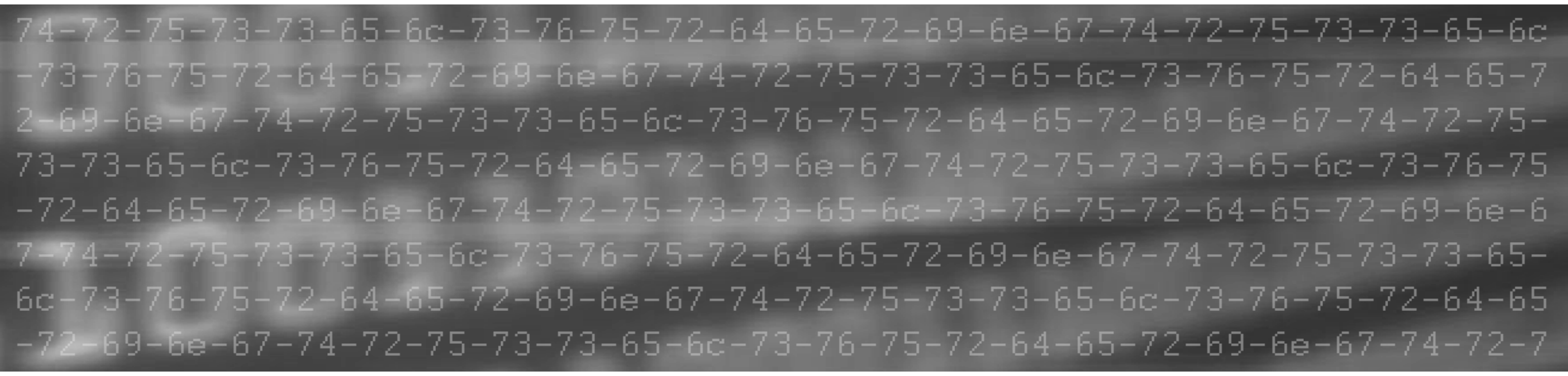
CENTRE FOR
CYBER SECURITY

FE

Threat Assessment

The cyber threat against the Danish telecommunications sector


74-72-75-73-73-65-6c-73-76-75-72-64-65-72-69-6e-67-74-72-75-73-73-65-6c
-73-76-75-72-64-65-72-69-6e-67-74-72-75-73-73-65-6c-73-76-75-72-64-65-7
2-69-6e-67-74-72-75-73-73-65-6c-73-76-75-72-64-65-72-69-6e-67-74-72-75-
73-73-65-6c-73-76-75-72-64-65-72-69-6e-67-74-72-75-73-73-65-6c-73-76-75
-72-64-65-72-69-6e-67-74-72-75-73-73-65-6c-73-76-75-72-64-65-72-69-6e-6
7-74-72-75-73-73-65-6c-73-76-75-72-64-65-72-69-6e-67-74-72-75-73-73-65-
6c-73-76-75-72-64-65-72-69-6e-67-74-72-75-73-73-65-6c-73-76-75-72-64-65
-72-69-6e-67-74-72-75-73-73-65-6c-73-76-75-72-64-65-72-69-6e-67-74-72-7

Threat Assessment Branch under the Centre for Cyber Security

February 2017

February 2017

Threat assessment: The cyber threat against the Danish telecommunications sector

This threat assessment outlines existing cyber threats against the Danish telecommunications sector. Telecommunications are of vital importance to the functioning, stability and security of Danish society.

Key Assessment

- Exploitable by all types of cyber criminals, DDoS attacks constitute the greatest threat to the accessibility of telecom services, just as they pose a threat against the business operations of the telecommunications industry. The threat from DDoS attacks is assessed as **VERY HIGH**.

- Like other Danish companies and authorities, the telecommunications sector is the target of an extensive threat from cyber criminals. The threat from cyber criminals against the telecommunications industry is assessed as **VERY HIGH**.

