CENTER FOR CYBERSIKKERHED

The cyber threat against Denmark in light of Russia's invasion of Ukraine

The purpose of this threat assessment is to inform Danish decision-makers, authorities and companies of the cyber threat against Denmark in light of the Russian invasion of Ukraine. Its purposes include providing a more detailed outline of the background for the CFCS's decision not to change the threat levels for the cyber threat against Denmark and giving a description of the factors that could impact the development of the threat.

Key assessment

- Russia's invasion of Ukraine has changed the security policy landscape and created an uncertainty that extends to the cyber realm. Even though this has not prompted a change to the Centre for Cyber Security's current threat levels, the pace and tension of the current situation mean that the security policy setting, and, by extension, the threat levels may change with little warning.

- The threat from cyber espionage against Denmark continues to be **VERY HIGH**. The Centre for Cyber Security (CFCS) assesses that in the current situation, Denmark is continuously facing a persistent, active and serious threat of cyber espionage. The CFCS assesses that the Russian invasion of Ukraine has not significantly changed Russia's and China's enduring focus on conducting cyber espionage against Denmark.

- The threat from cyber crime against Denmark continues to be **VERY HIGH**. Cyber crime constitutes a serious threat to Danish authorities, companies and citizens across society. The Russian invasion of Ukraine has not to any significant degree impacted the cyber crime threat against Denmark.

- The threat from destructive cyber attacks against Denmark continues to be **LOW**. The CFCS assesses that states with sufficient capabilities to launch destructive cyber attacks, including Russia, still have no intentions of directing this type of cyber attack against Denmark.

- The threat from cyber activism against Denmark continues to be **LOW**. Even though Russia's invasion of Ukraine has intensified activities in cyber activist environments, activist activities have so far largely been launched in direct response to the war and has been focused on Russia, Ukraine and Belarus.

- The threat from cyber terrorism is **NONE**. The threat remains unaffected by the Russian invasion of Ukraine.

Introduction

The present report is an updated threat assessment by the Centre for Cyber Security (CFCS) under the Danish Defence Intelligence Service (DDIS) concerning the cyber threat against Denmark in the light of the Russian invasion of Ukraine. The purpose of the assessment is to provide a condensed and updated overview of the threat landscape and the factors that could impact the development of the threat.

The Russian invasion of Ukraine on 24 February 2022 has left Denmark facing a changing and in many ways more unpredictable security policy landscape. This uncertainty extends to the cyber realm where the threat situation may change with little warning if, for instance, the relationship between the NATO countries and Russia were to deteriorate even further.

The pace and tension of the current situation increases the risk of misunderstandings. As a result, security policy conditions – and by extension the threat levels – may change with little warning.

The situation in Ukraine thus serves to highlight the immediate seriousness of the cyber threat. Even though the CFCS does not at the current moment see a basis for adjusting the threat levels, the CFCS urges all Danish authorities and companies to ensure that their cyber security risk assessments are updated and that their mitigating measures match the current situation.

The assessment of the cyber threat is divided into sections addressing different types of cyber threats: cyber espionage and cyber crime; destructive cyber attacks; cyber activism and cyber terrorism.

Two parameters form the core of DDIS assessments of threat levels: the capabilities held by potential threat actors and the intentions of potential threat actors. The overall assessments of the capabilities and intentions of threat actors are expressed through a five-step threat level scale, ranging from **NONE** to **VERY HIGH**.

Danish companies and authorities will highly likely remain constant targets of cyber espionage and cyber crime, independently as well as in consequence of the current crisis.

The CFCS assesses that the intention of directing destructive cyber attacks against Danish targets remains limited. Several states, including Russia, have the capabilities to launch destructive cyber attacks. If such an attack were to be directed against, for instance, critical infrastructure with the purpose of disrupting critical functions, its effect could be comparable to that of a military attack against a Danish target. At present, the CFCS assesses it less likely that Russia has any intention of directing a destructive cyber attack against Denmark. Consequently, the threat from destructive cyber attacks remains **LOW**.

