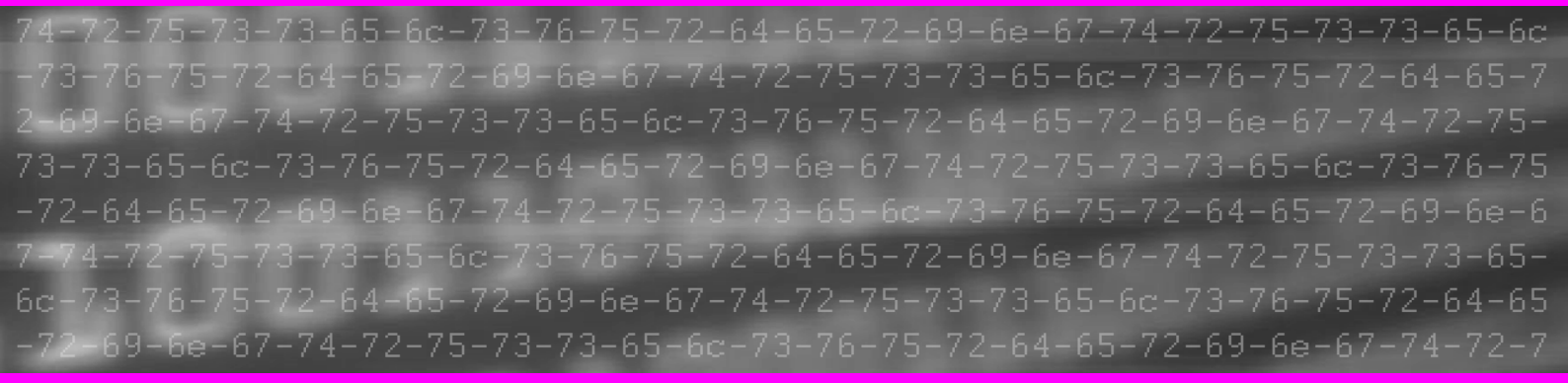
CENTRE FOR
CYBER SECURITY

Threat Assessment

Foreign hackers threaten Danish public research



Threat Assessment Branch under the Centre for Cyber Security

February 2017

CENTRE FOR CYBER SECURITY

Threat Assessment: Foreign hackers threaten Danish public research

This assessment outlines the cyber threat to Danish research at public institutions. The threat is mainly from cyber espionage from foreign states but also includes exploitation of IT infrastructure. Danish universities and public research environments are vulnerable targets.

Key Assessment

- It is likely that foreign states conduct cyber espionage against Danish public research institutions.
- Foreign states have the intent and capability as well as the resources to launch advanced cyber attacks. Attack examples from abroad show that research environments are attractive targets to hackers.
- Hackers have relatively easy access to Danish research as universities and public research environments are traditionally very open, making them highly vulnerable to cyber attacks.
- The threat from cyber espionage against Danish public research institutions is **HIGH**.

Analysis

The Danish Defence Intelligence Service Centre for Cyber Security (CFCS) assesses it likely that foreign states repeatedly conduct espionage against Danish research. They have both a political and commercial interest in Danish research. Also, foreign states may have an interest in the infrastructure of the research institutions with a view to targeting other Danish targets or targets abroad. These states have the capability as well as the resources to launch very advanced and persistent cyber attacks.

In the context of high-priority political issues, foreign states may gain insight into the scientific knowledge and advice on which the Danish government and parliament base their key decisions. In other contexts, states may seek to obtain a competitive and commercial edge by gaining access to information on the work of researchers and Danish research results prior to publication.

Successful unauthorized access to intellectual property and not-yet-published research results by foreign states could hold severe implications for Denmark. Moreover, it may damage the reputation of Danish universities and complicate future funding, recruitment and collaboration.

Danish research is a relatively easy target for foreign states as Danish research institutions traditionally are very open.

Danish research is interesting to foreign states
It is likely that hackers affiliated with foreign states conduct cyber espionage against Danish research. Their interest in Danish research environments may be rooted in multiple factors.

For instance, the possibility of gaining a commercial or competitive edge. Danish research is competing in an international race to publish research results, secure funding and recruit top researchers and students. Several foreign states are likely actively engaged in securing a competitive advantage for their own universities and researchers. Examples of research fields where the international competition is fierce are space science, computer science, energy research and drug development.

