DANISH DEFENCE INTELLIGENCE SERVICE

Assessment of the hybrid threat to Denmark

On 3 October, the Danish Defence Intelligence Service (DDIS) published an updated assessment of the hybrid threat to Denmark.

Russia highly likely sees itself as being in conflict with the West, in which the hybrid means employed are kept below the threshold of armed conflict. The DDIS assesses that Russia is currently conducting hybrid warfare against NATO and the West.

It is highly likely that the hybrid threat from Russia against NATO will increase in the coming years.

Date: 3 October 2025

Danish Defence Intelligence Service
Kastellet 30
DK-2100 Copenhagen

Tel.: +45 33 32 55 66
E-mail: FE-MYN@fe-ddis.dk
www.fe-ddis.dk

Summary assessment of the current DDIS threat levels

- The threat of sabotage against the Danish Armed Forces is **HIGH**.
- The threat of destructive cyber attacks against Denmark is **MEDIUM**.
- The threat of military provocations against NATO member states is **HIGH**.
- The threat of malign influence operations against Denmark is **LOW**.
- The threat of conventional military attacks against Denmark is **NONE**.

The hybrid threat to Denmark

Russia's war in Ukraine has led to a significant increase in tensions in Denmark's neighbouring regions. Russia is carrying out hybrid attacks against the West on a much larger and more aggressive scale than before the war in Ukraine.

Russia uses hybrid activities to weaken NATO's political cohesion and decision-making capacity. Russia's aim is not to achieve quick gains, but rather to create a sustained state of uncertainty in which NATO's cohesion is gradually undermined. Russia will likely become more willing to intensify its hybrid attacks if the alliance fails to respond.

Hybrid warfare

Hybrid tools includes political, economic, informational, and military means used by a state to weaken and undermine other states. These means may be employed individually or in combination to achieve the greatest possible effect.

Hybrid warfare is not a legal concept entrenched in international law. The DDIS uses the term "hybrid warfare" to describe a stage in which a state employs a combination of hybrid means, including military means, in a very aggressive manner to apply pressure on and undermine another state while remaining below the threshold of armed conflict.

A state may decide to employ hybrid warfare activities when it assesses that traditional diplomatic tools will not achieve the desired effect and that a conventional armed conflict is too risky. However, this would require the state to assess that the hybrid attacks do not carry a significant risk of escalation into armed conflict.

The nature of hybrid warfare is difficult to determine conclusively, including identifying the actors behind each individual incident. Consequently, the assessments of the DDIS are based on an overall evaluation of the actors' abilities, intentions and capabilities.

Since the spring of 2025, Russia's aggressive military behaviour towards NATO countries has further intensified. On 25 September 2025, Russian Foreign Minister Sergey Lavrov publicly stated that NATO and the EU have declared war on Russia and are directly participating in it through their support for Ukraine. Russia highly likely sees itself as being in conflict with the West, in which the hybrid means employed are kept below the threshold of armed conflict.

Russia has likely concluded that it can employ these hybrid means without risking escalation or retaliation. In addition, Russia likely believes that NATO member states are behind similar activities directed

at Russia. Based on this, the DDIS assesses that Russia is currently conducting hybrid warfare against NATO and the West.

Consequently, the hybrid threat from Russia against NATO will highly likely increase in the coming years.

As an example, Russia has deployed fighter jets to protect its shadow fleet as it carries Russian oil out of the Baltic Sea and has violated the airspace of NATO states with, for instance, fighter jets, helicopters and attack drones. The states that have been most affected by Russian airspace violations in recent months are Poland, Estonia, Finland, and Romania.

Russia's aggressive military behaviour may serve multiple purposes, including testing NATO members' response capabilities and causing concern among member states that NATO is headed towards war with Russia.

Hybrid warfare is unfolding across multiple domains and is evolving gradually. Russia will highly likely develop new methods and means to apply pressure on Denmark in the coming years.

In light of recent incidents, including those in the Baltic Sea Region, the DDIS has prepared an overall updated assessment of the threat to Denmark, including the various hybrid threats.

The sabotage threat
The threat of sabotage against the Danish Armed Forces is **HIGH**.

Since 2023, Russia has orchestrated a series of sabotage operations against targets in Europe. Russia is likely conducting a conventional sabotage campaign to undermine Europe's support for Ukraine.

Russia often use individuals who are not directly linked to Russian intelligence services to carry out sabotage operations. Consequently, Russia has only partial control over the saboteurs. The attacks have generally been relatively simple to execute.