Cyber espionage

The threat from cyber espionage against Denmark continues to be **VERY HIGH**. The CFCS assesses that the invasion has not significantly changed Russia's and China's continued focus on conducting cyber espionage against Denmark.

The CFCS assesses that in the current situation, Denmark remains faced with a persistent, active and serious cyber espionage threat. Danish authorities and companies are constant targets of cyber attacks whose purpose is to give foreign states access to sensitive and valuable information that Danish organizations wish to protect. Recent years have also seen a rise in the threat against the transportation and research sectors.

Already prior to the Russian invasion of Ukraine, the Danish foreign and defence ministries were high-priority cyber espionage targets. The persistent threat against organizations associated with these ministries is the result of foreign states, including Russia, being on the constant lookout for information relating to foreign, security and defence policy.

It is highly likely that Russia's invasion of Ukraine has not diminished its special focus on conducting cyber espionage against authorities and organizations in Denmark that contribute to shaping Denmark's foreign, security and defence policies.

Cyber espionage against knowledge relating to these issues will continue and may give foreign states, including Russia, insight into Danish foreign and security policy decisions as well as Danish military capabilities and plans. Such knowledge can be abused, including to weaken Denmark's foreign policy clout in relation to the war in Ukraine and cooperation inside frameworks such as the EU and NATO, for example.

Other states besides Russia also pose a cyber espionage threat. The CFCS assesses that the current security policy situation does not change China's position as a major cyber espionage perpetrator, whose tools of action include cyber-enabled attacks to gain access to knowledge of equipment and technologies that can be used for civilian as well as military purposes.

Cyber crime

The threat from cyber crime continues to be **VERY HIGH**. The threat is directed against authorities, companies and private citizens across society. Though the Russian invasion of Ukraine has triggered several responses inside the criminal environment, it has not significantly affected the general threat from cyber crime against Denmark.

Financial gain remains the key driver for criminal hackers, who continue to be opportunistic in their attacks, and cyber criminal networks will continue to attack Danish targets independently of the Russian invasion of Ukraine. In the short term, the war thus has no direct impact on the threat posed by cyber criminals. The most serious cyber crime threat continues to emanate from targeted ransomware attacks that have the potential to impact critical services.

There have been incidents of criminal hackers taking advantage of the current focus on the war to spread phishing emails, including emails asking for humanitarian aid for Ukraine. In their phishing attacks, criminal hackers often seize on topical issues, as was the case in connection with the outbreak of the Covid-19 pandemic in 2020.

There have been several responses from criminal hackers to the invasion of Ukraine, which is unsurprising as there is a large Russian-speaking criminal hacker community. The Conti ransomware hackers have threated to retaliate if the West were to attack critical infrastructure in Russia or Russian-speaking countries. Following these threats, the Conti group has suffered a data leak damaging the group's activities. Several competing ransomware groups have announced that they are apolitical, citing that their networks include hackers in both Russia and Ukraine, among others. The CFCS assesses that despite its announcements, financial gain is still the main motivation for the Conti group.

Destructive cyber attacks

The threat from destructive cyber attacks against Denmark continues to be **LOW**. The CFCS assesses it less likely that Russia or other foreign states have intentions of launching an attack of this kind against Denmark. At present, Russia has no intention of escalating the war into a full-blown war with NATO.

Danish authorities and companies in Ukraine may fall victim to destructive cyber attacks originally targeting Ukrainian IT infrastructure, as was the case with the 2017 NotPetya attack that also affected Danish company A.P. Møller Mærsk.

What are destructive cyber attacks?
The CFCS defines destructive cyber attacks as attacks that could potentially result in:
- Death or personal injury,
- significant physical damage or
- destruction or manipulation of information, data or software, rendering it unfit for use unless extensive restoration is undertaken.

Danish companies and authorities with a presence in Ukraine may also become collateral victims of destructive cyber attacks in Ukraine, even if Russia has no intention of striking Danish targets specifically. The repercussions of such attacks may include power outages or network disruptions.

If the security situation brought about by the war between Russia and Ukraine escalates into a military confrontation between Russia and NATO, the threat from destructive cyber attacks against Denmark will increase. The specific threat level will depend on the nature and further evolvement of such a crisis.

