

2025 in outline

The year 2025 is characterized as a year in which much has been set in motion. A new advisory process regarding the digital safety of citizens has commenced. In addition, exploratory discussions were held for a potential new advisory process concerning the resilience of the energy sector. The advisory processes on AI and cybersecurity, and on the resilience of the communication infrastructure, took further shape.

Advisory projects

Digital safety of citizens

The digital resilience of citizens is under increasing pressure due to cybercrime, online fraud, and data misuse. To strengthen this resilience in a targeted manner, the Council approved a new advisory process on this matter on September 25. The process focuses on prevention, victimization, reporting behavior, and providing a course of action. A subcommittee has been formed comprising a delegation of Council members as well as several experts from outside the Council, including representatives from various ministries, the General Intelligence and Security Service (AIVD), the Public Prosecution Service, the Police, the ECP Platform for the Information Society, and the financial sector. The first steps consist of further defining the research directions and preparing the advisory process.

Energy sector resilience (SEIN)

The energy sector is one of the vital sectors in the Netherlands, as an energy shortage brings society to a virtual standstill. The consequences of an energy outage are therefore far-reaching. Consequently, the continuity of the energy supply is of vital importance. The Council acknowledges that the Dutch energy infrastructure is relatively robust and that extensive research is already being conducted, including on behalf of the former Ministry of Climate and Green Growth (KGG) and the Top Sector Energy. At the same time, geopolitical developments, growing cyber threats, and incidents in countries such as Spain and Portugal are causing us concern; for the Council, this is reason for a joint exploration. Consequently, discussions were held in the second half of the year with key stakeholders in the field, including CIOs and CISOs of grid operators and producers, representatives of trade associations, public parties, and the academic community. Based on these discussions, a starting document was developed at the end of the year.

AI and cybersecurity

Artificial intelligence (AI) is increasingly being deployed as a weapon, and the Netherlands is insufficiently prepared for this. With the deployment of AI, cyberattacks are faster, larger in scale, and more difficult to detect, while Dutch defensive capabilities are too weak to counter these attacks due to a lack of AI expertise. As early as 2023, the Council alerted the Cabinet to the dangers of AI. Due to rapid technological developments and geopolitical shifts, the Council has taken up this theme again. The knowledge gap is the biggest problem: the expertise is currently primarily in the hands of malicious actors, often states with offensive cyber programs. This advisory process culminates in a Signal Letter on AI and cybersecurity, which will be ready in draft form by the end of the year.

Communication infrastructure resilience (SECCOM)

The telecommunications and internet infrastructure is the digital backbone for all vital sectors in the Netherlands, including healthcare, energy, transport, banking, and the government. Without this infrastructure, our society grinds to a halt. The Dutch digital communications infrastructure is of high quality and the sector functions well. Geopolitical developments raise the question of whether resilience is still sufficient. The digital landscape has vulnerable characteristics: geographical concentration of data center infrastructure around Amsterdam, dependence on a limited number of critical third parties, missing failover mechanisms, and limited capacity to handle power outages. This calls for measures to increase robustness. Therefore, the Council has commissioned an in-depth study for advice to the Cabinet. A large part of the activities in 2025 was dedicated to this study, carried out by TNO.

Informant's letter

With a view to the formation of a new Cabinet following the national elections in October, the CSR has drafted a letter addressed to the informateur. In it, the Council advocates for structural investments in the digital resilience of the Netherlands. The letter was finalized in draft form at the end of the year.

Annual Review

March

- Progress report on the pilot of data breach notifications for investigation purposes, as a follow-up to the CSR advice [Making data breach notifications available for investigation purposes \(2020\)](#)
- Dialogue with new management of the National Cyber Security Center (NCSC)

June

- Publication of new version of the Cybersecurity [Handbook for Directors and Business Owners](#)
- Dialogue with the Court of Audit regarding three studies in the field of digitalization and cybersecurity within the central government
- Dialogue regarding ABRO (General Security Requirements for Central Government Contracts) with the Ministry of the Interior and Kingdom Relations.