- The aim of cyber espionage against the telecommunications sector is to gain access to sensitive data and customers and to exploit vulnerable infrastructure. The threat from cyber espionage against the telecommunications sector is assessed as **HIGH**.
- Cyber activism is a relatively rare phenomenon in Denmark, and CFCS assesses that the threat from cyber activism against the telecommunications sector is **MEDIUM**. However, if single issues draw the attention of activists, the threat level may suddenly rise.
- Even though cyber crime poses a serious threat to the telecommunications industry, CFCS assesses that the threat from cyber crime against the telecom services is **LOW.**
- CFCS assesses that the threat from destructive cyber attacks conducted by foreign states, including attacks against the telecommunications sector, is currently **LOW**. However, the threat has the potential to increase in connection with deepening political or military conflicts in which Denmark is involved.
- CFCS assesses that no terrorist group currently has sufficient capability to launch full-blown online terrorist attacks against the telecommunications sector. Consequently, the threat from cyber crime is assessed as **LOW**.

Introduction

This threat assessment describes the cyber threats against the Danish telecommunications sector. The assessment is prepared by the Threat Assessment Unit under the DDIS Centre for Cyber Security (CFCS) and outlines the cyber threats against the telecom services and service providers. The purpose of this threat assessment is to advise telecommunications companies about the cyber threat in order to facilitate the best possible counter measures.

The assessment firstly outlines the cyber threats that may disturb the availability, confidentiality and integrity of the telecom services. From a societal perspective, these are the most severe threats as they target critical infrastructure. Such threats include DDoS attacks and cyber espionage.

Secondly, it is an assessment of the cyber threats that target the telecom service providers' business, including cyber crime and cyber espionage which are among the most serious threats against the business.

The Danish telecommunications sector is defined as the commercial service providers that publicly provide the telecommunication services and infrastructure which allow authorities, companies and citizens to communicate electronically. Typical telecommunication companies comprise the service providers of fixed lines, mobile telephony and satellite telephony as well as the Internet Service Providers (ISP) providing Internet connections, and the companies providing corporate network solutions.

Before the digitization of the Danish telecommunications infrastructure in the eighties, the telecommunications network was primarily used for voice traffic. Though this function was essential for society, a brief disconnect of the telecommunications network would not seriously upset the operations of most authorities and companies. However, this is not the case today. Published in 2014, The National Strategy for Cyber and Information Security highlights the need for increased cyber security in the telecommunications sector, stating that the telecommunications sector is vital to the functioning, stability and security of Danish society. The telecommunications sector has evolved from being a provider of voice services to being the provider of the digital platforms on which the services provided by other critical sectors depend.

To identify the cyber threats against the Danish telecom services, it is important to understand these services as well as the core areas that support them:

- **Telecom service**
  A telecom service is an electronic communications service, which transfers voice, images, text messaging or combinations of these between so-called network termination points. A network termination point may be a router, TV receiver box, computer, mobile phone, etc. Telecom services include mobile telephony, fixed telephony, Internet access, coast radio and broadcasting as well as other types of radio and television programme transmissions.

- **Telecommunications infrastructure**
  The telecommunications infrastructure comprises the equipment and transmission connections which form the basis of the services provided by a telecom service provider. A segmented

telecommunications infrastructure with multiple networks ensures an infrastructure that is more resilient against cyber attacks. This segmentation is facilitated by the existence of multiple telecom service providers with individual telecommunications infrastructure.

- **Telecom service providers**
  Telecom service providers own and operate the telecom infrastructure. In practice, this means that the availability of the telecom services depends on the existence of these private-owned companies and their access to resources that are necessary to establishing and operating the telecom infrastructure. The telecom service providers are largely dependent on the systems, tools and data stored on their administrative networks. As these networks – unlike many of the control systems in the telecommunications infrastructure – are often directly connected to the Internet, they are potential targets of cyber attacks.

- **Subcontractors**
  The telecom service providers often depend on subcontractors to operate their business and maintain their telecom services. Their tasks range from establishment and operation of telecommunications infrastructure and administrative networks to service tasks such as cleaning and maintenance of buildings and installations. Subcontractors may have access to sensitive information via the telecom service provider, either via data connections between the telecom service provider and the subcontractor or via physical access to the service provider's documentation, administrative network or telecom infrastructure. As a result, cyber attacks against a telecom service provider may also be launched via subcontractors.

