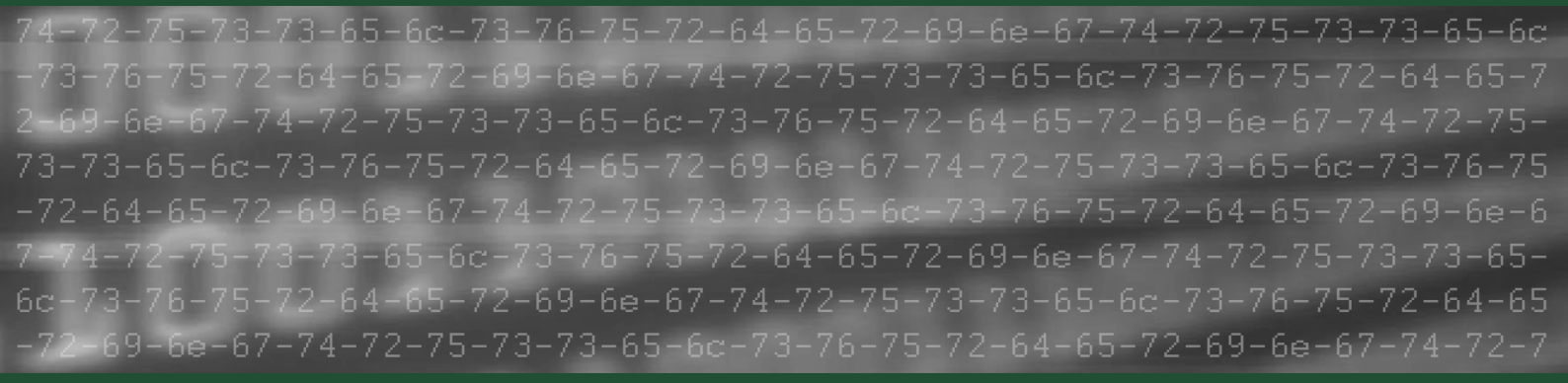
CENTRE FOR
CYBER SECURITY

Threat Assessment

The cyber threat against Denmark



Threat Assessment Branch under the Centre for Cyber Security

February 2017

CENTER FOR CYBERSIKKERHED

February 2017

The cyber threat against Denmark

This report addresses the threat from cyber activities against Danish authorities and private companies. The main threat emanates from state-sponsored cyber espionage and from cyber crime. State and criminal hackers are continuously developing their skills and their attack methods are growing ever more sophisticated.

Key assessment

Cyber espionage against public and private targets continues to constitute the most severe cyber threat against Denmark. The threat against Danish interests is highly active and emanates in particular from foreign states.

The threat from cyber espionage against Danish authorities and private companies is **VERY HIGH**.

The threat from cyber crime is increasing in scale and complexity and is conducted by, among others, organized criminals. Cyber criminal services are also for sale online. The most frequently used attack methods include ransomware and DDoS.

The threat from cyber crime against Danish authorities and private companies is **VERY HIGH**.

Even though the capability for cyber activism against Danish authorities and companies is present, examples of such activities are few. Still, the threat from cyber activism may change overnight for companies, authorities or private individuals who find themselves in activists' spotlight for political or ideological reasons.

The threat from cyber activism against Danish authorities and private companies is **MEDIUM**.

At present, known terrorist groups do not have the capabilities required to launch fully fledged fatal or massively destructive terrorist attacks via the Internet.

The threat from cyber terrorism against Danish authorities and private companies is **LOW**.

Introduction: the cyber threat is ever changing

Advanced economies typically have a higher degree of Internet dependence than developing countries do. That makes them natural targets for foreign states and criminals, who intent to use the cyber domain for malicious purposes.

Danish authorities and private companies depend extensively on the Internet in their daily dealings, and operation of critical infrastructure is increasingly connected to the Internet. This presents a number of challenges. On the one hand, digitization creates new and innovative opportunities; on the other hand, it makes users and society vulnerable to cyber attacks. The dynamic nature of IT technology is reflected in the ever-changing threats, whose volatile character forces authorities and companies to constantly adjust their cyber security measures and level of preparedness. This threat assessment outlines and assesses the main cyber threats against Danish digital networks.

The dark figures are high when it comes to knowledge about cyber attacks against authorities and companies. In some cases, this is the result of organizations wanting to minimize attention surrounding attacks or simply not being aware that they have in fact been the target of an attack.

As many private companies only report cyber attacks if the attack has been successful and has resulted in realized losses, there is a lack of overall statistical data on failed or prevented attacks. All attacks, regardless of their success or failure, are relevant to form a complete threat picture. The Centre for Cyber Security collaborates with authorities and private companies and describes the cyber threat based on the collected knowledge.

Threat picture

The threat picture can be described from multiple angles. This assessment focuses on the motivation of the actor behind the individual threats and the severity of the threat impact on the targeted authority or company.

