Ministry of Defence

Cyber security

Defence Cyber Strategy

The Netherlands Defence organisation will ensure improved and more intensive security of the digital environment, or cyberspace.

In its Defence Cyber Strategy, the Netherlands Defence organisation prioritises the following 6 points:

1: Digital security must be addressed on all fronts
The armed forces use digital systems in almost all of their operations. They are used for logistics, command and control, intelligence, force protection, manoeuvre and firepower. Defence Cyber Command (DCC) is made up of military personnel from all 4 armed forces Services.

2: Strengthening the Defence organisation's digital resilience
The Defence organisation is responsible for protecting its own networks and systems. Joint Information Technology Command (JITC) will ensure that the digital resilience of the organisation is strengthened.

The JITC will have a dedicated team, the Defence Computer Emergency Response Team (DefCERT), working to protect the digital infrastructure of the Defence organisation. The team will assess the risks and weak points of the main Defence networks 24/7 and advise on security measures.

3: Capability of mounting military cyber operations
The Netherlands armed forces must not only be able to defend itself against cyber attacks, but must itself also be capable of mounting cyber attacks, in support of other operations, for example. The JITC will cooperate as closely as possible with the Defence Intelligence and Security Service (DISS).

4: Strengthening of the intelligence position in the digital domain
The Netherlands armed forces must have an insight into the possible threats from cyberspace in order to arm itself appropriately. This includes insight into technological threats and into the possibilities and intentions of potential or actual adversaries and attackers.

- In the coming years, the DISS will be given more capability for covertly gathering information from the cyber domain. As a result, the DISS will more regularly be able to infiltrate networks and computers for gathering information. The service will also be able to better monitor essential networks and investigate the attack capabilities of third parties.
- The DISS and the General Intelligence and Security Service (GISS) will be given a joint unit for signals intelligence: the SIGINT Cyber Unit (cyber and signals intelligence).
- The DISS is going to cooperate closely with the Joint Information Management Command, the Netherlands Forensic Institute, the National Police Services Agency and the Royal Netherlands Marechaussee.

More about this topic

- Threats in the digital environment
- Cyber Command

Belongs to

- Royal Netherlands Army

5: Gaining a stronger knowledge base and increasing innovative ability in cyberspace

The Defence organisation will upgrade its knowledge, know-how and skills required for ensuring a secure digital environment:

- The Defence Cyberspace Centre of Expertise (DCEC) will enhance knowledge regarding cyber operations. DCEC will undertake cooperation with research institutes such as the Netherlands Organisation for Applied Scientific Research (TNO).
- The Defence organisation will establish a cyber laboratory and a test environment, where personnel will be able to carry out research and development.
- The Defence organisation's personnel policy will move towards recruiting and retaining personnel with cyber expertise.
- In 2012, a Senior Lecturer in Cyber Operations was appointed at the Netherlands Defence Academy.

6: The intensification of national and international cooperation

The Defence organisation will initiate cooperation in the area of cyber security on various fronts:

- The Defence organisation will be represented in the National Cyber Security Centre (NCSC).
- The Defence organisation will be represented in the Cyber Security Council. This comprises representatives from government bodies, private enterprise and science.
- The Defence organisation will work together with the IT innovation platform 'Veilig Verbonden' [Safe Connection].
- The Defence organisation operates large, complicated systems and thus accrues knowledge regarding system security. Defence will undertake cooperation with other NATO countries in this area