- **Operations centres and field service**
  In an effort to prevent system failures and technical breakdowns, operations centres conduct round-the-clock monitoring, adjustments and error control of the telecommunications infrastructure, and so-called field service technicians conduct daily inspections and repairs of the infrastructure. The competence and daily routines of the operations centres to detect and correct errors help mitigate the effects of destructive and disturbing cyber attacks.

- **The power supply**
  Threats against the energy sector are not included in this assessment. Nevertheless, it is important to mention that without a stable power supply system, the telecom infrastructure would collapse. Network components and operations systems would shut down or equipment would break down due to insufficient cooling. Emergency power or battery back-up is frequently installed on vital infrastructure elements, but battery back-up in particular only mitigates the effect of brief power outages.

The potential impact of cyber threats on the telecom services

Generally, the telecom service providers and the critical telecommunications infrastructure are relatively resilient against cyber attacks. Disruptions in the telecom services are most often caused by hardware errors in the telecommunications infrastructure, severed cables or other incidents that are unrelated to the cyber threat.

However, the telecommunications sector is exposed to a number of serious cyber threats targeting the telecommunications infrastructure, and the telecom providers and its customers. If the cyber threats are in fact carried out, this could compromise the accessibility, confidentiality and integrity of the telecom services. The most serious and visible threats are the ones directed against accessibility, while threats to confidentiality or integrity may make it impossible or inadvisable to use a certain telecom service in situations where confidentiality and integrity are vital for the user.

The threat from DDoS attacks

Distributed Denial of Service attacks, so-called DDoS attacks, constitute the greatest threat to the accessibility of the telecom providers. These attacks occur frequently and may target authorities, companies and citizens. DDoS attacks are carried out online and, to a lesser extent, via mobile networks, against telecom service providers, their customers, and the telecommunications infrastructure.

The telecommunications sector is quite resilient against DDoS attacks, and it is mostly the telecom customers that suffer when DDoS attacks are launched. However, based on the frequency of these attacks combined with the fact that DDoS attacks are launched via the telecommunications infrastructure, thus affecting the accessibility of the telecom services, CFCS assesses that DDoS attacks constitute the greatest threat against the availability of the telecom services and that this threat is **VERY HIGH**.

DDoS
Distributed Denial of Service (DDoS) is a cyber attack in which an attacker exploits compromised computers to generate an overwhelming amount of data traffic against a web server or network, making the web server or the network unavailable during the attack.

DDoS attacks are the tools of trade of online gamers, who want to annoy their opponents; and cyber criminals who test companies' security levels, demanding money to stop an attack or using DDoS attacks to mask more serious cyber attacks. Controlled DDoS attacks are also launched legally by, for instance, security companies to test a company's resilience against this type of attack.

Cyber criminals likely used a DDoS attack to divert attention when hackers stole sensitive customer data and credit card information from the British telecom service provider TalkTalk in 2015.

State-sponsored actors may also use DDoS attacks against the telecommunications sector and its customers to disrupt the availability of the telecom services. CFCS does not know of any DDoS attacks against the Danish telecom sector which can be attributed to foreign states.

The comparatively uncomplicated launch of DDoS attacks may explain their high occurrence. Hacker forums offer tools, advice and guidance, just as there are available programmes for computers, smartphones and tablets that are able to generate small-scale DDoS attacks. Also, it is possible to order small-scale DDoS attacks online – for free or at a charge. Such attacks may disturb the victim, while only posing a minor challenge for the telecommunications infrastructure.

A more serious threat is posed by strong cyber actors with access to botnets capable of generating very powerful or advanced DDoS attacks against the telecommunications infrastructure, the telecom service providers or their customers. These attacks may constitute a serious threat against the telecommunications infrastructure.

