National Coordinator for
Counterterrorism and Security
Ministry of Justice and Security

The CSAN 2025 in a nutshell

November 2025

The digital threat landscape is becoming increasingly diverse and unpredictable. State actors, cybercriminals and other malicious actors are carrying out a wide range of attacks. Moreover, geopolitical unpredictability is spilling over into the digital domain. State actors are developing or expanding cyber programmes by using non-state actors or private organisations. Furthermore, shifting geopolitical relations can make digital dependencies risky even if they previously were not. Malicious actors can also use generative AI, which makes attacks easier and more scalable.

All these developments are unfolding at the same time and influence one another, which makes the threat landscape increasingly complex. Building and maintaining digital resilience is certainly not getting any easier, but it does not need to be overly complex either. Basic digital principles provide an effective barrier against a large proportion of cyberattacks. Digital security has long ceased to be just a matter for technical experts. Especially for non-digital factors such as geopolitics, it is – or should be – a matter for the boardroom.

Cyber capabilities are increasing, and there is a mixture and proliferation of actors

Countries are increasingly willing to use their power to promote their geopolitical interests, thereby expanding their cyber capabilities. State actors use cyberattacks to achieve their political, military, and/or economic goals and are able to promote their interests without crossing the legal threshold of armed conflict. Some state actors make ingenious use of companies and organizations or so-called state-sponsored groups. State-sponsored groups include cybercriminals or hacktivists who are not officially part of a state. However, these groups are often tolerated, supported, or directed by state actors. This blending of state cyber capabilities with non-state organizations leads to further complexity and an unpredictable threat landscape.

Threat to telecom sector is real, Netherlands also targeted

For years, there has been a justified focus on the resilience of critical infrastructure; after all, the continuity of a vital process such as telecommunications is of great importance to the functioning of our society. Incidents in the US telecoms sector show that the sector is of interest to actors and that the threat is manifesting itself. In the Netherlands, too, a number of small internet service and hosting providers have been targeted by malicious actors. Although there have been no major incidents in the Netherlands to date and resilience within the sector is robust, the sector remains an attractive target for malicious actors. It is therefore essential to maintain digital resilience in critical sectors at all times.

Geopolitical developments emphatically expose dependencies

Europe, and therefore the Netherlands, is dependent on providers from mostly non-European countries for many different digital processes and services. For example, public organizations in all kinds of sectors are increasingly dependent on services provided by a few large technology companies in the US.

In the current geopolitical context, we must take into account that countries are weighing their own interests more carefully, which means that the Netherlands may be confronted with dependencies that could be used as leverage. It is precisely these geopolitical developments that could make dependence on digital services and processes from other countries risky or potentially risky.

Generative AI amplifies existing threats to digital security

In recent years, the development of generative AI has accelerated. The technology behind it does not constitute a threat, but specific applications – combined with the intent of the actor using it – can give rise to new risks. Generative AI can be used in multiple ways: both to support malicious activity and as a defence against threats. At present, generative AI primarily amplifies existing digital threats.

In addition, generative AI itself is a potential target. This involves attacks aimed at disrupting or misleading AI systems.

Annual Review

Although nuances are changing, there have been no major shifts in the threat landscape. There is a wide variety of incident types, causes, attackers, and degrees of impact. Both state actors and cybercriminals carry out cyberattacks on Dutch targets and/or affect Dutch interests. Edge devices remain of interest to malicious actors. DDoS attacks also continue to occur. In addition, there are regular cybersecurity incidents at suppliers/service providers that lead to data breaches at customers. In addition to incidents caused by cyberattacks, there are again numerous examples of disruptions resulting from unintentional actions, such as software errors.

The CSAN was prepared by the National Coordinator for Counterterrorism and Security (NCTV). This involved close cooperation with, among others, the National Cyber Security Center (NCSC). The CSAN is published annually by the NCTV.

Read the entire CSAN 2025 online:
Cyber Security Assessment Netherlands | National Coordinator for Security and Counterterrorism (nctv.nl)