National Coordinator for Security and Counterterrorism
Ministry of Justice and Security

Disruption of society looms ahead

Biggest threat is espionage, disruption and sabotage by nation-state actors

Countries such as China, Iran and Russia have offensive cyber programmes against the Netherlands.

This means that these countries are deploying digital resources in order to achieve geo-political and economic objectives at the expense of Dutch interests. Disruption and sabotage have the greatest impact on national security.

Most critical processes and services are completely dependent on ICT

Dependence on digitised processes and systems has increased to such an extent that any impairment to these systems and processes can cause socially disruptive damage.

Fallback options and analogue alternatives are virtually non-existent. The scale of the threat and the fact that resilience is lagging creates risks for national security.

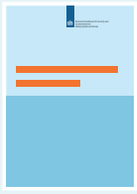
Cyber Security Assessment Netherlands 2019

The CSAN provides insight into threats, interests and resilience in relation to cyber security and the effect these factors have on national security.

Not all areas have resilience in order

Boosting resilience is the most important tool in reducing risk, affecting the various threats and dependency levels has proven to be a complex challenge.

Measures are not always taken as the costs and benefits of cyber security are unevenly distributed. Unsecure products and services are the Achilles heel of cyber security. The Netherlands is dependent on a limited number of providers from a limited number of countries. This makes society more vulnerable to the shifting intentions of these providers and countries.



The CSAN is published annually by the National Coordinator for Security and Counterterrorism and is written in cooperation with public and private partners.

Read the entire CSAN at **www.nctv.nl**