Cyber criminals have carried out DDoS attacks against the telecommunications infrastructure in Denmark as well as abroad, seriously impeding the availability of the providers' telecom services.

Even though the cyber threat from DDoS attacks is very high, their impact on the telecom services is most often negligible due to the high capacity of the telecommunications infrastructure that allows it to handle even the huge amounts of data generated by most types of DDoS attacks without being overloaded. As a result of the segmentation of the backbone networks of the large Internet providers that helps limit the disruptive effect of effective DDoS attacks to a restricted part of the telecommunications infrastructure, even large-scale attacks will generally only disrupt customers on a limited part of the telecommunications infrastructure. Also, several service providers have installed systems and procedures to contain and handle major DDoS attacks against their company or customers without causing any noticeable implications for other customers. However, a DDoS attack is typically not immediately detected by the service provider, resulting in a certain lapse of time prior to initiation of any counter measures, during which the implications of a major DDoS attack may affect the telecom services.

Data from security companies that provide protection against DDoS attacks indicates an increase in bandwidth of the large-scale attacks, partly as the result of an increasing number of everyday products being connected to the Internet, a development called Internet of Things (IoT). When many devices are connected to the Internet, some of them will unavoidably contain vulnerabilities that can be exploited to launch a DDoS attack. The risk is particularly high if the device is manufactured by a company that gives low priority to the integration of cyber security into the Internet-connected devices.

Recent examples outside Denmark of massive DDoS attacks exceeding 600 Gbit/s include the attacks against news media KrebsOnSecurity in September 2016 and the DNS service provider Dyn in October 2016, the latter rendering several

DDoS attacks against companies using TDC DDoS solutions in 2015

- 80 % on 100 Mbit/s or above
- 57 % on 1 Gbit/s or above
- Strongest attack was 39 Gbit/s

Source: TDC DDoS threat assessment 2015

The Internet bandwidth capacity of many small and medium-sized companies is below 50 Mbit/s, while that of large companies is often below 1 Gbit/s.

Targeted DDoS attacks may be effective even though they fail to exceed the bandwidth of the company's Internet connection.

European and US websites unavailable. Both attacks supposedly exploited unsafe IoT devices, which used known default passwords.

Today, it is possible to launch DDoS attacks from smartphones, tablets and computers that are connected to a mobile network. As a result of the increasing bandwidth in mobile networks and the increasing processing power in mobile units, these units can now be used in botnets and exploited to conduct DDoS attacks.

The telecom service providers are also exposed to DDoS attacks that are aimed at their administrative networks, including web servers. Such DDoS attacks do not pose an immediate threat to the telecom services unless the attacks are massive, as described above. However, a DDoS attack may render an online service inaccessible – making sales, support or self-service solutions unavailable to customers – which can be harmful to business operations.

In the event that critical parts of a telecom service provider's business are outsourced to subcontractors, for instance to a provider of cloud computing, the telecom service provider may be disrupted by a DDoS attack against its subcontractor.

The threat from cyber espionage against telecom service providers

Cyber espionage against public authorities and private companies remains the most significant cyber threat against Denmark. Danish authorities and companies are regular victims of cyber espionage attempts primarily from state-sponsored actors.

Cyber espionage also poses a threat to telecom service providers and the confidentiality of the telecom services and may even jeopardize the availability of telecom services. Cyber espionage against telecom service providers may be used to map the providers' telecommunications infrastructure or to access information about the providers' customers to facilitate espionage against authorities, companies and other customers with the providers.

Cyber espionage against the telecommunications infrastructure may also target vulnerabilities in the supply chain to implement or access information about vulnerabilities in hardware used in the telecommunications infrastructure. This is known as Supply Chain Threats.

CFCS assesses it highly likely that state-sponsored actors outside Denmark have the intent and capability to conduct cyber espionage against the telecom sector. However, the CFCS has not seen the same high level of state-sponsored cyber espionage against the Danish telecom sector as against other Danish sectors.

CFCS assesses that while the threat of cyber espionage against Danish authorities and companies generally is **VERY HIGH**, the threat of cyber espionage against the telecom sector is assessed as **HIGH**.