April

- [Executives' Dinner](#) on Operational Technology, organized for executives from the public and private sectors and academia. Operational technology is the collective term for hardware and software systems for managing processes, such as controlling and monitoring (industrial) equipment.

September

- Visit by State Secretary for the Interior and Kingdom Relations Van Marum to the council.

November

- Working visit by the council to The Hague Security Delta (HSD), a cluster of 300 companies, government and knowledge organizations in The Hague
- [Executives' breakfast](#) on the importance of risk-based governance and basic hygiene in cybersecurity, organized in collaboration with the Center for Information Security and Privacy Protection (CIP). The central question was how executives can gain more control over cybersecurity at a time when digital threats are increasing and organizations are becoming increasingly dependent on complex chains.

December

- [CSR response](#) to new edition of Cybersecurity Landscape Netherlands
- Appointment of Martijn Jonk as acting secretary of the CSR, succeeding Raymond Doijen

Outlook

By the year 2025, much will have been set in motion at the CSR, in parallel with the rapidly increasing dynamics in geopolitical, technological, and economic spheres. For example, while AI was still a promise in 2023-2024, it is now manifesting itself at a rapid pace as a systems technology with unprecedented effects, including on digital security. The solutions have not changed, but the urgency to apply them now has grown significantly. The sentiment is that the time for talking is over; action must be taken, as a small country in a rapidly becoming more insecure world. Europe is the stage for action for this; cooperation within the EU is essential.

In this changing, increasingly complex, and international playing field for cybersecurity and digital safety, the CSR envisions its task for the coming years even more clearly: to bring together private, public, and academic parties, mobilize forces, and translate these into solution-oriented advice for the Cabinet, Parliament, the business community, and society. The leading themes in this regard are resilience, autonomy, AI, and cybercrime.

Composition and changes to the CSR and the office

The reference date for this overview is 1 January 2025. Changes occurred in the council during the year; see the section Changes for details.

Private sector

- Mr. Th.J. (Theo) Henrar (Acting Co-Chair), Chairman of FME (employer's organization for the technology industry), member of the CSR on behalf of FME
- Ms. C. (Claudia) de Andrade, CIO, Director Digital & IT Port of Rotterdam, member of the CSR on behalf of the CIO Platform
- Mr. J.P. (Joost) de Bruin, CEO of Ordina Netherlands and member of the General Board of NLdigital, member of the CSR on behalf of NLdigital
- Mrs. Mr. S.C. (Sylvia) van Es, President Philips Netherlands, member of the CSR on behalf of VNO-NCW
- Mr. J. (Joost) Farwerck, CEO and Chairman of the Executive Board of KPN, member of the CSR representing the vital sectors
- Mr. E.F.M. (Eppo) van Nispen tot Sevenaer, Chairman ECP, Platform for the Information Society, member of the CSR on behalf of ECP
- Mr. S.J.A. (Steven) van Rijswijk, CEO of ING and Board Member of the Dutch Banking Association, member of the CSR representing the financial sector

Public sector

- Mr. P.J. (Pieter-Jaap) Aalbersberg EMPPM (co-chair), National Coordinator for Counterterrorism and Security (NCTV)
- Mr. E.S.M. (Erik) Akerboom MPM, Director-General of the General Intelligence and Security Service (AIVD)
- Mr. M. (Michiel) Boots, Director-General for Economy and Digitalisation at the Ministry of Economic Affairs and Climate Policy
- Mr. Lieutenant General M.L.E. (Ludy) Schmidt, Deputy Commander of the Armed Forces at the Ministry of Defence
- Ms. E. (Eva) den Dunnen-Heijblom MSc, Director-General for Digitalisation and Government Organisation at the Ministry of the Interior and Kingdom Relations
- Ms. J.C. (Janny) Knol MA, Chief of Police
- Mr. A.R.E. (Guus) Schram MSc, Attorney General and Deputy Chairman of the College of Attorneys General

