CENTRE FOR CYBER SECURITY

Threat assessment:

# The cyber threat against Greenland

1st edition March 2023

## Table of contents



CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

1. edition March 2023

# Threat assessment: The cyber threat against Greenland

The purpose of this threat assessment is to inform Greenland authorities and decision-makers on the cyber threat against Greenland. The assessment can form part of the efforts by Greenland companies and authorities in preparing cyber security risk assessments.

# Key assessment

- Foreign states and criminal hackers constitute a persistent cyber threat against Greenland.

- The threat of cyber espionage against Greenland is **VERY HIGH**. Greenland's central location in the Arctic contributes to the serious threat of cyber espionage against Greenland. Knowledge obtained through cyber espionage can be abused by foreign states at the expense of Greenland's interests.

- The threat of cyber crime against Greenland is **VERY HIGH**. The consequences of, in particular, ransomware attacks can not only be deeply detrimental to the targeted authorities and companies but may also jeopardize critical societal functions.

- The threat of destructive cyber attacks against Greenland is **LOW**. It is less likely that foreign states have the intention of using destructive cyber attacks against Greenland. The threat may, however, increase with little warning, as several states hold destructive cyber capabilities. Also, it is possible that the impact of destructive cyber attacks directed against other countries could extend to affect the supply of critical services in Greenland.

- The threat of cyber activism against Greenland is **LOW**. The threat of cyber activism against Greenland may rise with little or no warning if single issues related to Greenland were to land in the crosshairs of activist hackers.

- The threat of cyber terrorism against Greenland is **NONE**. Militant extremists have limited intentions to launch cyber attacks whose effect is comparable to that of conventional terrorism. In addition, they lack the capabilities required for such attacks.

# Introduction

Greenland is facing a serious cyber threat that mainly stems from foreign states and criminal hackers. Both foreign states and criminal hackers have significant resources to carry out cyber attacks, and constitute a persistent threat against Greenland.

Cyber attack incidents in 2022 have impacted critical functions in Greenland, resulting in problems such as down-time in citizen-facing services in the central administration and healthcare system. These incidents are a testament to the seriousness of the cyber threat.

By virtue of their location and geography, Arctic communities such as Greenland are particularly dependent on secure supplies of food, power and heating. Cyber attacks against these functions – whether committed by state or non-state actors – can thus carry particularly serious implications.

Cyber threats transcend national borders. States and criminal hackers worldwide continually carry out attacks. Consequently, the assessment of the cyber threat against Greenland is not solely based on the analysis of incidents in Greenland alone, it also factor in the development in the cyber threat against Denmark and other countries in the neighbouring regions of Denmark and Greenland.

The assessment also includes issues of a foreign and security policy nature with the potential to impact the threat, including the interest of foreign states in Greenland and the Arctic.

In addition to assessing the threats of cyber espionage and cyber crime, CFCS also assesses the threats emanating from cyber activism, destructive cyber attacks and cyber terrorism.

**Cyber attacks impacted citizen-facing services**

Naalakkersuisut's Digitization Agency detected a security breach in the central administration on 25 March 2022. To mitigate the breach, communication going in and out of Greenland via the administration's servers was shut down, cutting off the access to websites through the secure login solution NemID and delaying the payment of social benefits and bills. Head of Naalakkersuisut Múte B. Egede said to Greenlandic media that the incident was the consequence of a cyber espionage attack.

On 9 May 2022, Naalakkersuisut informed that the Greenlandic healthcare system was hit by system breakdowns, resulting in problems accessing the doctor.gl website and delivering emails to the healthcare sector. Naalakkersuisut announced on 18 May 2022 that a cyber attack was the cause of the system breakdown. The rebooting of the system meant that healthcare staff could not access patient medical records.

# Cyber espionage

The threat of cyber espionage against Greenland is **VERY HIGH**. As a result, Greenlandic authorities and private companies will highly likely fall victim to cyber espionage attempts within the next two years.

The main drivers behind cyber espionage are political and financial factors, and states continually engage in attempts at cyber espionage in order to gain access to sensitive and valuable information, including against Greenland.