The Centre for Cyber Security (CFCS) under The Danish Defence Intelligence Service (DDIS) defines cyber threats as malicious activities in which a digital system or network is exposed to a cyber attack enabling the attackers to get unauthorized access to systems and data. Regular use of the Internet for malicious purposes, such as recruitment for terrorist groups via social media, is not part of this definition of cyber threats. In this assessment, the CFCS outlines and assesses activities whose purpose is to:

- Conduct espionage via the Internet
- Carry out crimes of acquisition via the Internet
- Launch activist actions via the Internet
- Perform terrorist attacks via the Internet

The CFCS also gives an account of state involvement in destructive attacks via the Internet.

The threat levels depend on the actors' intentions and cyber capabilities.

The CFCS judges an actor's cyber capabilities based on its available human and material resources. These may include technically skilled hackers and developers of malware or knowledge of targets that is useful for social engineering. Resources may also include IT infrastructure, time, money and access to information. The cyber capability level will thus depend on several types of resources and the ability to combine them. Consequently, the CFCS may rate an actor with great technical skills who lacks the requisite infrastructure or knowledge about a target low in terms of cyber capabilities. The same holds true of an actor with extensive knowledge on a target but who lacks the technical know-how to exploit this knowledge.

The assessment is based on the current threat picture whose warning horizon is 0 to 2 years. However, due to the dynamic nature of the cyber threat, the threat picture may in some respects change overnight both generally and as regards the threat facing the individual authority or company.

Definitions and cyber terms used throughout the assessment as well as the threat levels and probability degrees applied by the DDIS are included at the end of the report.

Cyber espionage

The CFCS assesses that the threat from cyber espionage against Danish authorities and private companies is **VERY HIGH** and mainly posed by foreign states. In recent years, the CFCS has noted an increase in attacks by states and in continuous attempts at compromising Danish authorities and companies.

Foreign states may be interested in spying against Denmark based on strategic, political and commercial considerations. Thus, the purpose of cyber espionage may be to gain insight into political preparations ahead of key negotiations or to copy a company's products and intellectual property in a bid to obtain a competitive edge.

If states succeed in obtaining unauthorized access to valuable data such as information on national security policy or politically hot topics, for instance the Arctic, the repercussions could be highly detrimental to Denmark. In addition, such access may harm the reputation of Danish authorities and companies, undermining the trust of citizens, clients and partners.

Several state or state-sponsored hackers hold both the ability and the resources to launch sophisticated cyber attacks in which compromise of information can be difficult to detect. These hackers are skilled at adjusting to new technologies and they are continuously improving at concealing their activities and identities.

Russia – a leading actor in the cyber realm

Russia has long invested intensively in its cyber capabilities and now holds sophisticated capabilities to launch extensive cyber espionage campaigns against political and military targets in the West. Russia also has access to cyber capabilities suited to bolster the country's conventional military operations, for example targeted operations against critical infrastructure.

Chinese cyber espionage

China's cyber espionage capabilities are quite extensive. Several Chinese authorities, including the Chinese military, have publicly been criticized in the West for orchestrating large scale espionage via the Internet against a large number of targets abroad. China uses its cyber capabilities for obtaining information of economic, political and military importance.

Foreign states interested in foreign and security issues

Though the threat from cyber espionage is directed against the entire spectrum of Danish state activities, authorities engaged in Danish foreign and security policy are high-risk targets of cyber espionage attempts. The CFCS knows of several attempts at cyber espionage against the Danish Ministry of Foreign Affairs and the Ministry of Defence and affiliated agencies.

State-sponsored hacker group attacks Danish ministries

In 2015 and 2016, the same foreign actor repeatedly tried to access information from the Danish Ministry of Foreign Affairs and the Ministry of Defence and affiliated agencies through different kinds of cyber attacks. These attacks included spear phishing campaigns to lure the targeted individuals into revealing their email login information. Attempts have also been noted to access email accounts through automated testing of thousands of passwords. The CFCS assesses that a foreign state-sponsored hacker group was responsible for these attacks and that the threat is persistent.

The threat against private companies is particularly directed against research-intensive and high-tech industries and companies engaged in specific geographic areas. In recent years, state actors have specifically targeted such companies. Sub-contractors and service companies affiliated with these industries are also the targets of attacks as they often have access to sensitive information.

In 2016, the CFCS published sector-specific assessments of the threat from cyber espionage against, among others, the defence and aerospace industry and Danish public research. The repercussions of cyber espionage for the affected companies or research institutions include reduced competitiveness and loss of intellectual property.

Hacking into political research fields may provide foreign states with insight into the research and advice on which the Danish government and parliament base key decisions. Through compromise of other research fields, states may seek to obtain a competitive and commercial edge by tapping into Danish research efforts and research results before they are published.

As more states are increasing their cyber capabilities, it is likely that they will attempt to launch attacks, as industrial espionage and intellectual property theft are ways to strengthen economic development without major costs or risks. The threat posed by regional threat actors against Danish representations abroad may also intensify as a reflection of the increased cyber capabilities in several states.