Cyber espionage against the telecom sector is also used to exploit vulnerabilities in the telecommunications infrastructure to launch potential future cyber attacks. This could include:

- Mapping critical network components and support and operations systems within the provider’s telecommunications infrastructure in order to prepare future potential destructive cyber attacks.
- Access to technical operational instructions on the provider’s network components, which may also be used to prepare destructive cyber attacks or compromise confidentiality in the telecom services.
- Access to critical configuration data and passwords to central servers and control systems, thus enabling additional cyber attacks against the service providers’ telecommunications infrastructure.
- Identification of key employees with access to sensitive data or critical systems. This information may be used to launch targeted cyber attacks against key employees in order to gain access to such systems and data.
- Mapping of systems which can be compromised and exploited as a Launchpad for additional cyber attacks against targets in and outside Denmark.

In addition to cyber espionage against individual companies in the telecom sector, cyber espionage may also be launched via the so-called SS7 network, which connects all mobile networks. State-sponsored actors in particular may exploit vulnerabilities in the SS7 design to monitor or tap private individuals, even if these individuals are physically located in other countries. Also, it is potentially possible to prevent calls from or to certain individuals or to completely disconnect certain mobile services.

Exploitation of the vulnerabilities in the SS7 network requires that the actor has access to the network. This access is provided by private companies on commercial terms and conditions or may be obtained via cooperation with an existing provider. We assess that foreign states may have obtained such an access in an effort to exploit the SS7 network to conduct espionage.

It is possible for the individual telecom service provider to mitigate some of the vulnerabilities in the SS7 design, making it more difficult to spy against its customers or influence the telecom services via the SS7 network. In cooperation with other Nordic telecom authorities, the CFCS released the paper ”*Common Nordic Recommendations on SS7 Security Issues*” in December 2015, comprising a series of recommendations to mitigate vulnerabilities in the SS7 design. These guidelines are only available for telecom service providers in the Nordic countries.

The threat against the telecom services coming from cyber crime

In the context of this assessment, cyber crime comprises criminal acts involving the use of IT, in which the actor is motivated by economic gains. In general, cyber crime poses a limited threat to the availability of telecom services.

CFCS assesses that the threat from cyber crime against the telecom services is **LOW**.

The low threat level is the result of more factors such as cyber crimes typically being aimed at corporate business operations and not the telecommunications infrastructure, and that targeted cyber attacks against critical systems in the telecommunications infrastructure require particular technical knowledge and capability, which we believe only few cyber criminals possess. In addition, as cyber criminals will often target the telecom provider’s administrative networks, the control systems in the telecom infrastructure are often logically separated from these administrative networks.

However, technical staff and subcontractors with telecommunications providers often have remote access to the telecommunications infrastructure via the administrative network. If this access is insufficiently protected, cyber criminals may gain access to the infrastructure, which may ultimately threaten the telecom services.

As a result of the cyber criminals' use of DDoS attacks and attempts at compromising customer hardware such as cable modem and DSL routers, customers may be compromised or lose their access to Internet, TV or telephony.

Some planning, development and operations of the telecommunications infrastructure is facilitated by IT systems stored on the telecom service providers' administrative network. Consequently, a cyber attack involving ransomware against a service provider's administrative network may temporarily prevent the service provider from performing its operational tasks. However, these IT systems are usually less crucial to the availability of the telecom services and are, for instance, used to plan and test changes in the telecom infrastructure, traffic analysis, frequency and IP planning or billing. Thus, CFCS assesses that even though such an attack can delay projects or damage the provider's reputation and financial status, the attack will only pose a limited threat to the telecom services.

Some cyber criminals exploit the possibility that sender identity in online calls (VoIP) and text messages can be falsified and misused in spear phishing attacks and fraud attempts. This misuse poses a threat to the integrity, but not to the availability of these telecom services.

The threat from destructive cyber attacks

A number of countries are building up cyber capabilities, which can be used against various types of critical infrastructure, including the telecom sector. These capabilities could be used in connection with military operations, but also enable the countries to launch destructive operations without using traditional weapons.

