National Coordinator for Security and Counterterrorism
Ministry of Justice and Security

Digital risks have not diminished and remain fundamentally the same.

The primary digital risks to national security are espionage and sabotage by other countries.

There is also a risk of large-scale system failures due to human error, technical breakdowns or cyberattacks by criminals. The digitalisation of our society continues to proceed at a rapid pace. Digital security has become a prerequisite for a functional society.

Cyber risks are intertwined with other risks.

Cyber incidents can spread quickly and widely, impacting other domains around the world and striking at the very heart of society.

This is particularly true when such incidents occur simultaneously with other crises. A large-scale cyber incident during the current COVID-19 pandemic would have major repercussions.

Cybersecurity Assessment for the Netherlands 2020

The CSAN offers insight into digital threats, interests and resilience, in a national security context.

Boosting resilience is key, but cyber resilience is not yet evident everywhere.

By enhancing our cyber resilience, we can reduce both the likelihood of cyber incidents occurring and their impact.

Digital risks are sometimes underestimated. Individual parties do not always feel called upon to contribute to the cybersecurity of society as a whole. We also lack a complete, accurate overview of the cyber resilience of critical processes in the Netherlands.

What does this mean for your organisation?

This is the first edition of the CSAN that seeks to help answer this question. Use the three threat scenarios and answer the key questions. Think about whether the scenarios could happen at your organisation and consider what precautions you have taken and what to do if an incident occurs despite your best efforts.

The CSAN is an annual publication of the NCTV, produced in collaboration with the National Cyber Security Centre (NCSC).

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