States use 'hack and leak' to impact internal affairs in other countries

Experience from abroad shows an increase in the attempts by foreign states at using cyber espionage to influence political and democratic processes as well as popular opinion in the public domain. Influence campaigns between states are not a new phenomenon, but using cyber capabilities is a recent development. In a so-called 'hack-and-leak-operation', actors obtain access to information that they subsequently leak, often selectively. This may include the leaking of private emails and confidential documents that put politicians in a bad light prior to elections.

The ambition to influence internal affairs in other countries may also be economically motivated or reflect a desire to counter what some states perceive as Western attacks on their values and culture. Some states perceive themselves to be engaged in a war of information against the West and believe that the West escalates conflicts through its media and use of soft power.

In 2016, both the United States and Germany publicly announced that state actors were responsible for hacks against parties and politicians and subsequent leaks of information. Examples include the leak following the hack against the Democratic National Committee in the United States and an increase in the number of spear phishing attacks against German parties, which the German security service labels an attempt at influencing the upcoming federal elections.

Not only political parties or authorities are targets of hack-and-leak-operations. The so-called Sony hack from 2014 is an example of a cyber attack, where multiple strategies were used, including hack and leak.

Hackers attacked film company and leaked personal data and emails.
In 2014, the Sony Pictures Entertainment film company was hacked. The company's computers were

infected with destructive malware that ruined data and systems, and the hackers gained access to intellectual property and confidential information. Subsequently, the hackers leaked emails that incriminated the senders, personally sensitive and medical information about employees, managers' salaries, copies of unreleased films and other information. The hack resulted in a number of lawsuits against Sony Pictures from former employees and massive criticism of the company's handling of the case. In the Sony case, the United States attributed the hack and leak to a state actor with a political motive.

In other contexts, attempts at influence and the poorly concealed use of information obtained through cyber espionage may be a reaction to sanctions or a way to project power. Based on a 'divide and conquer' principle, states may also try to influence relations between other countries and destabilize alliances such as the EU or NATO. States may also try to sway public opinion on issues such as regional secession from nation states. Cyber espionage is not the only means to this end as states extensively use classic propaganda tactics and misinformation campaigns, for instance on social media.

Cyber crime

In this threat assessment, the term cyber crime covers incidents in which perpetrators use IT to commit criminal acts with the purpose of enrichment, including theft of money or financial information, fraud and extortion. The focus is on crimes against authorities and companies or acts against larger groups of individuals that impact on companies, such as attacks against the clients of a bank. The CFCS bases its assessment on, among other things, information from the Danish Police's National Cyber Crime Center (NC3) and assesses that the threat from cyber crime against Danish authorities and private companies continues to be **VERY HIGH**.

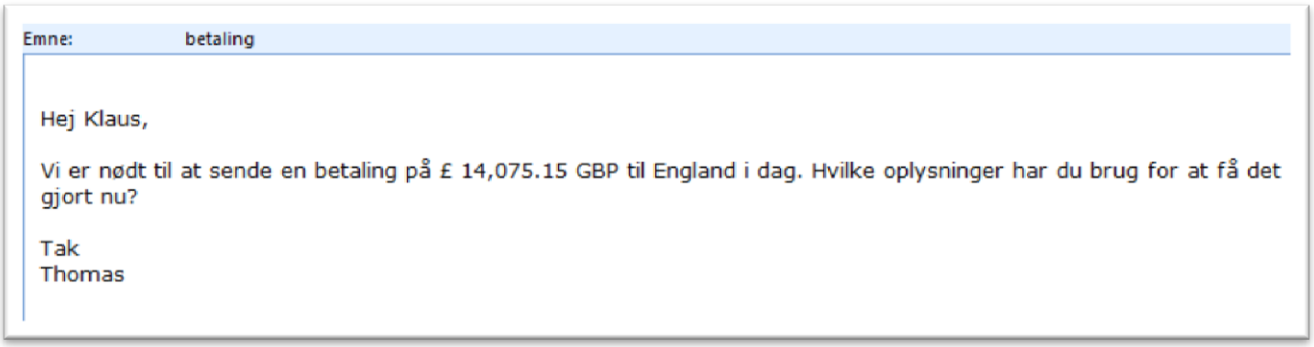
Organized criminals lure money from Danish companies

NC3 informs that 2016 saw a steep increase in incidents of so-called Business Email Compromise (BEC) scams. These scams involve actors using social engineering to lure the staff of a company to transfer money or inadvertently grant access to systems believing that they act on orders from the management.

Such incidents are increasingly linked to organized crime in which the hackers behind BEC scams have set up 'firms' specialized in this kind of scam. The criminal firms have staff trained in special language fields or staff responsible for profiling the employees of the targeted company to uncover their access areas and to determine who will be the most inclined to believe a false email. The firms also have sub-contractors used for activities such as money laundering.