DTU Space is Denmark's national space research institute whose main focus is to generate knowledge and technologies to benefit Danish society. DTU Space also conducts research in drones and provides advice on the construction and use of drones to Danish authorities.

Hackers may also be interested in gaining access to sensitive personal information or university IT infrastructure. Sensitive personal information includes medical and statistic records used by researchers and faculty and student information, which could be exploited by foreign intelligence services. In 2012, a professor at the University of Copenhagen was convicted of espionage for passing on student information and CVs of employees at the Centre for Military Studies to foreign diplomats. This particular incident was a case of physical handover of documents rather than a hack.

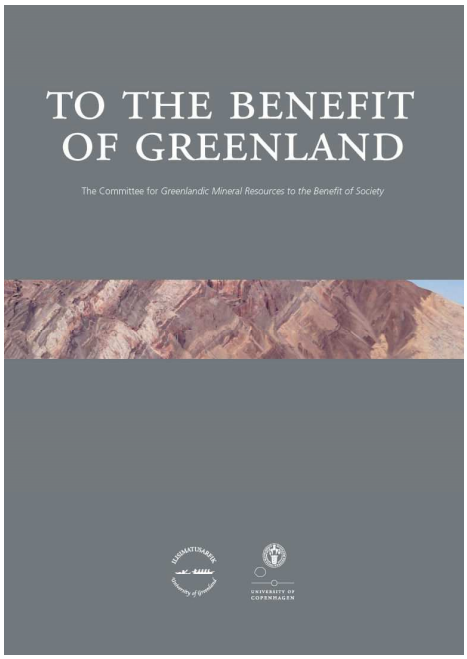
Universities usually have large IT infrastructure, which could be used as a gateway to launch attacks against other parts of society, for instance Denmark's central administration or other

institutions with which the universities are regularly in contact. Servers and work computers may be used in a larger network aimed at building a large attack infrastructure and maintaining anonymity. Foreign states regularly launch cyber campaigns aimed at locating and exploiting vulnerabilities in a company's or public service's IT systems.

Some researchers work with areas that may attract great political attention, for instance research in security and defence policy or geopolitical matters. CFCS holds information that foreign states launch targeted cyberattacks against Danish authorities to gain access to information on Denmark's foreign and security policy. Within the past few years, the Danish Ministry of Foreign Affairs and the Danish Ministry of Defence have been victims of several state-sponsored cyber espionage campaigns. The threat against Danish authorities is directed at the entire state sector, and research communities are also targets. In 2014, a foreign intelligence service tried to trick several public service employees into downloading malware in connection with an international research project.

Researchers supply scientific knowledge that form part of the foundation on which the Danish government and the Folketing (parliament) base their political decisions. Access to their research could grant hackers insight into future Danish policies, for instance Danish participation in NATO operations, defence activities or Arctic operations. This type of information makes Danish research a prime target for foreign states.

Examples: interest in the Arctic, politics and technology
CFCS assesses that foreign states are interested in various research areas, for instance Arctic research and defence and security research. Below are examples of areas of interest to foreign states and not examples of registered cyberattacks.



The Arctic has become a key area of interest for a number of states, which are likely determined and able to gain access to key political or commercial information to promote their own Arctic interests.

Several Danish universities and research institutions, including the Danish Geological Survey of Denmark and Greenland (GEUS), are engaged in Arctic affairs, for instance research into natural resources, raw materials and mining, or energy and climate.

The AAU Arctic Centre is part of Aalborg University, DTU Polar is part of the Technical University of Denmark (DTU), and the Greenland Perspective is a collaboration between the University of Copenhagen and Ilismatusarfik (University of Greenland). The researchers regularly supply Danish

and Greenlandic politicians with scientific advice. In 2014, the Committee for Greenlandic Mineral Resources to the Benefit of Society published the report 'To the Benefit of Greenland'. The report presents a review of five potential scenarios for Greenland's development and contains a number of recommendations on raw materials extraction, for example mining or oil drilling. The report also discusses Greenland's potential economic independence of Denmark.

Other researchers are engaged in topics relating to conflicts, territorial borders, NATO, military targets and methods or the shaping of public opinion. These issues are all topics of interest to foreign states and are among the research topics at the University of Southern Denmark's (SDU) Centre for War Studies or the University of Copenhagen's Centre for Military Studies (CMS). The CMS provides research-based public sector services with reports and advice on current security and defence matters to the Danish parliament, the parties behind the Danish Defence Agreement as well as the Danish Ministry of Defence. In 2016, the CMS delivered reports on NATO's missile defence system, fighter bombers and maritime security and development in Africa.