Foreign states, including Russia and China, have a special interest in knowledge related to foreign, security and defence policy issues. As an example, foreign states may be interested in information about Greenland's relations to the Kingdom of Denmark and to foreign states.

Cyber espionage may also be used against other parts of the Greenlandic society in order to gain insight into other issues such as raw materials, natural resources, commercial conditions, critical sectors and intellectual property.

The key location of Greenland in the Arctic is a factor contributing to the serious threat of cyber espionage against Greenland. Both Russia and China have a strong interest in the Arctic. Russia, for its part, sees itself as the leading Arctic nation with a historic right to play a dominant role in the region. China, for its part, is working to widen its influence on Arctic matters in a bid to gain access to resources and sea routes. Cyber espionage can be used as a tool by both countries to widen their respective political manoeuvre room and further their interests in the Arctic, potentially at the expense of Greenlandic interests.

Greenland's close ties to Denmark means that Greenlandic organizations are exposed to a shared threat, as they may become victims of threats targeting authorities and companies in Denmark that are affiliated with or important to Greenland. Such organizations may include Greenlandic authorities and companies with links to Danish authorities that are part of foreign and security policy alliances, including EU and NATO.

Recent years have seen an increase in the threat against transport and research in Denmark. As aviation and shipping are of particular importance to Greenland, and Danish and Greenlandic research institutions work closely together, CFCS assesses that the threat against these sectors also extends to Greenland.

Cyber espionage also hits more randomly across sectors and borders, with states launching opportunistic cyber attacks. This can for instance happen in connection with the publication of vulnerabilities or supply chain attacks through, for instance, IT providers in which foreign states compromise multiple victims in rapid succession. Following the initial compromise, the states can take their time in deciding which accesses, data or accounts to follow up on.

**Cyber espionage can lead to other threats**
Cyber espionage against Greenland can lead to other types of cyber attacks. Knowledge gleaned and accumulated through cyber espionage may, for example, become utilized in potential future influence campaigns. As an example, this could happen in connection with a future conflict of interest in the Arctic where Greenland could come to play a prominent role against Russia or China.

In addition, cyber espionage can provide foreign states with knowledge of or access to IT systems that can be exploited in destructive cyber attacks against Greenland.

**Attempt at influencing the Kingdom of Denmark**
An attempt at influencing the Kingdom of Denmark unfolded in November 2019 when a fake letter allegedly written by then Greenland Minister of Foreign Affairs Ane Lone Bagger to US Senator Tom Cotton started circulating on the Internet. The letter mentioned issues such as Greenlandic-US cooperation, a future vote on independence for Greenland, and a specific agreement on the status of Greenland and support from the United States. Circulation of the fake letter highly likely had the dual purpose of sowing division in the Kingdom of Denmark and generating distrust between Denmark and the United States about the latter's intentions in the Arctic.

# Cyber crime

The threat of cyber crime against Greenland is **VERY HIGH**, indicating that authorities and private companies in Greenland are highly likely to fall victim to cyber crime attempts within the next two years.

CFCS uses the term cyber crime collectively to describe actions whereby hackers use cyber attacks to commit crimes for financial gain. These crimes generally include different forms of theft, fraud and extortion.

Cyber crime is a worldwide problem, and authorities, companies and citizens in Greenland too face the constant threat of cyber crime. The transnational nature of cyber crime reflects that some cyber criminals cast the widest net possible to target multiple victims, for example through phishing emails distributed widely to thousands of victims across the world.

Other types of cyber crimes target public authorities or private companies, which could end up costing the individual victims millions of DKK.

**Ransomware attacks are the most serious cyber crime threat**
At present, ransomware attacks are the most serious cyber crime threat against Greenland. Ransomware attacks involve cyber criminals compromising and encrypting data on key public and private IT systems, subsequently demanding ransom in exchange for decryption. In addition, cyber criminals often threaten to leak the stolen data unless a ransom is paid.

Ransomware attacks can cause serious damage, not only to the targeted authorities and companies but also to critical societal functions.

In May 2021, US oil company Colonial Pipeline suffered a ransomware attack that led to a six-day operational shutdown. The fallout of the attack demonstrated the damaging consequences of ransomware attacks on critical supply chains.