The CFCS has information from NC3 that in 2016, a number of these firms have targeted Danish companies across sectors.

Particularly the latter half of 2016 saw such attacks against Danish companies. During this period, police-reported cases alone show losses for Danish companies exceeding DKK 180 million. Such losses naturally impact significantly on the affected companies and may also hold severe personal repercussions for the employees that fell for the scams.

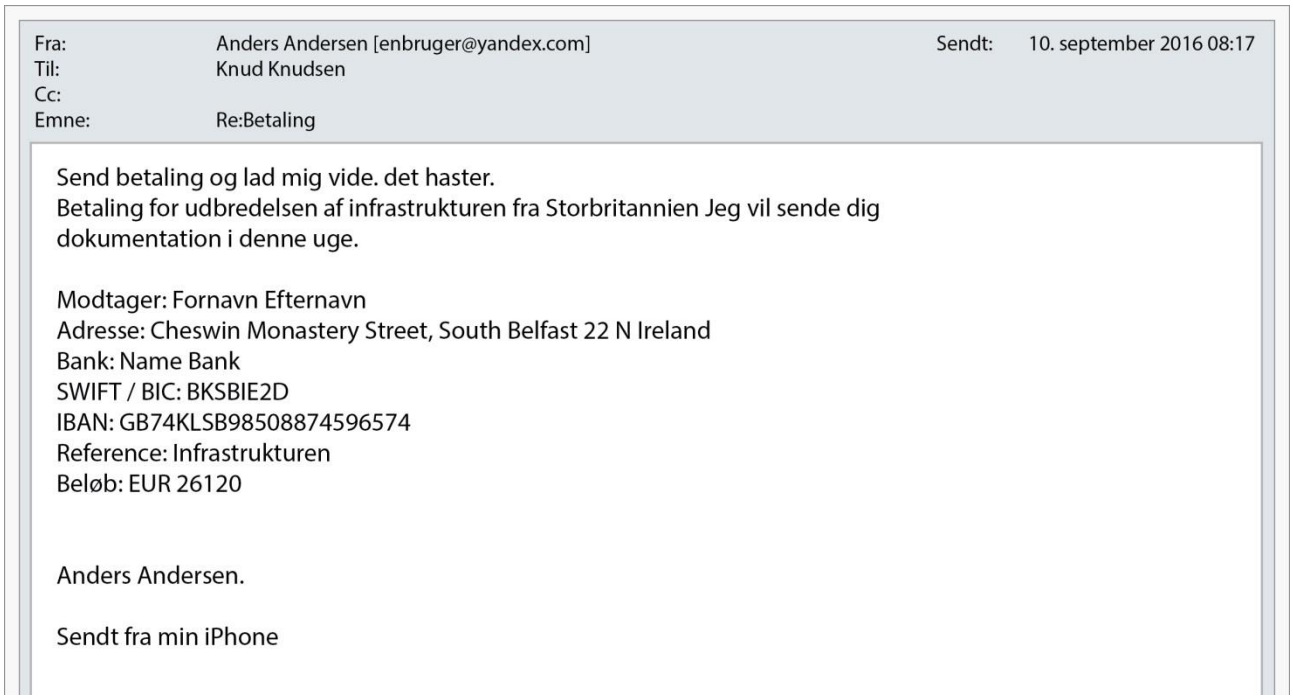


Emne: betaling

Hej Klaus,

Vi er nødt til at sende en betaling på £ 14,075.15 GBP til England i dag. Hvilke oplysninger har du brug for at få det gjort nu?

Tak
Thomas



Fra: Anders Andersen [enbruger@yandex.com] Sendt: 10. september 2016 08:17
Til: Knud Knudsen
Cc:
Emne: Re:Betaling

Send betaling og lad mig vide. det haster.
Betaling for udbredelsen af infrastrukturen fra Storbritannien Jeg vil sende dig dokumentation i denne uge.

Modtager: Fornavn Efternavn
Adresse: Cheswin Monastery Street, South Belfast 22 N Ireland
Bank: Name Bank
SWIFT / BIC: BKSBIE2D
IBAN: GB74KLSB98508874596574
Reference: Infrastrukturen
Beløb: EUR 26120

Anders Andersen.

Sendt fra min iPhone

Examples of false emails from BEC scam attempts in Denmark. The first email attempts familiarity. The second, though written in poor Danish, gives instructions on where to transfer money. All names, addresses and emails have been changed.

Hackers have also been known to gain direct access to banks and payment systems and make transfers themselves. That was the case in a 2016 incident in Bangladesh that has been dubbed the greatest Internet bank robbery ever.

Central bank loses 100 million dollars due to cyber attack

In February 2016, hackers gained access to systems at Bangladesh's central bank and tried to transfer USD 951 million to false back accounts in different locations in the world via the global interbank financial system SWIFT. The hackers succeeded in transferring approx. USD 100 million before the attack was detected and stopped. Security companies have linked the attack to similar attacks against banks in other countries.

