National Coordinator for Security and Counterterrorism
*Ministry of Security and Justice*

## Digital resilience lags behind

**The resilience of individuals and organisations is lagging behind the increasing threat.**

This will lead to increased risks unless extra countermeasures are taken.

## Democratic processes are being influenced

**Digital attacks are being used to influence democratic processes.**

Cyber attacks have influenced democratic processes in a number of countries. In the Netherlands, countermeasures were taken in the run up to the elections for the Dutch House or Representatives.

## Vulnerable internet of things

**The vulnerability of the Internet of Things has resulted in disruptive attacks that endorse the need to enhance digital resilience.**

More and more devices are connected to each other across the internet. This provides opportunities, but also creates risks.

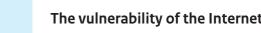## Professional criminals and countries biggest threat

**Professional criminals and state actors continue to be the most significant threat and inflict the most damage.**

Professional criminals seek financial gains. Countries conduct digital espionage, sabotage and exert influence. Over 100 countries world-wide use digital means for espionage to obtain confidential information from governments and companies.

## Strong dependency on infrastructure services

**Many organisations are dependent on a limited number of foreign digital infrastructure service providers which means that the social impact of disruption is large.**

Disruptions can have a substantial impact on society.

# Cyber Security Assessment Netherlands 2017

*The Cyber Security Assessment Netherlands 2017 offers insight into interests, threats and resilience in the field of cyber security.*

*The CSAN is drawn up in close collaboration between the National Cyber Security Centre and both public and private partners and is an annual publication of the NCTV.*

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