Technological research is also a political focus area. For example, several Danish universities are engaged in drone research. The DTU Space Centre conducts research in drones and provides advice to public sector services on the construction and use of drones. The SDU is leading a government-funded research project, which brings together the expertise of researchers from five different Danish universities, aimed at ensuring that Denmark becomes a world leader in the development of drones.

Espionage via advanced cyberattacks

Espionage against public and private targets still poses the biggest cyber threat against Denmark. State-sponsored APT attacks are a very active threat to Danish interests. Hackers have developed increasingly sophisticated methods and capabilities to conceal their activities and identities.

APT

APT stands for Advanced Persistent Threat. APT attacks are a particularly advanced, targeted and persistent kind of hacker attack. The attackers gain access to a network by exploiting vulnerabilities in software used for example by a university. APT attacks require huge resources, technical expertise and specific knowledge of the intended target. The hackers use specialized tools enabling them to stay undetected in the target's network for an extended period of time. APT actors persistently attack their targets. The aim of most APT attacks is to conduct espionage. States and state-sponsored groups are highly likely behind most APT attacks.

Many actors, including states, also conduct campaigns that involve scanning a wide range of IT networks systematically in order to locate vulnerabilities in IT systems. In 2015-16, the CFCS detected numerous attacks against a specific IT system, which is used by several Danish organizations, including research institutions. These types of attacks are not necessarily espionage attempts. Hackers often look for vulnerabilities that will allow them to install their own backdoors in the systems and build a network of servers and computers. They are then able to attack through these networks later or use them to attack other priority targets.

Abroad, cyberattacks against universities are becoming increasingly frequent. A study among British universities shows that 83 per cent of the universities fall victim to frequent and increasingly advanced cyberattacks. 3/4 of the universities also respond that apart from the financial consequences, their reputations suffer as a result of the attacks, key research projects are delayed or cancelled, and the attacks affect national security.

There is no exhaustive information on the number of cyberattacks against Danish research institutions. Universities and other institutions are responsible for their own IT security and they only report security incidents to some degree to the Danish IT security service DKCERT. The individual universities do not necessarily report averted attacks or minor incidents to the central IT department. In addition, advanced foreign state-sponsored attacks may go undetected.

Abroad, most attacks are launched by states which are known to possess huge APT attack capabilities. However, as an increasing number of states improve their cyber capabilities, it is likely that they will also attempt cyberattacks, as intellectual property theft is a relatively inexpensive way to bolster economic development.

Hackers have easy access to Danish research

The levels of cybersecurity vary from university to university and among departments and centres. At central level, institutions often have well-consolidated systems, and Danish research institutions regularly receive information on vulnerabilities from DKCERT, which monitors the research net. Locally, however, the variations are greater.

Most public research environments have an open source culture where knowledge sharing is the key objective. In Denmark, it is also a national requirement that universities communicate and exchange knowledge. Consequently, universities face a specific challenge in finding the balance between maximum knowledge sharing and protection of data and results. Researchers advocating a large degree of openness may find it difficult to see the value in restrictions motivated by security concerns and may choose to stray from the guidelines set forth by the management.

In addition, the majority of public researchers do not believe that their work is sufficiently interesting in a political or economic context to require strong security measures. Consequently, neither researchers nor the management have traditionally focused a lot on the cyber threat.

Management often leave cyber defence issues to the IT department or focus on pure system solutions. Departments and centres rarely prepare strategic analyses in cooperation betwen researches and management to determine what they will protect and what the consequences will be in case of security breaches. Similarly, they rarely make targeted efforts to train employees and raise the level of cyber conduct awareness.

In addition to the eight universities on the map, Denmark has eight approved technological service institutes (GTS), three sector research institutes and a number of other public research institutions.

Phishing is a widespread attack method that exploits human online behaviour. An increasing number of Danish institutions fall victim to phishing attacks. Most successful phishing attacks are the result of human error rather than system failure. Though it may prove difficult to detect well-designed false emails, raising awareness among the employees is a step in the right direction.