Cyber criminals also peddle their services via online black markets. These services include tools for Distributed Denial of Service (DDoS) attacks and malware for ransomware attacks. This concept is called 'crime as a service', and the characteristics assigned to state-sponsored hackers, cyber criminals and other malicious actors, respectively, have become increasingly blurred. Crime as a service makes it possible for criminals without major IT skills to commit cyber crime. Bitcoin and other digital currencies are the payment methods of choice when cyber criminals charge for their services or demand ransom in connection with ransomware attacks.

Ransomware is an increasing problem

Ransomware is among the most prominent cyber crime threats. In addition to private individuals, hackers direct ransomware attacks against companies in particular, but also against authorities and public institutions. If the attack is successful, malware is installed that encrypts data and demands ransom to restore the victim's access to his or her data. Ransom is usually demanded in Bitcoins. The hackers very often use phishing and social engineering to make their victims click on links in emails, text messages or advertising banners that install malware. The human factor is thus of major importance in the efforts to avoid falling prey to ransomware. To a company or organization falling victim to a ransomware attack will often entail inability to perform certain tasks and functions as long as the attack is ongoing.

Denmark has particularly seen broad ransomware campaigns in which hackers target multiple targets at a time without refining or customizing the wording used in emails or text messages. Still, it is highly likely that hackers will assess a target's value and readiness to pay in order to determine the level of the ransom before attacking.

Ransomware attacks against foreign hospitals

Several hospitals in the United States, the UK and Germany have been the targets of ransomware attacks. Hackers have encrypted emails and patient charts and left messages on staff computers that they must pay ransom to have the data encrypted. In at least two incidents in 2016, cyber attacks

impacted directly on the treatment of patients in US hospitals. In the UK, a hospital was forced to postpone transplant surgery and other operations due to a ransomware attack. In other cases, hospitals have chosen to pay the ransom.

Excerpt from a UK hospital homepage following cyber attack that forced the hospital to postpone operations

Distributed Denial of Service attacks grow increasingly sophisticated

Distributed Denial of Service attacks, also known as DDoS attacks, are among the methods used by cyber criminals. The attacks are frequently seen in the financial sector and the online retail industry, among others. DDoS is not only a threat to the main target of the attack but also to the tele infrastructure transferring the attack, which means that indirect victims also can be exposed to interrupted or slow tele services. The CFCS assesses that the threat from DDoS attacks constitutes the key threat to the availability of the Danish tele services, though they remain skilled at protecting against and averting such attacks.

The most serious DDoS attacks are continuously getting stronger and more sophisticated, just as an increase has occurred in the use of 'booters/stressers'. These are online tools developed to stress test servers with DDoS attacks but which can also be used for malicious purposes. DDoS can also be used for attempts to divert attention from other serious cyber attacks.

Organizations with access to medical and personal data and intellectual property are also targets of DDoS attacks. The purpose of such attacks is to blackmail the organizations into paying for the attack to stop and to regain access to own data.

Hacks against bank accounts and payment cards affect both clients and companies

The financial sector is a natural target of cyber crime. Companies within the financial sector are not only exposed to cyber attacks directed against the company's own systems and infrastructure, their clients are targets as well. This is the case in connection with criminals trying to access client accounts in Danish banks or conduct payment card fraud. Cyber crime is also a problem for legitimate web shops with hackers trying to exploit vulnerabilities in their payment systems to redirect payments or steal payment card information from their customers. Here, cyber criminals can tap into a vast market as 77 per cent of the Danish population between ages 16 and 89 have shopped online for items like clothes, travels, leisure and recreation events and everyday goods, and the trend is on the rise.

Nets recommends that Danish banks replace 100,000 payment cards after online fraud

In September and October 2016, Nets - provider of payment products, including payment cards, in Denmark - became aware that payment cards that were issued in Denmark and used online were increasingly being exploited. Nets publicly announced that the source of the exploitation was a foreign webshop and that a large amount of personal card information had been compromised. Nets recommended that the Danish banks, which are responsible for issuing payment cards in Denmark, replaced an initial 15,000, and subsequently 100,000 cards in a pre-emptive measure. The incident was one of the biggest potential compromises of payment cards seen in Denmark so far.

Over the first three quarters of 2016, Danish banks reported 970 attempts to FinanceDenmark, the Danish Bankers Association, by cyber criminals at accessing Danish online banks by luring information from bank clients. FinanceDenmark has not yet released the numbers from the fourth quarter, but confirms a large increase in the last quarter of 2016. Using phishing, smishing and social engineering, cyber criminals lure bank clients into revealing their personal account information, either directly or by luring them to enter false websites that look like their online home banking sites.

Cyber activism

Cyber activism is typically driven by ideological or political motives. Cyber activists may focus on single issues, individuals or organizations which they perceive as opponents of their cause. Despite capabilities in cyber activist communities, the CFCS only has knowledge of a limited number of cyber activist attacks against Danish authorities and companies and assesses that the overall threat from cyber activism is **MEDIUM**.