CFCS assesses that while the threat from destructive cyber attacks from foreign states, including attacks against the telecommunications sector, is **LOW** at present, the threat from destructive attacks could grow in connection with deepening political or military conflicts in which Denmark is involved.

A destructive cyber attack may involve deletion or manipulation of configuration data or software in critical systems or network components. CFCS estimates that the impact of a single destructive cyber attack against the telecommunications infrastructure most often will be short-term as the implications of the attack will be quickly detected by the service provider's operations centre, which will often be capable of mitigating the damages and re-establishing the telecom services within a few hours. However, repeated attacks may generate serious disruptions for longer periods of time.

Destructive cyber attacks against the telecom infrastructure require that the attacker has gained unauthorized access to or compromised the telecommunications infrastructure. The attackers may employ cyber espionage methods to obtain this access. As a result, an attacker, who has compromised a system with the intent to carry out cyber espionage, will often be capable of exploiting this access to launch a destructive attack.

The interruption of the YouSee TV signal on New Year's Eve 2016 may be an example of a destructive cyber attack. During the time of writing this threat assessment, the YouSee incident is still under police investigation and it has yet to be established whether the incident actually involved a destructive cyber attack and if so, who was responsible for the attack.

A foreign state will likely weigh the benefits of a destructive cyber attack targeting the telecommunications infrastructure against the possibility of monitoring voice and data traffic via the same telecommunications infrastructure. However, disruptions in parts of the telecommunications infrastructure may be a means to force communications over to alternative communications systems, allowing the attacker to tap into communications. For instance, a disruption of the 3G mobile network will often force the users to switch to the less secure 2G network.

The threat from cyber terrorism

CFCS assesses that at present no terrorist group has the capability to launch actual online terrorist attacks. Cyber terrorism is motivated by ideology, and just like other acts of terrorism its ultimate goal is to draw attention to the terrorist group's cause by causing destruction of property or loss of life and ultimately causing fear among the population.

CFCS assesses that the threat of cyber terrorism against the telecom sector is **LOW**.

However, the threat of cyber terrorism will increase if terrorist groups succeed in attracting members with sufficient technical skills, or if established cyber activists groups or employees with access to critical systems become radicalised.

CFCS assesses that the telecommunications infrastructure has developed a resilience that is likely strong enough to limit the consequences of cyber terrorism against the telecom services, hampering the terrorists' attempts to raise public fear. However, a physical terrorist attack combined with a cyber attack against the availability of telecom services could boost public fear, thereby increasing the impact of the physical attack.

Cyber threats against the telecom service providers' business operations

Companies in the telecommunications sector are exposed to the same cyber threats as companies in other sectors. Unlike the threats against telecom services, the cyber threats against the telecom service providers' business operations will rarely or only indirectly affect the availability of telecom services.

The threat from cyber crime against the telecom service providers' business operations

Cyber criminals seldom distinguish between the various types of companies, and companies in the telecommunications sector are thus exposed to the same threat from cyber criminals as other Danish companies and authorities.

We assess that the threat from cyber crime against the telecom services providers' business operations is **VERY HIGH**.

Cyber crime poses an increasing threat to Denmark. In particular, the use of ransomware has increased in extent and complexity in recent years. Ransomware is a form of malware used to hold a victim's data hostage by rendering the data unavailable until a ransom fee has been paid. Other methods include theft of corporate intellectual property and data, which contains personally sensitive data or payment or credit card information. Telecom service providers are typically in possession of such customer data.

A recent example from Denmark involves the telecom service provider 3, which in February 2017 fell victim to extortion by criminals, who had gained access to customer data from 3's customer database. At the time of writing this threat assessment the incident is still under police investigation.

Another example of cyber crime involves the British telecom service provider TalkTalk, which was exposed to theft of unprotected customer data by cyber criminals in 2015. According to the company, it suffered a loss of DKK 400 million and lost 100,000 customers.