Ukraine hit by a multitude of cyber attacks in 2022
In January and February 2022, Ukraine was hit by a number of cyber attacks. So far, the attacks have included DDoS, defacement and wiper attacks that deployed different types of destructive malware targeting the Ukrainian government and government institutions, among others.

Several of the destructive wiper attacks against Ukraine so far likely served the purpose of causing panic in the Ukrainian population and dismantling Ukraine's ability to function and defend itself. As their impact is disruptive rather than destructive, DDoS and defacement attacks do not fall within the CFCS's definition of destructive cyber attacks.

The extent and impact of the destructive cyber attacks launched against Ukraine remain unclear. Ukraine may also have been hit by cyber attacks that have gone unreported by the media or the Ukrainian authorities.

State actors may try to disguise their cyber attacks as cyber crime
Ukrainian authorities have been hit by cyber attacks that deployed destructive malware posing as ransomware. Cases in point are the 2017 NotPetya attack and the January 2022 cyber attacks that deployed the destructive WhisperGate malware.

State actors also launch cyber attacks that apply cyber criminal tactics possibly to conceal the perpetrator of the attacks.

The purpose of the concealment may be to blur the objective of the attacks, making it more difficult to attribute them to specific countries. State actors may feel more encouraged to launch destructive cyber attacks if they believe that they may successfully disguise such attacks as cyber crime.

Cyber activism

The threat from cyber activism against Denmark continues to be **LOW**.

Cyber activism is typically motivated by various ideological or political concerns. Cyber activist attacks are launched by non-state actors or groups in an attempt to draw attention to their cause or to punish organizations.

Though the number of activist cyber attacks has dropped over the past few years on a global scale, the Russian invasion of Ukraine has galvanized some elements of the activist community into action. Activist networks still have the capabilities to launch cyber attacks.

However, it has been several years since Danish targets were the focus of significant activist cyber attacks. The CFCS assesses that cyber activists show little interest in attacking targets in Denmark. So far, activist activities triggered by the Russian invasion have to a wide extent been performed in direct continuation of the war and have mainly targeted Russia, Ukraine and Belarus.

The hacker group known as Cyber Partisans has launched activist cyber attacks against the railway system in Belarus, disrupting the system's routing and switching devices both prior to and after the Russian invasion of Ukraine.

At the moment, cyber activist attacks like these are attracting the bulk of the media's attention. Activists identifying with the Anonymous hacker group have declared cyber war on Russia. Since the group's declaration of war, Russian media have been among the targets of different activist cyber attacks. For example, Anonymous claimed responsibility on Twitter for hacking Russian state TV channels to air footage of the war in Ukraine. Subsequently, the websites of several Russian media outlets were hacked and replaced with anti-Putin and anti-war messages.

States conduct influence campaigns under the guise of cyber activism
The threat from influence campaigns by means of cyber attacks exclusively covers the threat from cyber attacks launched by foreign states to sway public opinion.

Foreign states, including Russia, actively use cyber attacks to sway public opinion abroad. In Ukraine, several government websites were defaced with false claims that Kyiv had surrendered and signed a peace agreement with Russia.

There are several examples of attacks on the Baltic countries aimed at undermining support for NATO's presence in the region. It is likely that cyber attacks will be a regular occurrence to weaken cohesion within NATO.

Cyber terrorism

The threat from cyber terrorism is **NONE**. The threat remains unaffected by the Russian invasion of Ukraine.

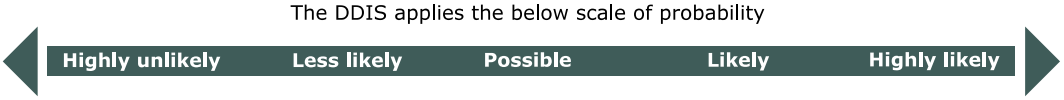
Serious cyber attacks aimed at creating effects similar to those of conventional terrorism presuppose technical skills and organizational resources that militant extremists do not possess at this point. At the same time, their intent to conduct cyber terrorism is limited.

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.

The DDIS applies the below scale of probability



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