However, there are examples of warnings of and calls for cyber activism that have not resulted in actual incidents.

#OpIcarus campaign screendump from Opicarus blog

Illustrative of this were the calls for and warnings of hacker attacks against major financial institutions globally, including the Danish National Bank, in 2016 by an alleged fraction of the Anonymous hacker community on social media. The people behind the calls for attack referred to a campaign that Anonymous launched in 2011 called #OpIcarus, which has also been linked to the physical manifestation 'Occupy Wall Street'. The 2016 warning did not, however, result in actual attacks in Denmark.

Due to the case-by-case nature of cyber activism, the threat may increase overnight for a specific authority, company or private individual that catch the attention of cyber activists. In addition to DDoS attacks and defacement of websites or other types of harassment, cyber activists also use leak of sensitive information obtained through hacking of, for instance, personal email accounts.

Danish hackers found guilty of leaking politicians' personal information
In 2016, two Danish men were found guilty of politically motivated hacking of websites belonging to 101 companies and organizations. In 2014, the two men hacked into the systems of the Socialist People's Party (SF) and gained access to party members' personal data. The hackers published the names, addresses and social security numbers of 22 SF politicians and 91 members of the Danish parliament. The hackers allegedly intended to harass politicians who had voted in favour of the Centre for Cyber Security Act, which the hackers perceived as a violation of privacy.

State actors also use cyber activism as a cover in local conflicts and to shape public opinion. This kind of activism is termed 'false flag' and is outlined in subsequent sections.

Cyber terrorism

In this threat assessment, the term cyber terrorism refers only to the use of the Internet as a vehicle to launch a terrorist attack causing death or massive material damage. Thus, the term cyber terrorism does not cover terrorist groups' use of the Internet for other malicious purposes such as cyber harassment, including website defacement, or criminal acts aimed at raising funds for terrorism. Known terrorist groups' use of social media for recruitment and propaganda

purposes is not considered cyber terrorism either. The CFCS assesses that the threat from cyber terrorism against Denmark is **LOW**.

The CFCS assesses that actors who have been known for attempts or have expressed intent to launch conventional terrorist attacks, such as militant Islamist groups, do not at present have the necessary capabilities to execute acts of cyber terrorism. Even though militant Islamist groups likely want to develop cyber attack capabilities, doing so is not a high priority for them in the short term.

However, the threat will increase if terrorist groups manage to recruit technically skilled members or if established hackers become radicalized. The threat picture may also change, if terrorists choose to purchase services on the black markets of the Internet.

If terrorist groups manage to bolster their cyber skills, a number of potential scenarios are conceivable. For instance, terrorists could use cyber capabilities to amplify the effect of a conventional terrorist attack or receive assistance from state actors who are interested in launching destructive cyber attacks under false flag.

Destructive cyber attacks

In this threat assessment, a destructive cyber attack is defined as a tool that can be used by various actors for different purposes. Thus, the intended effect of a cyber attack determines whether or not a cyber attack is defined as destructive. Therefore, 'destructive cyber attacks' does not constitute its own threat category on a par with cyber espionage or cyber terrorism. Nevertheless, it makes sense to describe and assess the threat from state-sponsored destructive attacks, in particular, as certain states have the necessary cyber capabilities to launch destructive cyber attacks.

The term destructive cyber attacks refers to cyber attacks resulting in death, personal injury, extensive damage to physical objects or destruction or manipulation of information, data or software, rendering them unusable.

There are several examples of foreign states launching cyber attacks against industrial control systems abroad. The cyber attacks can be used in a hybrid with more conventional attacks and physical enablers, for example insiders. Hackers often use spear phishing attacks to spread malware and gain access to user names and passwords, allowing them to take over control of the system. So far, state-sponsored attacks have mainly caused inconvenience, sent political messages or been about retaliation, but without causing serious damage or loss of life.

The CFCS assesses it less likely that foreign states with destructive cyber capabilities will launch actual destructive cyber attacks against industrial systems or critical infrastructure in Denmark.

However, if a political or military conflict arises between Denmark and such a foreign state, Danish infrastructure and systems can become targets for this type of cyber attacks.

Cyber attacks caused blackout in Ukraine
In December 2015, a number of electricity companies in western Ukraine fell victim to a cyber attack. The hackers gained access to the electricity companies' control systems and cut the power in the targeted region. Half of the residents in the region were left without electricity for up to 6 hours. Open sources report that a foreign state was responsible for the attack, and that there have been several other attempts at compromising Ukrainian electricity companies and other targets in the country in 2016.

In Saudi Arabia, companies and authorities in energy, air transportation and other sectors have been attacked multiple times with the so called Shamoon malware, which deletes data on a computer's hard disk. The abovementioned Sony hack and the attack on TV5 Monde outlined below are also examples of destructive cyber attacks.