The threat from cyber espionage against the telecom service providers' business operations

Cyber espionage against telecom service providers focuses on gaining unauthorized access to confidential information on technologies, processes, strategies and commercial data aimed at bolstering a certain company or a country's industry or economy in general. Cyber espionage against telecommunications companies is primarily a threat to the companies' financial situation and business operations.

CFCS knows of state-sponsored actors who actively conduct cyber espionage against companies in Denmark.

CFCS assesses that the threat from cyber espionage against companies in the Danish telecommunications sector is **HIGH**. Below are listed types of information, which may be attractive targets for cyber espionage:

- Confidential data from high-tech subcontractors in the telecommunications sector such as design and operational instructions and software, which may be attractive to actors who want to gain unauthorized access to the technology.
- A telecom service provider's proprietary tools and systems, which often remain unprotected by patents, etc.
- Sensitive data on the telecom service provider's internal situation, work methods and technical solutions, competitive information such as business strategies, internal minutes, price agreements with customers and subcontractors, sales material, etc.

The threat from cyber activism

The aim of cyber activism is to promote an ideological or political message via cyber attacks. Cyber activism typically targets single issues and individuals, organizations or companies, which the activists perceive as opponents of their cause.

The threat from cyber activism against the telecom services and the telecom industry is assessed as **MEDIUM**.

Typical cyber activism methods include so-called website defacement, where the attackers change the visual appearance of a website in order to promote their agenda, leaking sensitive customer data or internal documents as well as DDoS attacks against a government or company website. Unless the attack involves an unusually large-scale DDoS attack, the methods of cyber activists do not pose an immediate threat to the telecom services.

Cyber activism is a relatively rare phenomenon in Denmark, but single issues may draw the attention of activists, increasing the threat unexpectedly. Some cyber activists are motivated by the idea of a free and open Internet. Network neutrality, session logging and registration of mobile customer activity are current telecommunication topics in the public debate and may catch the attention of cyber activists.

Telecommunications trends and their impact on cyber threats

The technology that supports the telecommunications sector is under constant development. New services and technologies can help reduce operations costs, increase profits or market shares, and first-movers in terms of new technology and new services enjoy considerable business advantages.

Subcontractors and telecom service providers must implement and operate these new services and technologies in a way that takes into account the new types of threats and vulnerabilities that come with new technology.

Below are examples of new technologies and services that may influence the nature of the threat:

- Network Function Virtualization (NFV) is the concept of software emulating hardware. NFV may enable quicker implementation of new telecom services and streamline the telecommunications infrastructure. Unlike the widespread, specialized hardware and software technology used in the current telecommunications infrastructure, the NFV is based on standard servers and software from global subcontractors. A cyber attack against these servers will require less expertise than a cyber attack against the current specialized network components.
- Software Defined Networks (SDN) will streamline large-scale network operations, like the telecommunications infrastructure. Network changes will be introduced more rapidly than they are today. For example, network components can be connected by simply selecting the end-points on a graphical user interface as the principal software will ensure automation of the necessary changes in the intermediate network components. However, the transition from decentralized to centralized network administration exposes the network to additional vulnerabilities in case of unauthorized access to the centralized administration. In addition, as a result of potential vulnerabilities in the standard interface between the central administration

and the individual network components all SDN devices, regardless of manufacturer, may be compromised by using the same method.

- Cloud Computing allows for the transfer of data, telecommunications infrastructure or telecom services to centralized data centres operated by a Danish or foreign subcontractor. If a telecom service provider uses this option, the service provider may find it difficult to maintain control of the parts of the business that is transferred to the ‘cloud’. As a result of a transfer, data and infrastructure, which were previously protected on the provider’s internal network, may be exposed to the same cyber threats and vulnerabilities as the cloud service operator.
- Narrowband IoT (NB-IoT), SIGFOX and 5G are network technologies specialized in supporting wireless communication between physical devices. NB-IoT is based on existing LTE mobile networks while SIGFOX necessitates the build-up of a new national access network. SIGFOX and NB-IoT are expected to become commercially available in Denmark in early 2017. The 5G mobile technology is in the process of being developed and is expected to become commercially available around 2020. The new technologies will help accelerate the spread of loT units, including the realization of Smart Cities, but may also introduce new vulnerabilities, which cyber actors will attempt to exploit.
- Mobile technologies and services like Voice over LTE, Wi-Fi calling and Internet connected Small Cells are already used and sold by Danish telecom service providers. The technology can improve mobile coverage in buildings and enable voice calls via the LTE mobile network, but the services also create an environment for new vulnerabilities and cyber threats, as Wi-Fi technology and the Internet become part of the mobile network infrastructure.