While most cyber criminals rely on extortion and theft as their primary techniques for monetizing stolen information, some hackers still specialize in fraud, including so-called Business Email Compromise (BEC) scams that involve cyber criminals posing as executives and authorizing wire transfers to their own accounts.

**Cyber resilience can mitigate both cyber espionage and ransomware**
The attack techniques used in the initial phases of a cyber espionage attack and a ransomware attack share multiple similarities. In both types of attack hackers try to gain access to critical IT systems, such as email servers, by using phishing techniques and exploiting known vulnerabilities.

This means that Greenlandic authorities and companies that strengthen their cyber resilience in order to prevent cyber espionage attempts also gain an improved resilience against ransomware attacks and vice versa.

Even though the motives behind the two threat are different, authorities and companies can use some of the same techniques to strengthen their protection against both threats.

# Destructive cyber attacks

The threat of destructive cyber attacks against Greenland is **LOW**, indicating that authorities and companies in Greenland are less likely to fall victim to destructive cyber attacks within the next two years.

It is less likely that foreign states have the intention to launch destructive cyber attacks against Greenland at present.

Foreign nation states primarily use destructive cyber attacks as a tool in conflicts. Several states, including Russia, have destructive cyber attack capabilities. Foreign nation states continually develop their capabilities to launch destructive cyber attacks at short notice.

Consequently, the threat of destructive cyber attacks against Greenland may increase with little or no warning if the security situation, for example as a result of the war between Russia and Ukraine, escalates into a military confrontation between Russia and NATO. Particularly, the threat may increase if a conflict were to revolve around Greenland or the Arctic.

Although the threat of destructive cyber attacks is currently **LOW**, the threat against Greenland is still significant, as destructive cyber attacks may carry very serious consequences, including disruption of access to critical functions and services such as electricity and transportation, or Internet disruption. A destructive cyber attack may also lead to extensive damage to data and systems.

Furthermore, it is possible that Greenland can become a collateral victim of destructive cyber attacks directed at other countries, for example if foreign suppliers of critical services in Greenland fall victim to destructive cyber attacks.

In February 2022, US satellite communication provider Viasat fell victim to a destructive cyber attack. Even though the attack targeted Ukrainian military communication, the consequences of the attack extended far beyond the Ukrainian border, affecting customers in a number of countries.

# Cyber activism

The threat of cyber activism against Greenland is **LOW**, indicating that authorities and companies in Greenland are less likely to fall victim to attempts of cyber activism within the next two years.

Cyber activists often use overload attacks, so-called DDoS attacks, and hack and leak attacks against authorities and companies.

CFCS assesses that even though some cyber activists are capable of launching cyber activist attacks on authorities and companies in Greenland, Greenland is at present less likely to become a target of cyber activist attack.

The threat of cyber activism to Greenland may increase with little or no warning if single issues connected with Greenland catch the attention of cyber activist groups. As overload attacks, in particular, are easy to launch and require little preparation, the threat of such attacks may quickly increase.

Cyber attacks launched by pro-Russian cyber activists on several NATO countries in response to the conflict in Ukraine have increased the threat of cyber activism to Denmark. However, there are no signs that this threat extends to Greenland as well. Should Greenland come to play a more active role in the conflict in Ukraine the threat may increase.

# Cyber terrorism

The threat of cyber terrorism against Greenland is **NONE**, indicating that authorities and companies in Greenland are highly unlikely to fall victim to attempts of cyber terrorism within the next two years.

CFCS defines cyber terrorism as cyber attacks aimed at creating effects similar to those of conventional terrorism, including cyber attacks causing bodily harm or major disruptions of critical infrastructure.

CFCS assesses that militant extremists have limited intentions to launch cyber attacks whose impact is comparable to that of conventional terrorism and that they lack the capabilities required for such attacks.

# 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 highly unlikely. |
| **LOW** | A potential threat exists. Limited capacity and/or intent to carry out attacks. Attacks/harmful activities are less 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 highly likely. |

The DDIS applies the below scale of probability


*"We assess" corresponds to "likely" unless a different probability level is indicated.*