A number of Russian plans and operators were uncovered, and the intensity of the sabotage campaign declined from autumn 2024.

Destructive cyber attacks
The threat level of destructive cyber attacks against Denmark is **MEDIUM**.

Since 2023, hacker groups aligned with Russia have increasingly launched destructive cyber attacks, including against Western critical infrastructure. The targets were all poorly protected. In Denmark, pro-Russian hackers caused water pipes to burst at a Danish water utility in December 2024, leaving some of its customers temporarily without water.

In addition, hackers aligned with Russia have repeatedly carried out disruptive cyber attacks aimed at rendering Danish government and corporate websites unavailable. The DDIS assesses that some of the pro-Russian hacker groups are linked to the Russian state.

At the same time, Russian state-sponsored hackers are attempting to infiltrate digital systems in Danish and Western critical infrastructure, likely partly in an effort to prepare destructive cyber attacks that Russia could choose to launch at a later date.

It is likely that Russian state-sponsored hackers have shown a growing interest in Danish critical infrastructure over the past few years.

It is less likely that Russia, in the current circumstances, will carry out destructive cyber attacks aimed at causing severe widespread disruption to essential societal functions.

Military provocations
The DDIS assesses that the overall threat of military provocations against NATO member states is **HIGH**.

The threat of military provocations stems from Russia's increasingly aggressive behaviour since its full-scale invasion of Ukraine in 2022.

Since 2022, Russian military units have exhibited increasingly threatening and aggressive behaviour, engaging in reckless navigation, simulated attacks on NATO forces, and jamming of civilian and military ship and aircraft communications systems as well as GPS signals.

There are also examples of Russia having acted very aggressively towards NATO states operating close to its borders – for instance, in September 2022, a Russian fighter jet fired an air-to-air missile towards a British reconnaissance aircraft above the Black Sea.

In addition, Russia has repeatedly violated the airspace of several NATO states with attack drones and fighter jets, among other things. This type of violation has intensified over the past few months.

Malign influence
The threat of Russian malign influence operations against Denmark is **LOW**.

The DDIS assesses that Denmark is currently not a separate, priority target of Russian malign influence operations.

Russia, however, continuously seeks to shape political decision-making and public opinion across Europe, including in Denmark. Russia's influence operations are ongoing and have, since the start of the war in Ukraine in 2022, primarily been aimed at sowing discord in Europe and weakening Western support for Ukraine.

The influence operations are conducted both via online platforms and through "influence agents" – individuals who cooperate with foreign

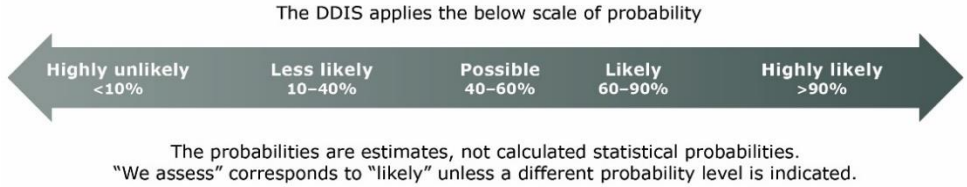
intelligence services to establish and exploit relationships abroad for influence purposes.

The military threat
The threat of conventional military attacks against Denmark is **NONE**.

Russia views itself as being in conflict with the West and is preparing for a potential war with NATO. While no decision to initiate such a war has been made, Russia is building up its military and expanding its capabilities to make that decision.

At present, Russia continues to seek to avoid actions that could trigger NATO's Article 5.

Nevertheless, it is highly likely that Russia will employ hybrid tactics to test and shift the threshold for what could invoke NATO's collective defence under Article 5.



Threat levels
The Danish Defence Intelligence Service uses the following threat levels.

NONE	There are no signs of a threat. There are no actors with both the capacity and intention for attacks/harmful activity.
LOW	There are one or more actors with the capacity and intention for attacks/harmful activity. However, either the capacity or the intention or both are limited.
MEDIUM	There are one or more actors with the capacity and intention for attacks/harmful activity. However, there are no indications of specific planning of attacks/harmful activity.
HIGH	There are one or more actors that have the capacity for and are specifically planning attacks/harmful activity or that have already carried out or attempted attacks/harmful activity.
VERY HIGH	There is either information that one or more actors are initiating attacks/harmful activity, including information about time and target, or that one or more actors are continuously initiating attacks/harmful activity.

An applied threat level reflects the DDIS' assessment of the intention, capacity and activity of one or more actors based on the available information.