Commercial cooperation between service providers and the merger of the telecommunications infrastructure have been a way to reduce the service providers’ costs and improve customer services. National roaming agreements and merger of mobile networks will improve the customers’ mobile coverage, reducing the service providers’ need to expand their mobile network. The increased centralization of the telecommunications infrastructure and the subsequent decreasing degree of redundancy may make the telecommunications infrastructure more vulnerable to cyber attacks.

Outsourcing of telecommunications infrastructure or operational tasks is already being used by Danish telecommunications companies. Outsourcing places high demands on the telecom service provider in terms of maintaining full control of the telecommunications infrastructure. If a Danish service provider outsources significant parts of its business operations to countries, which deviate significantly from Danish standards in terms of legislation, security culture, national stability, corruption or crime, it may change the cyber threat against the telecom services in Denmark. If significant parts of the operations or telecommunications infrastructure are outsourced to other countries, a potential repatriation or transition to another subcontractor may pose a challenge.

Recommendations

CFCS recommends that the senior management level at telecom service providers takes appropriate action based on the threats described in this assessment. The senior management must ensure the technical competencies required to continue the work. In addition, CFCS recommends that the telecom service providers make use of a risk-based approach to cyber defence. Telecom service providers should prepare risk assessments based on the current threat picture, including conditions related to acknowledged vulnerabilities. Telecom service providers must understand their own IT infrastructure, IT processes, etc. in order to acknowledge and address the vulnerabilities that they face. The ISO/IEC-27001 standard provides an excellent basis for preparing a risk-based information security policy.

Finally, critical network components as well as operations and control systems in the telecommunications infrastructure should be separated logically or physically from the telecom service provider's administrative network and protected from unauthorized access via the Internet. This is particularly important, if the service provider has allowed for remote access to the telecommunications infrastructure via the Internet. Such access must be protected with a two-factor authentication.

CFCS recommends that all telecom service providers cooperate closely with their subcontractors in an effort to ensure that devices and telecommunications infrastructure are installed, configured and maintained according to best practice.

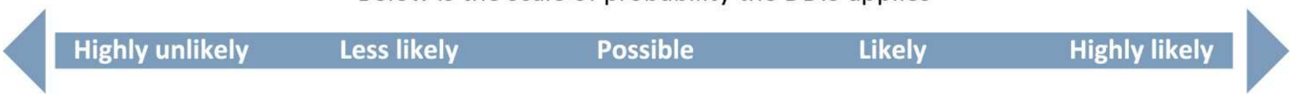
Based on lessons learned, we would like to emphasize the importance of effective logging and well prepared crisis control as well as updated information on company infrastructure design and construction.

Definition of threat levels

Below is a short description of the threat levels used by DDIS.

Threat levels	Description
None	There are no indications of a threat. There is no acknowledged capability or intent to attack. Attacks/harmful activities are highly unlikely.
Low	There is a potential threat. There is limited capability and/or intent to attack. Attacks/harmful activities are less likely.
Medium	There is a general threat. There is capability and/or intent to attack and possible planning. Attacks/harmful activities are possible.
High	There is an acknowledged threat. There is capability, intent to attack and planning. Attacks/harmful activities are likely
Very high	There is a specific threat. There is capability, intent to attack, planning and possible execution. Attacks/harmful activities are highly likely.

Below is the scale of probability the DDIS applies


Highly unlikely
Less likely
Possible
Likely
Highly likely