Development trends and methods transverse threats and threat actors

Whether the purpose is espionage, criminal activity, activism or terrorism, there are methods that transverse the type of cyber threats. For instance, the use of DDoS attacks, phishing campaigns and social engineering is not specific to one purpose. Different hackers will exploit the same vulnerabilities or technological development, and the same hacker or hacker group may in various connections play different roles and conduct their illegal activities for different purposes.

Advanced cyber attack tools are increasingly available to more people. Cyber capabilities that mainly used to be available to state actors are now to some extent also used by cyber criminals and cyber activists.

It may prove difficult for investigators to distinguish between attackers if the hackers purchase infrastructure on the black market. In addition, the identity of physical actors is to some degree concealed in the cyber realm, forcing investigators to attribute cyber attacks to specific hacker groups and cyber personas based on IP addresses, activity patterns, methods and motives. Because the methods transverse the different objectives, it may be difficult to attribute attacks to specific actors, enabling different actors to carry out so-called false flag attacks. False flag operations allow attackers to make an attack appear to have been executed by someone other than the real perpetrator in a bid to maintain anonymity, divert attention from the real purpose of the attack or have someone else appear as the sender of the message. For instance, state actors may pose as political activists or terrorists.

Cyber activism against TV5 Monde looked like a terrorist attack

On the evening of 8 April 2015, French TV station TV5 Monde's 12 channels went off air. The station had been exposed to a very advanced cyber attack. A group calling itself 'the Cyber Caliphate' claimed responsibility for the attack on social media, leaving the media wondering if ISIL was behind the attack. Investigators have since then raised serious doubts as to whether ISIL was in fact the perpetrator and have instead linked the attack and the advanced methods used in the attack to a state-sponsored hacker group.

A hacker's job is not only about technical skills or system vulnerabilities. The human factor also enters into the equation. Phishing campaigns and social engineering are widespread techniques used to penetrate the first barriers of an organization and circumvent even updated and advanced systems. Hackers not only advance their malware, they also continuously improve the quality of phishing emails or create fake domains that are almost identical to the real ones.

There have been several recent examples in Denmark and abroad in which hackers have sent credible spear phishing emails to official authorities or lured employees to enter their login details on fake login pages. Also an increasing number of hackers develop their skills to use legitimate websites to create watering holes and the users of the website with malware.

Some hackers increasingly use malware to target mobile phones. As mobile phones increasingly are also used as small computers, malware used to attack mobile devices is becoming more complex. The attack methods increasingly resemble methods used to attack actual computers. In this context, attackers also use social engineering, for instance by sending false text messages containing malware, so-called smishing.

Hackers may take advantage of people's increased use of cloud services to store data or access services via social media, webmail or to create backup of data on mobile phones. Cloud computing creates r new opportunities for the use of social engineering. For instance, hackers can gain access to sensitive information by sending false messages to users claiming that their passwords to email accounts or social media accounts are about to expire and luring them into clicking on links directing them to fake websites infected with malware. Companies can use cloud storage and access their data via the Internet, making the infrastructure of the cloud host and the company's data vulnerable to cyber threats on the Internet.

The increase in the use of Internet of Things (IoT) opens up new possibilities for threat actors. Forecasts from international IT and telecommunication companies estimate that in 2020 approximately 26 billion devices will be connected to the Internet. More people use such devices as for example refrigerators, lamps, cameras or virtual assistants. If good security practices are not implemented, new risks of compromise arise. Individual users may not be the intended target.

However, the increasing number of Internet-connected devices enables hackers to gain access to a target in more ways. Users may not be aware that hackers can gain access to a smart TV with a built-in microphone in a conference room, for example. Also, the numerous units may be used in so-called botnets, which can be used to launch DDoS attacks and cyber attacks against other and larger targets.

Baby monitors and DVD players brought down Netflix, PayPal and Twitter
In October 2016, a US domain host was exposed to a DDoS attack from a botnet. The attack created major availability problems for known Internet sites like Amazon, BBC, Fox News, the Guardian, Netflix, PayPal, Spotify and Twitter. A number of government websites in Europe were also affected. The hackers used compromised smart units such as cameras, printers, DVD players and baby monitors in the attack. Most of the units belonged to private individuals or small businesses.

It is also possible that cyber criminals will exploit the increased use of smart units in the future to hack devices and render them useless in order to extort money from the users. Or hackers may launch attacks against larger single targets such as future smart cars, smart container ships or smart cities.

Some actors launch campaigns that involve scanning a wide range of IT networks to systematically uncover vulnerabilities in the systems. In 2015-16, the CFCS detected numerous attacks targeting the vulnerabilities in a specific IT system used by several Danish organizations. The CFCS assesses that the attacks are not always direct attempts at espionage or criminal activity against the specific organization, but merely hackers looking into the possibility of installing backdoors in the systems or creating botnets in order to test attack scenarios or for later attacks against other priority targets.