Researchers are outward facing and often present knowledge in public forum. As such, it is not uncommon for them to be in contact with many different people and receive emails from new acquaintances, making them potentially vulnerable to spear phishing attacks. Even the most advanced system cannot fully protect against human error.

Phishing attacks

- Phishing is when an actor sends a large number of fake emails to a wide range of users, trying to trick them into opening attachments or clicking on embedded links containing malware causing damage to the victim's computer.
- Spear phishing is an email that targets specific individuals in an organization. It takes a greater effort for the actor to construct a targeted fake email that appears relevant and believable to the recipient. Spear phishing emails are often very convincing and harder to recognize as fake emails.
- CEO Fraud is a special type of spear phishing attack. Here, the actor poses as the CEO in emails sent to employees in an organisation. This way, the actor may lure employees to act on what they believe is an order from the CEO. So far, CEO Fraud has primarily been used for economic gains.

Another dimension of cyberattacks is the insider threat. Research institutions are highly international environments where researchers and students from around the world continuously gain full access to various systems, databases and intellectual property, including for shorter periods of time such as research stays and exchange during a semester or merely a few weeks.

A guest researcher may – intentionally or unintentionally – contribute to unauthorized access by doing even the simplest things such as clicking on a link in a phishing mail, insert a USB drive containing malware into a PC or otherwise grant hackers access to systems. Foreign states may also try to recruit international or Danish students to assist them in their activities.

International employees with limited Danish language skills may also find it difficult to recognize fake emails written in poor Danish – something which would otherwise usually raise a flag when it comes to phishing mails.

Non-state sponsored hackers, for example cyber activists, so-called hacktivists, or cyber criminals who typically have different agandas than states, could also exploit human and system vulnerabilities in research environments.

Hackers do not need to steal data to cause damage. They may cause just as much damage by deleting or changing data. They could also block employee access to their own data and demand ransom in exchange for a decryption key, as in the so-called ransomware attacks. If a university cannot guarantee the integrity of its data, this could undermine the quality of research and ultimately harm the reputation of the university.

The CFSC has information that over the past few years, several Danish universities have fallen victim to repeated attacks involving various techniques, including phishing campaigns - for instance CEO Fraud - ransomware and other attemtps at encryption of servers.

Advanced threats from state or state-sponsored actors	**Threats from "hacktivists" or cyber criminals**
Intellectual property theft aimed at commercial competition or political espionage	Damaged infrastucture, for instance overload of websites aimed at making a statement or merely cause inconvenience
Personal data theft aimed at espionage or recruitment	Personal data theft aimed at fraud or political activism
Access to and control of IT infrastructure aimed at building malicious infrastructure to launch new attacks, possibly against other targets	Deleted or changed data, encryption or denied access aimed at demanding ransom

Typical cyber threats and intentions

Recommendations

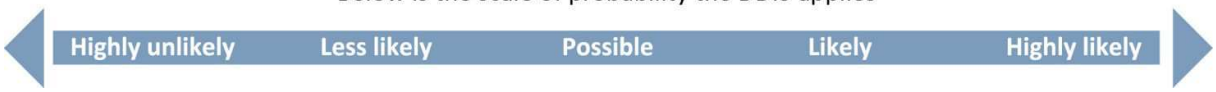
The CFCS recommends that management at all levels of Danish universities and research centres is aware of the cyber threat and take appropriate actions based on the threat assessment. The cyber threat is not merely and IT technological challenge, but also a question of employee behavior and knowledge of own vulnerabilities. Consequently, it is vital to involve the strategic management level in decisions relating to the topic.

The CFCS recommends that university management assesses the risks and decides on future initiatives. Universities should focus on both processes, techniques and behavior. Processes include preparing regular risk analyses and determining what knowledge the universities deem important to protect and what the consequences of a potential breach may be. Techniques could be finding vulnerabilities and uncovering and protecting IT infrastructure and IT processes. Behavior involves initiatives aimed at raising user awareness of the cyber threat and establishing staff training programmes that teach employees safe and appropriate cyberspace behavior.

The CFCS recommends that Danish universities and other research environments protect themselves against the cyber threat by seeking information and advice in the following publications which may provide some guidelines (in Danish):

- Cyberforsvar, der virker
- Spear phishing – et voksende problem
- Trusselsvurdering: Cybertruslen mod Danmark

Below is the scale of probability the DDIS applies



Threat levels

The CFCS uses the following five 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.