Scientific sector

- Prof. Dr. B. (Bibi) van den Berg, Professor of Cybersecurity Governance affiliated with the Institute of Security and Global Affairs at Leiden University
- Prof. Dr. Ir. H.J. (Herbert) Bos, Professor at the Systems Security Group VUSEC at the Vrije Universiteit Amsterdam
- Prof. Dr. Ir. C.E.W. (Cristian) Hesselman, Professor of Trusted Open Networking at the University of Twente and Director of Trusted Digital Infrastructures at SURF
- Prof. E.M.L. (Lokke) Moerel, Senior Of Counsel Morrison & Foerster LLP, Professor Tilburg University

Auditors

On behalf of the public sector

- Mr. Drs. EA (Ernst) Noorman, Ambassador in General Cyber and Security Service

On behalf of the private sector

- Ms. P (Petra) Oldengarm, Director of Cyberveilig Nederland

CSR Secretary's Office

- Mr. i r. W.M.G. (Raymond) Doijen, Secretary (until 6 December)
- Mr. M.W.M. (Martijn) Jonk MSc, Acting Secretary (from 7 December)
- Mrs. H.M. (Heidi) Letter, Coordinating Senior Advisor
- Ms. M.M.E. (Marloes) van Baren, Senior Communications Advisor
- Mr. A.P. (Arwin) Bosman, Senior Advisor
- Mr. M. (Marc) Brinkman, Senior Advisor
- Ms. N. (Nova) van der Kamp, Government Trainee
- Ms. B. (Bahar) Karacabey, Management and Policy Support Officer
- Mrs. S.N.N. (Salina) Stubbe, Management and Policy Supporter
- Ms. B.J. (Briede) Troost, Advisor

CHANGES IN THE COMPOSITION OF THE COUNCIL

Stepped down in 2025

- Mr. P.J. (Pieter-Jaap) Aalbersberg EMPM (co-chair), National Coordinator for Counterterrorism and Security (NCTV)
- Ms. C. (Claudia) de Andrade, CIO, Director Digital & IT Port of Rotterdam, member of the CSR on behalf of the CIO Platform
- Mr. J.P. (Joost) de Bruin, CEO of Ordina Netherlands and member of the General Board of NLdigital
- Ms. P. (Petra) Oldengarm, Director of Cyberveilig Nederland (auditor)

Joined in 2025

- Mr. R. (Rob) Bravenboer, Managing Director for Kyndryl Netherlands, Member of CSR on behalf of NLdigital
- Ms. L. (Liesbeth) Holterman, Director of Cyberveilig Nederland (auditor)

In 2025, Theo Henrar served as acting co-chair of the council. He replaced Sylvia van Es, who remained a council member.

Colophon

About the Cyber Security Council

The Cyber Security Council is a national and independent advisory body to the Cabinet, composed of high-ranking representatives from public and private organizations and academia. The CSR is committed to enhancing cybersecurity in the Netherlands at a strategic level. Due to the unique composition of the council (public, private, and academia), it is possible to strategically approach priorities, bottlenecks, and incidents from diverse perspectives and to develop an integrated vision of opportunities and threats. The CSR seeks cooperation with similar councils in other countries and encourages their establishment in countries that do not yet have an advisory body in the field of cybersecurity.

The council strives for the broadest possible coverage of perspectives in the field of cybersecurity. Therefore, the eighteen council members serve according to a 7-7-4 distribution key: seven from the private sector, seven from the public sector, and four from academia. In addition, the CSR has two observers.

The CSR has two co-chairs: one representing the public sector and one representing the private sector.

Read more at <https://www.cybersecurityraad.nl>

Cyber Security Council

Korte Voorhout 7

2511 CW The Hague

The Netherlands

Phone 070 - 7515 333

E-mail info@cybersecurityraad.nl

Website www.cybersecurityraad.nl

Mailing address:

P.O. Box 20011

2500 EA The Hague

The Netherlands

The Hague, June 2026