



Danish Cyber Fact Sheet

The Danish Cyber and Information Security Strategy

The main objectives of the Danish Cyber and Information Security Strategy are to:

- Maintain and reinforce trust amongst both citizens and businesses and ensure that efforts to strengthen cyber and information security do not preclude the user-friendliness and effectiveness of new technologies.
- Increase the protection of important functions in society against cyber attacks and thereby to safeguard national security.

To support these objectives, the Danish government has identified six strategic focus areas which are targeted with specific initiatives to raise the cyber and information security level of the Danish society:

- Professionalised and reinforced ICT oversight
- Clear guidelines for suppliers
- Strengthened cyber security and increased knowledge
- Robust infrastructure in the energy and telecommunications sectors
- Denmark as a strong international partner
- Strong investigation and high level of information

The Strategy is being revised in 2016 with the involvement of views and insights from interest groups, businesses and academia on how further efforts may benefit society most.



Denmark has developed a robust national cyber defence capability to protect its static networks. Furthermore, Denmark is in the process of developing a cyber defence capability to support deployable networks. In addition to the NATO requirements for cyber defence, Denmark intends to develop a military capability for cyber network operations.



Main actors:

The Centre for Cyber Security

- The Centre for Cyber Security is the national ICT security authority and was established in 2012.
- The Centre for Cyber Security's key mission is to strengthen the protection of ICT infrastructure that supports functions vital to the Danish society and to strengthen Denmark's general ability to resist advanced cyber attacks. Organizationally attached to the Danish Defence Intelligence Service (DDIS), the Centre has access to the intelligence-based knowledge about cyber issues available to the DDIS. The Centre provides advice on cyber-related issues as well as a Network Security Service to relevant authorities and companies.
- Furthermore, the Centre advises on preventive measures and issues guidelines and recommendations.
- Lastly, the Centre is the National Regulatory Authority on information security in the telecommunications sector. Its supervision of the Danish telecommunications providers includes agreements with the providers regarding the scope of their information security efforts.

The Agency for Digitisation

- The Agency was established in 2011 to speed up the digitisation processes required to modernise the Danish welfare society.
- The Agency is in charge of the digitisation of Denmark and is responsible for the implementation of the government's digital ambitions in the public sector.

The Police

- Investigate cyber crime.
- Preventive measures to ensure a minimum of cyber related crimes.
- Established National Cyber Crime Centre (NC3) in 2014.

In general, each ministry supervises own authorities and agencies, and is responsible for the information security within the ministries area of responsibility.