Recommendations

The CFCS recommends that the management in public authorities and private companies raise their awareness of the cyber threat and seek information and advice on how to protect themselves against cyber threats.

Public authorities and private companies should make targeted efforts to improve processes, technology and behaviour. Processes include preparing regular risk analyses and identify which data requires protection and what the consequenses of a potential breach would be. Technology could involve improving knowledge of in-house IT infrastructure and processes and regular identification and patching of system vulnerabilities. Behaviour involves initiatives aimed at raising user awareness of the cyber threat and establishing staff training programmes that teach

employees safe cyberspace behaviour. In addition, companies and public authorities should implement cyber attack contingency plans.

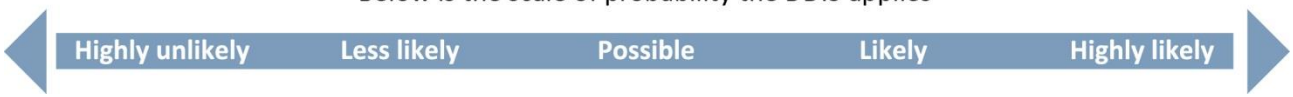
The CFCS recommends that public authorities and private companies follow the ISO 27000 standards as described by the Danish Agency for Digitisation.

In addition, it is crucial to hire people with the right skills to handle cyber security before a potential attack takes place.

The CFCS recommends that public authorities and private companies furthermore seek information on the nomoreransom.org website – an international collaboration in which the Danish National Police participates.

Centre for Cyber Security
February 2017

Below is the scale of probability the DDIS applies



Threat levels

The Danish Defence Intelligence Service uses the following threat levels:

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

Terms and definitions

- BEC scams: BEC stands for Business Email Compromise and is also known as 'CEO Fraud'. Rather than sending emails to a large group of random employees within a company, hackers create highly customized and credible emails that are ostensibly from the director, CEO or executive consultant to a member of staff. The purpose of the email is to entice the employee to act in the belief that it is under orders from the management.
- Botnet: Botnets are networks made up of remote-controlled computers infected with malware, allowing hackers to launch DDoS attacks.
- Cloud computing: The term is often referred to simply as the 'cloud' and covers the delivery of software and services over the Internet. Social media and online services such as Hotmail or Yahoo mail are examples of cloud computing, where the applications are saved in the cloud rather than on local computers. Data storage and backup services can also be provided by a cloud host. Unlike traditional hosting, which depends on just a single server, cloud hosting makes data available and accessible via multiple servers.
- DDoS attack: DDoS stands for Distributed Denial of Service and is an attack that renders websites and online resources unavailable to its intended users by flooding the target website or network with superfluous requests in order to overload the system and prevent legitimate requests from being fulfilled. The superfluous requests often come from compromised computers and devices that the hacker controls.
- Defacement: Website defacement is an attack on a website that changes the visual appearance of the site. For instance, hackers may add images or text to the site.
- False flag: False flag operations refer to covert operations designed to make a cyber attack appear to have been executed by someone else than the real perpetrator. Another phenomenon within this category is faketivists, which are fictitious personas created to emulate activists who then act as a public mouthpiece and thereby provide plausible deniability for a hack or information leakage.
- Internet of Things: Is also known simply as IoT, and refers to everyday devices, such as refrigerators or cameras, that are connected to the Internet. The devices are thereby able to transmit and receive data.
- Encryption: Encryption translates data into a secret code that renders information unintelligible to a third party. Encryption is often used to ensure that information transmitted via non-secure communication channels such as the Internet is not intercepted and read by unauthorized parties. However, hackers may also use encryption techniques to make data unintelligible for the owner of the data until a ransom is paid.
- Malware: Malware or malicious software refers to a program that is doing malicious, harmful or unwanted things, where it is installed.
- Phishing: Phishing is an attempt to trick users into disclosing sensitive information by clicking on files containing malware or embedded links to fake websites. Phishing often involves sending emails to a wide range of users.
- Ransomware attacks: Hackers try to install malicious tools encrypting data on the victim's computer or system. The hackers demand ransom in exchange for decrypting the data.

Hackers will often infect computers with malware by means of phishing, maybe targeted through social engineering. Most ransomware attacks are successful because the users have clicked on something embedded in an email, text message or online pop-up ads.

- Social engineering: Social engineering is an attack vector where the victim is manipulated into performing certain actions or divulging classified information. In the context of IT security, the term is used to describe the design of seemingly legitimate emails or websites that contain malware. Social engineering requires knowledge of the victim to be effective.
- Smishing: Smishing is phishing via text message.
- Spear phishing: Spear phishing differs from phishing in that spear phishing attacks target specific individuals. Spear phishing emails are often tailored to the specific recipient so they appear relevant and credible and they often appear to come from a trusted source.
- Watering hole: A watering hole is an attack vector where an otherwise legitimate website is infected with malware. Users who normally use the website without problems risk becoming infected with malware.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu