DANISH MINISTRY OF DEFENCE

Offensive Cyber Effects

Denmark has since 2016 contributed to NATO's cyber defence and in 2018 it was announced that Denmark can also contribute to NATO operations with effects from the offensive cyber capability

A contribution to NATO with offensive cyber effects means that Denmark delivers an effect to a target in a NATO Area of Operation using cyber capabilities (weapons). The capability is deployed from facilities in Denmark under national command, but the action takes place in the context of a NATO operation and against targets abroad. To support this, it may be necessary to deploy Danish personnel to take part in the planning and coordination of cyber operations from an international operations centre.

The Danish military capability for operations in cyberspace is planned to be fully operational by the end of 2019

Offensive cyber effects aim at supporting military operations. Cyber capabilities may be employed in support of other military means or independently against a given target. The capability operates in the virtual world but delivers effects in the physical world, and can be employed against targets connected to the internet or against targets that are part of a closed network, where an access has been found.

The Danish Defence Intelligence Service is responsible for providing defensive and offensive cyber operations in support of the Danish Defence.

The DDIS "Hacker Academy" has attracted many skilled employees for the offensive cyber capability.

Cyber capabilities – part of the military toolbox

Employment of offensive cyber capabilities in a military operation will take place under the commmand of the Chief of Defence. Prior to participation in an international operation it is assessed whether consent from the Parliament (Folketinget) is required – exactly as is the case for other conventional weapons.

Cyber in NATO

Cyberspace was recognized as a military domain along with the land, sea and air domains at the NATO summit in Warszaw in 2016. The cyber domain is now in the process of being integrated into NATO's command structure and concrete actions relating to the cyber defence and deterrence profile is are handled at political, strategical and operational levels.

The cyber capability is in daily use

When the cyber capability is not used for military operations, it is available for the Director of the Danish Defence Intelligence Service (DDIS), who can make use of the capability as a an additional tool for executing the service's daily tasks. This is a significant strenghtening of the Intelligence Service's overall capacity to gather information through cyberspace on activities of state and criminal actors. It ensures that full advantage is taken daily of the cyber capability and that a high level of expertise is developed and maintained.